

From: [I&A PB](#)
Cc: [I&A PB](#)
Subject: (U//FOUO) IA: Pre-Travel Activities Exhibited by US Persons Aspiring to Fight in Syria Provide Detection Opportunities, dated 6 January 2016
Date: Wednesday, January 06, 2016 1:21:41 PM
Attachments: [\(U-FOUO\) IA - Pre-Travel Activities by US Persons Aspiring to Fight in Syria Provide Detection Opportunities 01062016.pdf](#)

Colleagues,

(U//FOUO) The attached Intelligence Assessment: Pre-Travel Activities Exhibited by US Persons Aspiring to Fight in Syria Provide Detection Opportunities, dated 6 January 2016 has been released. CTAB members, Field Operations, IGA, OPA, and OLA are receiving this message and attachment to ensure uninterrupted access to I&A's finished analytic products.

(U) This product will also be available via NCTC Current and the I&A websites on HSDN and HTSN (JWICS); HSIN; and CapNet.

(U//FOUO) **Intended Audience:** Federal, state, local, tribal, and territorial government agencies and authorities; and the private sector

(U//FOUO) To locate the product on HSIN, go to HSIN Central page at <https://hsin.dhs.gov>, and copy and place the title in the search bar.

(U//FOUO) For more information regarding HSIN please visit http://www.dhs.gov/files/programs/gc_1156888108137.shtm or contact (b) (6) for access.

Very Respectfully,
I&A Intelligence Publications Division
Department of Homeland Security

(b) (6)

(b) (6)

(b) (6)



Homeland
Security

INTELLIGENCE ASSESSMENT



(U//FOUO) Pre-Travel Activities Exhibited by US Persons Aspiring to Fight in Syria Provide Detection Opportunities

6 January 2016

Office of Intelligence and Analysis

IA-0045-16

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

(U) All US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at (b) (6).

From the Secretary

6 January 2016

The accompanying assessment was prepared by the DHS Office of Intelligence and Analysis, in coordination with the Defense Intelligence Agency, Federal Bureau of Investigation, and National Counterterrorism Center. I urge you to review it closely, as it provides very useful information to address the current threat environment.

Let's all work hard for a safe 2016, and remain vigilant.

JCJ



Jeh C. Johnson

Secretary

Department of Homeland Security



**Homeland
Security**
Office of Intelligence and Analysis

INTELLIGENCE ASSESSMENT

6 January 2016

(U//FOUO) Pre-Travel Activities Exhibited by US Persons Aspiring to Fight in Syria Provide Detection Opportunities

(U) Prepared by the DHS Office of Intelligence and Analysis (I&A). Coordinated with DIA, FBI, and NCTC.

(U) Scope

(U//FOUO) This Assessment examines the pre-travel activities and trends associated with 42 arrested US persons who sought to or succeeded in traveling to Syria or Iraq to fight with or support fighting by foreign terrorist organizations (FTOs) or armed opposition groups since 2013. All of the examined individuals were arrested between January 2013 and November 2015 and are either awaiting trial, have already pled guilty, or been found guilty in a court of law. Thirty-six of the individuals were arrested attempting to travel to Syria or Iraq, and six were arrested following their return from Syria. Our findings are based primarily on (b) (3), (b) (7)(E). This Assessment is intended to inform federal, state, local, tribal, and territorial counterterrorism, law enforcement, and countering violent extremism (CVE) officials on observable activities violent extremists often engage in prior to traveling to conflict zones. It builds on a body of previously released I&A assessments related to US aspiring or successful foreign fighters' motivations, social media use, fundraising efforts, travel routes, and operational security practices. The cutoff date for information in this Assessment is 30 November 2015.

(U) Key Findings

(U//FOUO) Our review (b) (3), (b) (7)(E) of 42 aspiring or successful travelers to Syria or Iraq—with a median age of 22—indicated that (b) (3), (b) (7)(E)

We judge the individuals' public support primarily for the Islamic State of Iraq and the Levant (ISIL) was likely driven by their vulnerability to ISIL's messaging that offers them a cause to join, the willingness of many young people to publicly share their views on social media, and, in some cases, a probable lack of concern that law enforcement could learn of the individuals' support for violent extremist causes.

(U//FOUO) Despite the frequent consumption and influence of terrorist messaging on social media, 27 of these individuals (b) (3), (b) (7)(E)

. Seventeen of the individuals also (b) (3), (b) (7)(E)

(U//FOUO) Approximately half of the examined individuals (b) (3), (b) (7)(E)

. (b) (3), (b) (7)(E)

. Additionally, those we examined used a variety of techniques to (b) (3), (b) (7)(E)

(U//FOUO) Approximately half of the subjects engaged (b) (3), (b) (7)(E)

(b) (3), (b) (7)(E) The employment of these (b) (3), (b) (7)(E) measures, combined with half of the examined subjects (b) (3), (b) (7)(E)

(U//FOUO) Just over half of the individuals lived with family members during their radicalization and mobilization to violence, (b) (3), (b) (7)(E)

(U//FOUO) Parents, other family members, friends, religious leaders, and law enforcement attempted to intervene or dissuade travel to Syria in at least 15 cases, (b) (3), (b) (7)(E)

(U//FOUO) Frequent Public Posting of Terrorist Messaging and Contact with US- or Overseas-Based Violent Extremists (b) (3), (b) (7)(E)

(U//FOUO) Our review of (b) (3), (b) (7)(E) indicates that 19 of the 42 aspiring or successful Syria foreign fighters posted or praised on social media the messaging or actions of FTOs. These individuals' public signaling of their adoption of a violent extremist mindset most often (b) (3), (b) (7)(E). (b) (3), (b) (7)(E) they were most likely to generally praise ISIL; positively comment on ISIL videos, ISIL-related imagery such as the group's flag, issues of its English-language magazine *Dabiq*, or statements by its leadership; or pledge allegiance to the group.

(b) (3), (b) (7)(E) s'—the median age of the 42 individuals was 22—(b) (3), (b) (7)(E)

- » (U) A New York-based individual pledged allegiance to ISIL (b) (3), (b) (7)(E), asked that specific ISIL leaders be protected from harm, and posted several other pro-ISIL (b) (3), (b) (7)(E) (b) (3), (b) (7)(E). He was arrested in July 2015 for a previous trip to Turkey, on which he allegedly sought—unsuccessfully, as it turned out—to reach Syria to join ISIL.
- » (U) An Illinois-based individual posted a link on (b) (3), (b) (7)(E) to a video about ISIL Emir Abu Bakr al-Baghdadi in January 2015. (b) (3), (b) (7)(E). He was arrested in March 2015 and is currently awaiting trial for seeking to fight for ISIL overseas and allegedly discussed attacking police stations, courts, and a National Guard facility in the Homeland with his now-arrested cousin.
- » (U) A Pennsylvania-based woman currently awaiting trial for her March 2015 attempt to join ISIL in Syria made pro-ISIL posts (b) (3), (b) (7)(E) starting around August 2013, including posting a video of an ISIL Western fighter giving advice, a photograph of an ISIL child soldier, and a photograph of an ISIL fighter soliciting donations, (b) (3), (b) (7)(E)

(U//FOUO) Despite the growing trend of individuals using social media to view violent extremist messages, 27 of the 42 individuals (b) (3), (b) (7)(E) (b) (3), (b) (7)(E)

* (U//FOUO) DHS defines radicalization as the process through which an individual changes from a non-violent belief system to a belief system that includes the willingness to actively advocate, facilitate, or use unlawful violence as a method to effect societal or political change.

(b) (3), (b) (7)(E)

- » (U) Three of the examined individuals—two brothers and a former high school classmate from New Jersey—were arrested in the summer of 2015 for planning to travel to Syria to join ISIL, (b) (3), (b) (7)(E). The brothers lived together and probably reinforced each other's devotion to ISIL, and one of the siblings convinced his former classmate to join their plan to travel to Syria by "preying on his insecurities and pain," according to (b) (3), (b) (7)(E).
 - » (U) In April, six Minnesota-based individuals were arrested for their attempts to travel to Syria to join ISIL, (b) (3), (b) (7)(E). The group of friends watched videos together encouraging fighting on behalf of Islam, met secretly to plan their travel, and shared contact information with each other of ISIL members in Syria, (b) (3), (b) (7)(E).
 - » (U//FOUO) Twenty of the 42 individuals (b) (3), (b) (7)(E). This demonstrates the frequency with which aspiring fighters seek (b) (3), (b) (7)(E).
- (U//FOUO) Twenty-two of the examined individuals (b) (3), (b) (7)(E), and 17 of the 22 had never (b) (3), (b) (7)(E).
- » (U) An Illinois-based individual, who pled guilty in October 2015 to attempting to provide material support to ISIL, was in contact on multiple mobile messaging applications with a Western ISIL member named Abu Qa'qa he first communicated with (b) (3), (b) (7)(E). When the Illinois-based individual arrived in Turkey, an associate of Abu Qa'qa intended to take the US person to ISIL in Syria or Iraq, (b) (3), (b) (7)(E).
 - » (U) A North Carolina-based individual, who was arrested in March 2014 for his plan to travel to Syria to fight with al-Nusrah Front (NF), indicated he was talking online to an injured fighter in Syria and an Australia-based associate who encouraged him to maintain strong operational security, (b) (3), (b) (7)(E).
 - » (U) A Colorado-based woman began online relationships with multiple ISIL fighters and planned to travel to Syria to marry a 32-year-old Tunisian ISIL fighter with whom she talked via Skype, (b) (3), (b) (7)(E). The woman was arrested at a Colorado airport in April 2014, where she planned to depart to meet her Tunisian suitor.

(U//FOUO) Given that 34 of the 42 individuals were arrested after ISIL's June 2014 announcement that it had reestablished the Caliphate, (b) (3), (b) (7)(E).

* (U//FOUO) For more information, see the DHS-JTAC Intelligence Assessment "(U//FOUO) Syria-Based US and UK Persons' Public Social Media Activity Effective but Provides Terrorism Prevention Opportunities," released on 20 May 2015.

† (U//FOUO) DHS defines an HVE is a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor.

- » (U) A Mississippi-based couple arrested in August 2015 sought to join ISIL in Syria to provide medical aid to injured ISIL fighters and assist the group's media efforts to rectify alleged falsehoods about ISIL, (b) (3), (b) (7)(E). The female also indicated that she wished to raise the couple's future children in ISIL-controlled territory.
- » (U) A Texas-based individual desired to live in Syria with his wife and two children, and he also aspired to fight with ISIL, (b) (3), (b) (7)(E). He was sentenced to seven years in prison in June 2015 on charges of attempting to provide material support to terrorists.
- » (U) A Wisconsin-based individual indicated he did not like living in the United States and hoped to not return once he left for Syria, (b) (3), (b) (7)(E). He was arrested in April 2015 after traveling to Turkey in 2014 but failed to reach Syria and link up with ISIL or NF.

(U//FOUO) (b) (3), (b) (7)(E) Commonly Precede Attempted Travel to Conflict Zones

(U//FOUO) Approximately half of the examined individuals (b) (3), (b) (7)(E) in the months prior to their attempted travel, underscoring that some (b) (3), (b) (7)(E) Attempts by potential HVEs to (b) (3), (b) (7)(E)

- » (U) Seventeen individuals in the study (b) (3), (b) (7)(E) in the months preceding their travel, with three claiming (b) (3), (b) (7)(E), and four requesting (b) (3), (b) (7)(E). For example, a Minnesota-based individual who was arrested in November 2014 for attempting to travel to join ISIL first came to the attention of law enforcement in April 2014 when he (b) (3), (b) (7)(E).
- » (U) The FBI in April 2015 arrested two men in California after they traveled from Minnesota with the stated goal of traveling to Mexico (b) (3), (b) (7)(E). The previous month, the two individuals—along with four Minnesota-based associates who were subsequently also arrested in April—were in contact with a Syria-based associate who claimed he could help secure a (b) (3), (b) (7)(E).

(U//FOUO) (b) (3), (b) (7)(E)

- » (U) One of the six Minnesota-based individuals arrested in April 2015 tried to sell his car in the weeks before travel to raise additional funds, (b) (3), (b) (7)(E). Another individual in the group withdrew \$5,000 in cash from his financial aid debit card in the weeks prior to his failed May 2014 attempted departure for Syria, (b) (3), (b) (7)(E).
- » (U) A Texas-based individual sentenced in June 2015 for attempting to travel with his family to join ISIL stated in the months prior to his departure that he was waiting to get his tax refund before embarking, trying to earn money by

volunteering for a medical study, and considering raising money by selling his firearms, (b) (3), (b) (7)(E)

- » (U) A Colorado-based woman arrested in April 2014 for traveling to join ISIL claimed in an interview with law enforcement officials prior to her attempted departure that someone, probably an overseas violent extremist, had purchased the airline ticket for her, (b) (3), (b) (7)(E). Additionally, an Ohio-based individual who was arrested on terrorism-related charges in February 2015 after returning from Syria allegedly received from his Syria-based brother the contact information for a travel facilitator who assisted the Ohio-based individual in entering Syria from Turkey, (b) (3), (b) (7)(E).

(U//FOUO) Six arrestees are believed to have engaged (b) (3), (b) (7)(E) —in the months preceding attempted travel, (b) (3), (b) (7)(E). We assess this number possibly undercounts the number of arrestees who took steps to prepare for (b) (3), (b) (7)(E).

- » (U) Two North Carolina-based violent extremists engaged in physical training routines and participated in firearms and military tactics instruction before they were arrested in March 2014 for attempting to travel to Syria, (b) (3), (b) (7)(E).
- » (U) The Colorado-based woman arrested in April 2014 claimed in an interview with law enforcement officials that she joined the US Army Explorers program so she could be trained in military tactics and firearms, which she intended to use overseas while engaging in violence on behalf of ISIL, (b) (3), (b) (7)(E).

(U//FOUO) Many Attempted to Hide Their Intentions with (b) (3), (b) (7)(E)

(U//FOUO) Approximately half of the arrested subjects engaged in a range of (b) (3), (b) (7)(E) many of these may be detectable by family members, associates, or law enforcement officials. (b) (3), (b) (7)(E)

- » (U) Six weeks prior to attempting to travel to join ISIL in April 2015, a Pennsylvania-based woman allegedly shut down her Twitter account—where she frequently re-posted ISIL messaging and expressed a desire for “martyrdom” in Syria—and told an online associate she did so (b) (3), (b) (7)(E). Similarly, less than two months before being arrested in June 2015 for taking steps to travel to join ISIL, a New Jersey-based individual allegedly closed his Facebook account, (b) (3), (b) (7)(E).
- » (U) A separate New Jersey-based individual, who intended to join ISIL and was arrested in August 2015, changed cellphones, ceased using the home computer of the individual he was living with, claimed he was traveling abroad to study, switched to communicating on the phone in Arabic instead of English, and shaved his beard in the weeks prior to attempting to travel, (b) (3), (b) (7)(E).

(U//FOUO) (b) (3), (b) (7)(E)

* (U) For additional information, see the DHS and FBI Roll Call Release, “(U) Mobilization of Violent Extremists in the United States,” released on 17 January 2012.

(b) (3), (b) (7)(E)

» (U) (b) (3), (b) (7)(E)

» (U) (b) (3), (b) (7)(E)

» (U) Finally, five subjects attempted or succeeded in evading US law enforcement detection by (b) (3), (b) (7)(E)

(U//FOUO) Few Examples of Homeland Plotting by Examined Arrestees, but Interest Increasing Among Overall HVE Population

(U//FOUO) Only about 20 percent of the arrestees—eight of the 42 in this study—expressed an interest in undertaking Homeland plotting or allegedly took concrete steps to plan or assist a proposed attack in the United States, (b) (3), (b) (7)(E) s. Only three other arrested individuals publicly expressed online support for the 2015 terrorist attacks in Chattanooga, Tennessee and Garland, Texas. (b) (3), (b) (7)(E)

(U//FOUO) However, the surge in arrests in 2015 for Homeland plotting—as of September 2015, 17 arrests had been reported for the year compared to just two in 2014—(b) (3), (b) (7)(E)

† We further assess (b) (3), (b) (7)(E)

- » (U) Before being arrested for attempting to travel to join ISIL in March 2015, an Illinois-based individual—who served in the National Guard—discussed with his cousin attacking the military installation where he trained, offered to supply his cousin with military uniforms, and provided his cousin with the installation's training schedule, (b) (3), (b) (7)(E).
- » (U) A New York-based individual arrested in February 2015 for attempting to travel allegedly expressed interest in receiving guidance for engaging in an act of violence on US soil, such as killing the President of the United States or planting a bomb on Coney Island in New York. His arrested co-conspirator claimed that if he was unable to get travel documents to go to Syria, he would instead buy a machine gun and shoot law enforcement officers, (b) (3), (b) (7)(E).
- » (U) Prior to seeking to travel to Syria to join NF in April 2013, an Illinois-based individual provided suggestions on attack techniques and potential targets to an associate arrested in September 2012 for plotting to detonate a bomb outside an Illinois bar, (b) (3), (b) (7)(E). The former individual backed out of the plot in August 2012 because he suspected law enforcement was aware of it.

* (U//FOUO) For more on travel tradecraft, see DHS Intelligence Assessment, "(U//FOUO) 'Hidden City' Airline Ticketing a Viable and Utilized Method to Disguise Travel From United States to Syria," released on 8 December 2014.

† (U//FOUO) For additional information, see the DHS Reference Aid, "(U//FOUO) Analysis of ISIL-Related Arrests in the Homeland from January 2014-September 2015," released on 5 November 2015.

† (U//FOUO) DHS defines a lone offender as an individual motivated by one or more ideologies extremist ideologies who, operating alone, supports or engages in acts of unlawful violence in furtherance of that ideology or ideologies that may involve influence from a larger terrorist organization or a foreign actor.

(U//FOUO) Family Members Often First to Detect Pre-Travel Activities, (b) (3), (b) (7)(E)

(U//FOUO) Just over half of the individuals examined lived with family members at the time of their radicalization and mobilization to violence, likely indicating that parents and other close relatives are frequently best positioned to discover early indications that young people are preparing to engage in violent extremist activities overseas. (b) (3), (b) (7)(E)

- » (U) In April 2015, law enforcement was alerted to a New Jersey-based violent extremist who was increasingly displaying signs of radicalization to violence, including expressing support for ISIL orally and on Facebook, justifying the 2015 *Charlie Hebdo* attacks in France, changing his mobile phone, and expressing a newfound desire to study in Jordan, (b) (3), (b) (7)(E)
- » (U) Notebooks found in the residence and car that an Illinois-based individual—who was arrested in October 2014—shared with his parents outlined his plan for getting to Syria and revealed other pro-ISIL statements and symbols, (b) (3), (b) (7)(E)

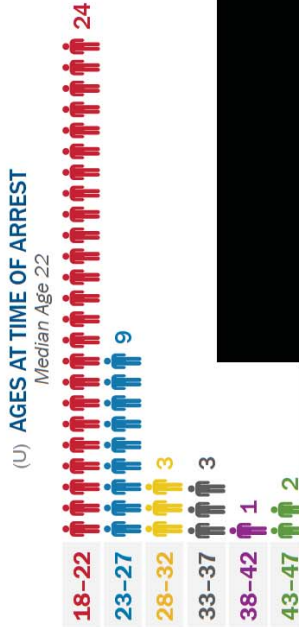
(U//FOUO) In at least 15 of the cases reviewed, parents, other family members, friends, religious leaders, and law enforcement officials (b) (3), (b) (7)(E)

- » (U) The parents of a now-arrested New York-based individual took away his passport between August and October 2014 to prevent him from traveling on a flight he booked from New York to Turkey, with the intention of continuing to Syria to join ISIL. (b) (3), (b) (7)(E) The individual had retrieved his passport or acquired a new one by July 2015, however, and was arrested while attempting travel. Similarly, the sister of a Michigan-based individual who aspired to join Lebanese Hizballah in Syria confiscated her brother's Lebanese passport in September 2013 to prevent him from traveling. (b) (3), (b) (7)(E) The individual then filed an application to become a US citizen in order to get a US passport; he was subsequently arrested in March 2014 at Detroit Metropolitan Airport.
- » (U) A Minnesota-based individual abandoned his plan to drive from Minnesota to California with the goal of continuing on to Syria after family members questioned the intended purpose of his travel as he was preparing his car for the road trip. (b) (3), (b) (7)(E) The individual was subsequently arrested in April 2015, however, with five other associates for attempting to travel to join ISIL. One of those associates—who previously attempted to travel to join ISIL in November 2014—abandoned his latest plan to leave for Syria after his father confronted him about his goal of joining ISIL. (b) (3), (b) (7)(E)
- » (U) After traveling to Turkey on his way to allegedly join ISIL in February 2014, a Texas-based individual decided to immediately return home after learning that his mother had purportedly been hospitalized, information that was falsely provided in order to convince him to come back. (b) (3), (b) (7)(E) Similarly, a North Carolina-based individual who booked travel to Turkey with intended onward travel to Syria in September 2013 abandoned his plans after stating that he “could not muster the strength to leave his parents” at that time, (b) (3), (b) (7)(E). The subject was arrested two months later for attempting to travel to join NF.

(U) Appendix A

(U) OVERVIEW OF PRE-TRAVEL ACTIVITIES EXHIBITED BY US PERSONS ASPIRING TO FIGHT IN SYRIA

(U//FOUO) I&A examined the pre-travel activities and trends—(b) (3), (b) (7)(E)—associated with 42 persons who sought to or succeeded in traveling to Syria or Iraq to fight or support fighting between January 2013 and November 2015. Nineteen of



(b) (3), (b) (7)(E)

(b) (3), (b) (7)(E)

(U//FOUO) Appendix B: Common Pre-Travel Activities of Aspiring Foreign Fighters

(U//FOUO) Some observed activities that may be suspicious include constitutionally protected activity. These activities should not be reported absent articulable facts and circumstances that support the source agency's suspicion that the observed behavior is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, such as indications of possible preparations for or attempts to travel overseas to engage in or support violence. The following activities were commonly present among the 42 cases of aspiring or successful foreign fighters we examined in this study, or in DHS' review of other recent HVEs who have sought to travel overseas for violent extremist purposes:

(b) (3), (b) (7)(E)



(U) Source Summary Statement

(U//FOUO) This Assessment is based primarily on I&A's review of (b) (3), (b) (7)(E), which we supplemented with (b) (3), (b) (7)(E). We have (b) (3), (b) (7)(E).
s. Some of these individuals also likely used encrypted communication platforms during their radicalization and mobilization to violence, (b) (3), (b) (7)(E).

(U) Report Suspicious Activity

(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit <http://nsi.ncirc.gov/resources.aspx>.

(U) Tracked by: HSEC-8.1, HEC-8.2, HSEC-8.3, HSEC-8.5

From: [REDACTED]
To: [Field Ops \(ALL\)](#)
Subject: FW: I&A Assessment on Pre-Travel Activities of Aspiring US Foreign Fighters
Date: Friday, January 15, 2016 2:54:57 PM
Attachments: [\(U--FOUO\) IA - Pre-Travel Activities by US Persons Aspiring to Fight in Syria 01062016.pdf](#)

FYI – IGA will be pushing to the HSAs as well.

From: Clark, Alaina
Sent: Friday, January 15, 2016 1:45 PM
To: (b) (6)
Cc: [REDACTED]
Subject: FW: I&A Assessment on Pre-Travel Activities of Aspiring US Foreign Fighters

Hi [REDACTED],

At the CVE meeting yesterday I&A briefed out on the attached product – I thought this might be something the HSAs are interested in. (b) (5)

[REDACTED]

[REDACTED]

[REDACTED]

Let me know your thoughts, happy to take your lead on this one.

Alaina

From: [REDACTED]
Sent: Thursday, January 14, 2016 3:31 PM
To: Clark, Alaina
Cc: [REDACTED]
Subject: I&A Assessment on Pre-Travel Activities of Aspiring US Foreign Fighters

Alaina-

Nice seeing you this afternoon at the CVE WG. Here is the new I&A assessment on pre-travel activities that we briefed during the meeting.

Feel free to forward the assessment, as you find appropriate, to your SLTT network, including HSAs.

Thanks and have a good afternoon,

[REDACTED]

(b) (6)
Homeland Violent Extremism Branch
Office of Intelligence and Analysis
U.S. Department of Homeland Security

(b) (6)

[REDACTED]

(b) (6)

From: [FusionCenterTraining](#)

To: (b) (6)

Cc: [Field Ops \(Field\)](#)

Subject: Announcing – 2 More Webinar Presentations - Tuesday, September 29th and Wednesday, September 30th

Date: Monday, September 28, 2015 11:33:19 AM

Attachments: [image003.jpg](#)
[image004.jpg](#)
[image005.png](#)
[image008.png](#)
[image007.png](#)

Announcing – 2 More Webinar Presentations

If you have not already registered please do so today!! Spaces Available!

1. **Fusion Centers and Countering Violent Extremism - Tuesday - 9/29/15 at 3:00 pm ET**
(2:00 pm CT, 1:00 pm MT, 12:00 Noon PT, 9:00 am HI)
2. **Sovereign Citizens, ISE-SARs and P/CRCL protections - Wednesday - 9/30/15 at 2:00 pm ET**
(1:00 pm CT, 12:00 pm MT, 11:00 am PT, 8:00 am HI)

There are still seats available for these webinars.

You are invited to register for one or more of a series of upcoming webinars for P/CRCL Officers and Fusion Center leadership. These webinars are on topics of current interest with a focus on privacy, civil rights, and civil liberties issues.

Length:

Each webinar is 90 minutes, designed to be interactive, and will include downloadable material relevant to the session. Each is being offered by national experts in the topic area.

Registration:

Within 24 hours of receiving your email, we will send instructions for logging in and any suggested pre-webinar reading.

Register by emailing us at FusionCenterTraining@dhs.gov

Please register separately for each session.

Note the webinar title in the subject line of your email.

<div data-bbox="386 304 418 336" data-label="Image"></div>	<p>Fusion Centers and Countering Violent Extremism</p> <p>Tuesday - 9/29/15 at 3:00 pm ET (2:00 pm CT, 1:00 pm MT, 12:00 Noon PT, 9:00 am HI)</p> <p>Discussion will include: A short briefing on the threat including on-line recruitment and recruitment from the US of overseas fighters; CVE issues for P/CRCL Officers to consider such as terminology in Intel and other products and looking at radicalization to violence through a cr/cl lens; Emerging trends in local level response to federal CVE initiatives; Overview of federal CVE initiatives.</p>
<div data-bbox="386 661 418 693" data-label="Image"></div>	<p>Wednesday - 9/30/15 at 2:00 pm ET (1:00 pm CT, 12:00 pm MT, 11:00 am PT, 8:00 am HI)</p> <p>Sovereign Citizens, ISE-SARs and P/CRCL protections</p> <p>This discussion will center around the recently released DHS document "SARs/ISE-SRAS and Sovereign Citizen Adherents", which provides a series of examples of potential ISE SARs and an analysis of whether each is appropriate for including in the Shared Data Repository. We will discuss a range of p/cl considerations associated with these analyses and address several operational issues.</p>

Webinar sponsor:

The DHS Office for Civil Rights and Civil Liberties

Questions?

Call (b) (6), at

(b) (6)
Program Coordinator
CRCL Institute
Office for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington, DC 20528

(b) (6)
(b) (6)
(b) (6)
(b) (6)

From: (b) (6)
To: [SLPO IO RD](#)
Cc: [SLPO Review:](#) [REDACTED] [Mcallister, Scott;](#) [REDACTED]
Subject: CVE Training Resource Webportal
Date: Wednesday, October 31, 2012 12:37:32 PM
Attachments: @

All,

On 1 October, Secretary Napolitano announced the launch of a new Countering Violent Extremism Training Resource Webportal, co-hosted by DHS and the FBI. The Webportal, developed in close partnership with IACP and other law enforcement association, is now available to federal, state, local, tribal, territorial and correction law enforcement training practitioners through the Homeland Security Information Network (HSIN). The Webportal provides access to hundreds of the most current Countering Violent Extremism training and training related materials, case studies, analytic products, and other resources. It also provides a platform for communication and information sharing about Countering Violent Extremism among DHS and other law enforcement training practitioners from across the country.

The Webportal was developed in response to demand for CVE training resource material that is accurate, appropriate, and that can be used by law enforcement training practitioners

From: (b) (6)
To: [SL Midwest](#)
Subject: DOI /FC P/CR/CL AND CVE AAR
Date: Monday, April 30, 2012 11:50:55 AM

Boss & Colleagues,

The DOI/FC hosted DHS' Privacy, Civil Rights and Civil Liberties (P/CR/CL) training on 17 April and Countering Violent Extremism (CVE) curriculum on 18 April. Since most of you have already hosted this training I'll keep this After Action Report brief and highlight only those areas that may be of help for future training venues.

The two training flyers we published, with assistance from Training Division, were passed previously in my WAR so to save Inbox storage limits please refer to that document but if anyone wants another copy, just email/call and I'll forward. There are no proprietary elements to either of these flyers so please use and edit them if they are of value to your next training venues.

(b) (5)

_____?" The third time I was requested
to provide information, I had to call RD (b) (6) and (b) (5)

For Privacy, Civil Rights and Civil Liberties we maxed out our training facility with 30 attendees. This is partly due to the fact that Director (b) (6) made the P/CR/CL mandatory for all Fusion Center Staff including our special agents. Overall, most of the critiques came in at the 4 and 5 level (out of 5 maximum possible) so I'm pleased, relieved actually, that our Fusion Center staff found it useful and informative.

For the CVE training, I (b) (5) for our 250 seat venue. (b) (5) we only had a final attendance of 75. (b) (5); there were no other big conferences in Iowa conflicting with our dates but from the outset, there just didn't seem to be interest or an enthusiastic response from our law enforcement, DHS Component or First Responder communities to this part of our two-day course offering.

As far as content, the P/CR/CL is understandably a bit dry as to content but two of the three instructors, (b) (6) were animated with good information flow and kept the participants' attention. (b) (6) was also part of the P/CR/CL presentation and my IT manager, our Iowa Privacy Officer, and I found his delivery a (b) (5). Fortunately (b) (6) had the smallest part of the P/CR/CL training block (b) (5). (b) (6) presented a condensed version of his CVE training during the last hour of the first day's P/CR/CL portion and (b) (6) always puts on a good session. I'd be interested

if others have evaluated (b) (6) in the same light (b) (5) .
(b) (6) was the sole presenter on the second day's CVE training and his critiques were also in the 4-5 range and (b) (5) .

Dang, thought I could keep this to one page. Please feel free to reach out to me if you have not yet had this training and would like clarification on any aspects of the preparation or execution of these courses.

V/R

[Redacted]

(b) (6)
U.S. Department of Homeland Security
State of Iowa Intelligence Fusion Center
(b) (6)

From: (b) (6)
To: [REDACTED]
Subject: FW: CVE Executive Meeting, 03/03/15, 9:00 A.M.
Date: Thursday, September 03, 2015 6:55:39 AM
Attachments: @

[REDACTED]
Rocky Mountain Regional Director
Department of Homeland Security
Office of Intelligence & Analysis

Office: (b) (6)

Cell: [REDACTED]

~~Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need to know" without prior approval of an authorized DHS official.~~

From: [REDACTED]
Sent: Wednesday, March 04, 2015 7:59 AM
To: Field_Operations; (b) (6)
Cc: hqdeppax_rd
Subject: FW: CVE Executive Meeting, 03/03/15, 9:00 A.M.

(b) (6)

Here is a recap of yesterday's FBI / DOJ hosted CVE meeting.

From: (b) (6)
To: [SL_RockyMountainRegion](#)
Subject: FW: ISIS In America
Date: Tuesday, February 09, 2016 1:39:04 PM
Attachments: [FYI #3 ISIS in America - Full Report 0.pdf](#)

RMR,

For those who haven't seen this.

V/r,

(b) (6)

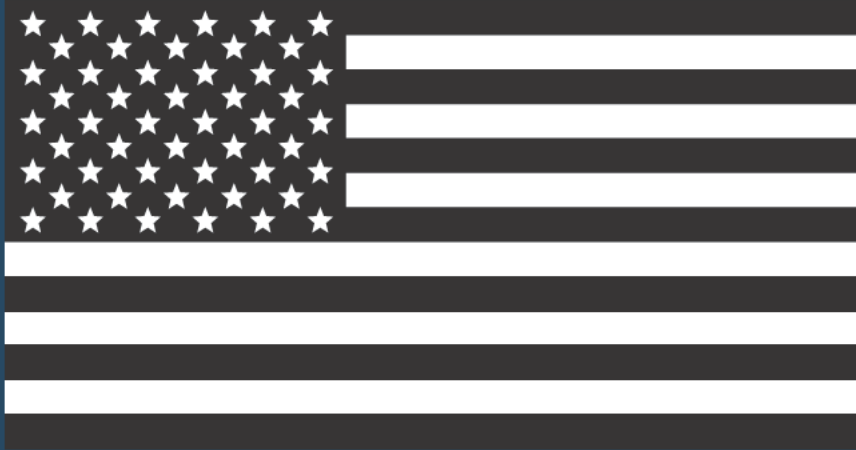
U.S. Department of Homeland Security
Minnesota Fusion Center (MNFC)

(b) (6)

(b) (6)

(b) (6)

ISIS IN AMERICA



FROM RETWEETS TO RAQQA

Lorenzo Vidino and Seamus Hughes
December 2015

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

ISIS IN AMERICA: FROM RETWEETS TO RAQQA

Lorenzo Vidino and Seamus Hughes
December 2015

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

All rights reserved. Printed in the United States of America. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

© 2015 by Program on Extremism

Program on Extremism
2000 Pennsylvania Avenue NW, Suite 2210
Washington, DC 20052
www.cchs.gwu.edu/program-extremism

CONTENTS

Acknowledgments	■	v
Foreword	■	vii
Executive Summary	■	ix
Introduction	■	1
A Snapshot of ISIS in America	■	5
From Keyboard Warriors to Battlefield Commanders: Understanding the Spectrum of ISIS in America	■	15
Conclusion	■	33
Appendix	■	35

Illustrations

1. Young (left) and Dakhalla	■	1
2. Young's Twitter account	■	1
3. ISIS Recruits in the U.S. Legal System	■	6
4. Excerpt from missing persons report filed by family of the Somali-American teens	■	8
5. Tweet posted by the 16-year-old Denver girl	■	8
6. Reposted by one of the Denver girls on Tumblr on the anniversary of their failed trip	■	8
7. Hoda Muthana's high school yearbook portrait	■	9
8. Muthana on life in the caliphate, January 2015	■	9
9. El Gammal, December 2013	■	10
10. Samy identifies himself: excerpt from El Gammal's criminal complaint	■	10

(continued on next page)

Illustrations, continued

11. Soofi (left) and Simpson ■ [10](#)
12. Usaamah Abdullah Rahim ■ [11](#)
13. Amiir Farouk Ibrahim's American passport ■ [11](#)
14. Douglas McCain, aspiring rapper turned jihadist ■ [12](#)
15. Hanad Abdullahi Mohallim's Twitter profile ■ [12](#)
16. Abdullah Ramo Pazara (right) in Syria ■ [12](#)
17. Abu Muhammad al Amriki explains his defection to ISIS ■ [13](#)
18. One of Abu Khalid al Amriki's final tweets ■ [13](#)
19. News of Abu Khalid al Amriki's death circulates on Twitter ■ [13](#)
20. Abu Abdullah al Amriki ■ [14](#)
21. ISIS announces Abu Abdullah al Amriki's death ■ [14](#)
22. Moner Abu Salha, a.k.a. Abu Hurayra al Ameriki ■ [16](#)
23. Ariel Bradley celebrates the Chattanooga shootings ■ [16](#)
24. Snapshot of life in the caliphate: image from Ariel Bradley's Instagram account ■ [17](#)
25. Mohammed Hamzah Khan on Twitter ■ [20](#)
26. Elton Simpson pledges allegiance to ISIS before his attack ■ [21](#)
27. The Radicalization Echo Chamber ■ [22](#)
28. Examples of ISIS supporters' imagery on social media ■ [23](#)
29. Clockwise: A user announces a new account; examples of node, shout-out, and amplifier accounts ■ [24](#)
30. Clockwise: Interjecting in the #BlackLivesMatter conversation; sharing a quote from Anwar al Awlaki; dismissing ISIS critics as "coconuts" ■ [25](#)
31. From the U.S. to Syria: Abdullah Ramo Pazara ■ [27](#)
32. Nader Saadeh ■ [28](#)
33. Alaa Saadeh ■ [28](#)
34. Samuel Topaz on Facebook ■ [28](#)
35. Facebook post by Mohamed Saeed Kodaimati ■ [29](#)
36. Mohamed Saeed Kodaimati ■ [29](#)
37. Shannon Maureen Conley ■ [30](#)
38. Christopher Lee Cornell ■ [31](#)

ACKNOWLEDGMENTS

THIS REPORT was made possible by the dedicated work of the Program on Extremism's staff, including its Research Associates, Sarah Gilkes and Patrick Hoover, who played an integral role in developing the research methodology, collecting the data, and contributing to written analysis; and the Program's team of Research Assistants: Audrey Alexander, Brooklyn Granowicz, Seth Harrison, Netanel Levitt, Raed Mourad, and Nicole Rickard. Thank you to Larisa Baste for her assistance in formatting the report.



The views expressed in this publication are solely those of the authors, and not necessarily those of the George Washington University.

About the Program on Extremism

The Program on Extremism provides analysis on issues related to violent and non-violent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public. The Program is part of the Center for Cyber and Homeland Security (CCHS) at the George Washington University.

FOREWORD

by Jane Harman

IN 2007, as a Member of Congress, I introduced the Violent Radicalization and Homegrown Terrorism Prevention Act. We were just starting to understand how terrorists could manipulate the Internet—Twitter was one year old—and my bill would have established a national commission to study the issue and advise Congress. After passing the House by an overwhelming bipartisan vote, the proposal was blocked in the Senate over claims it would reestablish J. Edgar Hoover’s COINTELPRO—a huge distortion.

Eight years later, the issue couldn’t be more urgent. The new radicalization crosses borders. Loners don’t have to leave their basements to find extremist messages. Some radical Islamists coordinate complex attacks using PlayStations, while some hatch plots without ever contacting a known terrorist. Paris, Beirut, a Russian jet downed over Sinai: these are just the most recent outbreaks of a terrorist pandemic.

In a democracy like ours, the expression of radical views is protected by the Constitution. Violent action—inspired by those beliefs—is not. Our challenge is to identify the triggers for violence and intervene at just the right moment to prevent it. But as *ISIS in America* makes clear, one size doesn’t fit all. Homegrown terrorists don’t fit a single profile. Using social media, our enemies can micro-target their audiences, selling a narrative we need to learn to counter.

Efforts like George Washington University’s Program on Extremism have a critical role to play. Based on extensive interviews, court records, and media reports, *ISIS in America: From Retweets to Raqqa* is a comprehensive study of known ISIS recruits in the United States. More

than 50 have been arrested this year alone, a new record, and hundreds are the targets of ongoing investigations. What drew them to ISIS’s twisted fantasy? How do we pull them away? How can we identify the next lone wolf before he—or she—sets off the next pressure cooker bomb?

This report is a deep, responsible start. It takes a 21st century approach: the Internet overhauled radicalization, and it should also upgrade the way we study it. As I argued this year in *Foreign Affairs*, some of the most important intelligence is no longer secret. Some of the best information is open-source, plastered on message boards or a 19-year-old’s Twitter feed. Policymakers have been slow to adapt; spies would still rather squint at satellite photos than scrape Facebook feeds.

As the head of the Wilson Center, chartered by Congress to bridge the worlds of scholarship and policy, I welcome this contribution to our national conversation. It is consistent with our values and our First Amendment principles to ask tough questions. We can’t win if we fear the answers. Going forward, *ISIS in America* will be a critical resource for scholars, citizens, and policymakers. It will form common ground for dialogue as we confront a shared challenge: maximizing liberty and security. I look forward to more work from the Program on Extremism, thank them for this effort, and applaud their commitment to knowledge in the public service.

■ ■ ■

Jane Harman is president and chief executive of the Woodrow Wilson Center in Washington. She represented California’s 36th Congressional District for nine terms.

EXECUTIVE SUMMARY

- WHILE NOT AS LARGE as in many other Western countries, ISIS-related mobilization in the United States has been unprecedented. As of the fall of 2015, U.S. authorities speak of some 250 Americans who have traveled or attempted to travel to Syria/Iraq to join the Islamic State in Iraq and Syria (ISIS) and 900 active investigations against ISIS sympathizers in all 50 states.
- Seventy-one individuals have been charged with ISIS-related activities since March 2014. Fifty-six have been arrested in 2015 alone, a record number of terrorism-related arrests for any year since 9/11. Of those charged:
 - The average age is 26.
 - 86% are male.
 - Their activities were located in 21 states.
 - 51% traveled or attempted to travel abroad.
 - 27% were involved in plots to carry out attacks on U.S. soil.
 - 55% were arrested in an operation involving an informant and/or an undercover agent.
- A small number of Americans have been killed in ISIS-related activities: three inside the U.S., at least a dozen abroad.
- The profiles of individuals involved in ISIS-related activities in the U.S. differ widely in race, age, social class, education, and family background. Their motivations are equally diverse and defy easy analysis.
- Social media plays a crucial role in the radicalization and, at times, mobilization of U.S.-based ISIS sympathizers. The Program on Extremism has identified some 300 American and/or U.S.-based ISIS sympathizers active on social media, spreading propaganda, and interacting with like-minded individuals. Some members of this online echo chamber eventually make the leap from keyboard warriors to actual militancy.
- American ISIS sympathizers are particularly active on Twitter, where they spasmodically create accounts that often get suspended in a never-ending cat-and-mouse game. Some accounts (the “nodes”) are the generators of primary content, some (the “amplifiers”) just retweet material, others (the “shout-outs”) promote newly created accounts of suspended users.
- ISIS-related radicalization is by no means limited to social media. While instances of purely web-driven, individual radicalization are numerous, in several cases U.S.-based individuals initially cultivated and later strengthened their interest in ISIS’s narrative through face-to-face relationships. In most cases online and offline dynamics complement one another.
- The spectrum of U.S.-based sympathizers’ actual involvement with ISIS varies significantly, ranging from those who are merely inspired by its message to those few who reached mid-level leadership positions within the group.

INTRODUCTION

LIKE MOST NEWLYWED COUPLES, 22-year-old Mohammad Oda Dakhalla and his 19-year-old wife Jaelyn Delshaun Young were planning for their future. Dakhalla, the son of a local imam, was about to start graduate school at Mississippi State University (MSU). Young, a one-time high school cheerleader and the daughter of a Vicksburg, Mississippi, police officer, was a sophomore chemistry major at MSU.¹ Yet, unbeknownst to nearly all their relatives and acquaintances, the couple had developed a parallel life and conceived a secret honeymoon: traveling to Syria to join the Islamic State in Iraq and Syria (ISIS).

In the early months of 2015 the couple's radical musings on Twitter attracted the attention of the Federal Bureau of Investigation (FBI). During a four-month investigation, Dakhalla and Young repeatedly expressed their wish to contribute to the growth of ISIS's self-proclaimed caliphate to undercover FBI agents online. Young—who went by “Aaminah al-Amriki” on Twitter—asserted that she was “skilled in math and chemistry and worked at an analytical lab here at my college campus,” and that she wished to “raise little Dawlah [ISIS] cubs.” She claimed Dakhalla wanted to do propaganda work to “assure [Muslims] the US media is all lies when regarding Dawlah” and later, “join the Mujahideen.”²

In another conversation, Young informed an agent that after their Islamic wedding, the couple intended to make the journey to Syria.³ She explained, “Our story will be that we are newlyweds on our honeymoon,” adding, “In sha Allah the planning will land us in Dawlah with the grace of Allah swt [Subhanahu Wa Ta'ala, Arabic for ‘The most glorified, the highest’].”⁴ As their anticipated departure date inched closer, the couple penned farewell letters to their families explaining their actions were both deliberate and voluntary.⁵

The couple's plans never materialized. Just as the pair set out on their journey to Syria, the FBI arrested them at a small regional airport in Mississippi on August 8, 2015. Young and Dakhalla were charged with



FIG. 1 Young (eft) and Dakhalla



FIG. 2 Young's Twitter account

1. WAPT News, “2 Mississippi Residents Charged with Trying to Join ISIS: Jaelyn Delshaun Young, Muhammad Oda Dakhalla Arrested,” August 12, 2015.
2. *United States of America v. Jaelyn Delshaun Young and Muhammad Oda Dakhalla*, Criminal Complaint (August 8, 2015).
3. Ibid.
4. Ibid.
5. Ibid.

attempting and conspiring to provide material support and resources to a designated foreign terrorist organization.⁶

The couple's arrest made national news, arriving at the tail end of a summer that saw an unprecedented number of ISIS-related arrests across the country. While the U.S.-based ISIS supporters who have been charged come from a wide range of ethnic and socio-economic backgrounds, many share core characteristics: they were American-born, under age 30, and had no previous history of radical views or activities. How could these seemingly ordinary young American men and, in growing numbers, women, be attracted to the world's most infamous terrorist organization? There is no simple answer to this question, as each individual's radicalization has its own unique dynamics. Still, cases like that of Dakhllalla and Young are increasingly emblematic of the dynamics of radicalization seen throughout America over the last few years.

From Hijackings to Hashtags: The Evolution of Jihadism in America

Violent extremism of the jihadist inspiration is not a new phenomenon in America.⁷ Already in the 1980s, a small number of American citizens and residents traveled to

Afghanistan to join the *mujahideen* seeking to repel the Soviet invasion.⁸ Throughout the 1990s, scattered clusters of American-based militants were involved in other foreign conflicts (e.g. Bosnia and Chechnya) or provided material support to al Qaeda and other Sunni extremist groups. One such cluster based out of New York and New Jersey carried out one of the earliest attacks on U.S. soil, the 1993 World Trade Center bombing.⁹

After the September 11, 2001, attacks, the U.S. counterterrorism community adopted a more aggressive posture, resulting in the discovery of dozens of individuals and cells across the country. American jihadists operating throughout the 2000s and early 2010s varied significantly in terms of their profiles, organizational affiliations, and operational capabilities.¹⁰ While some had deep links to al Qaeda and its affiliates, others were nothing more than sympathizers of jihadist ideology lacking operational connections.

Over time, the greatest threat to the U.S. homeland came to be posed not so much by groups operating overseas (although a number of plots conceived by al Qaeda and its affiliates have been thwarted over the last decade), but from "self-radicalized, homegrown extremists in the United States."¹¹ In fact, in 2010 then-Attorney General Eric Holder indicated that the terrorist threat had "changed

6. WAPT News, "2 Mississippi Residents Charged with Trying to Join ISIS: Jaelyn Delshaun Young, Muhammad Oda Dakhllalla Arrested," August 12, 2015.
7. An inherently controversial and arguably improper term, "jihadism" refers to the ideology adopted by groups such as al Qaeda and ISIS. The authors are aware that the term "jihad" has a number of meanings and that most Muslims use the term in ways different than these groups.
8. J.M. Berger, *Jihad Joe: Americans Who Go to War in the Name of Islam* (Washington DC: Potomac Books, 2011).
9. See Lorenzo Vidino, "Homegrown Jihadist Terrorism in the United States: A New and Occasional Phenomenon?," *Studies in Conflict & Terrorism* 32, no. 1 (January 2009): 1-17.
10. For more on jihadist networks in the U.S., see Brian Michael Jenkins, "Stray Dogs and Virtual Armies Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11," RAND Corporation, Occasional Paper, 2011.; Risa A. Brooks, "Muslim 'Homegrown' Terrorism in the United States: How Serious Is the Threat?" *International Security* 36, no. 2 (Fall 2011): 7-47.; Charles Kurzman, "Muslim-American Terrorism in the Decade Since 9/11," Triangle Center on Terrorism and Homeland Security, February 2012.; Scott Matthew Kleinmann, "Radicalization of Homegrown Sunni Militants in the United States: Comparing Converts and Non-Converts," *Studies in Conflict and Terrorism* 35, no. 4 (2012): 278-297.; Jerome P. Bjelopera, "American Jihadist Terrorism: Combating a Complex Threat," Congressional Research Service, January 23, 2013.; Charles Kurzman, "Muslim-American Terrorism: Declining Further," Triangle Center on Terrorism and Homeland Security, February 1, 2013.; Jessica Zuckerman, Steven P. Bucci, and James Jay Carafano, "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," The Heritage Foundation, July 2013.; and Lorenzo Vidino, "From KSM's Genius to Sheer Amateurism: The Post-9/11 Evolution of the Terrorist Threat in the United States," in Bruce Hoffman and Fernando Reinares, eds., *The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death* (Columbia University Press, 2014), 3-28.
11. Testimony of Robert S. Mueller, III, Director of the Federal Bureau of Investigation, United States Senate, *Annual Worldwide Threat Assessment*, Select Committee on Intelligence, February 5, 2008.

from simply worrying about foreigners coming here, to worrying about people in the United States, American citizens—raised here, born here, and who for whatever reason, have decided that they are going to become radicalized and take up arms against the nation in which they were born.”¹²

American jihadists have engaged in a broad spectrum of activities, ranging from providing logistical support to several foreign terrorist organizations (mainly al Qaeda and its various affiliates but also the Taliban, Pakistan’s Lashkar-e-Taiba, Indonesia’s Jemaah Islamiyah, etc.) to fighting in foreign conflicts, particularly in Afghanistan, Iraq, and Somalia. In several cases these individuals planned attacks on U.S. soil. Authorities have thwarted most of these plots. In fact, many were conceived partially after prodding from the FBI, which since 9/11 has made abundant use of “sting operations” to prevent aspiring jihadists from committing acts of violence. On other occasions, American militants succeeded, as in the cases of Little Rock (2009), Fort Hood (2009), and Boston (2013).

Between 2001 and 2013, more than 200 U.S. citizens and permanent residents were convicted of terrorism-related activities.¹³ This figure clearly indicates that a small but significant number of American citizens and residents embrace jihadist ideology and are committed to using violence, at times against fellow Americans, to this end.

Of course, when analyzed in comparative terms, these numbers and dynamics can be seen in a different light. Some argue that other forms of extremism constitute an equal, if not larger, threat to American domestic security. A study by the New America Foundation, for example, has calculated that since 9/11 almost twice as many Americans have been killed by white supremacists and other anti-government domestic radicals than by Islamist extremists.¹⁴

Moreover, while the challenge of jihadist radicalization certainly exists in the United States, its intensity and size

are significantly smaller than in most European countries. Due to multiple concurring factors—such as a comparatively more integrated American Muslim community and the sporadic and geographically-limited presence of radicalizing agents (radical mosques, extremist preachers, and recruiting networks)—America has witnessed little of the radicalization dynamics seen in countries such as France, Great Britain, Belgium, and Denmark. The American “jihadist scene,” assuming a coherent one exists, is significantly smaller, more decentralized, and less professional than that of most European countries.

By 2011 the jihadist threat on both sides of the Atlantic appeared to have somewhat plateaued. To be sure, the problem of homegrown radicalization clearly still existed. But the somewhat stagnant level of the threat, better law enforcement and intelligence practices, and the enthusiasm generated in the West by the promise of the Arab Spring suggested that jihadism was a manageable and potentially even subsiding problem.

In the last four years, though, jihadism in the West has received a boost triggered by staggering events on the ground in the Middle East. In particular, the conflict in Syria, the successes achieved on the ground by ISIS and other jihadist groups, and ISIS’s formation of a self-proclaimed caliphate have had a magnetic draw for many young Western Muslims.

The scale of this recent mobilization is unprecedented. In May 2015, the United Nations Security Council estimated more than 25,000 foreign fighters from more than 100 countries have joined ISIS and other jihadist groups in Syria.¹⁵ Even though precise data is virtually impossible to obtain, it is believed that some 5,000 European citizens or residents have become foreign fighters in Syria and Iraq, a number that dwarfs all previous mobilizations (Afghanistan, Bosnia, Chechnya, Iraq, Somalia, and Mali) combined.¹⁶

12. Jack Cloherty and Pierre Thomas, “Attorney General’s Blunt Warning on Terror Attacks,” *ABC News*, December 21, 2010.

13. Charles Kurzman, “Muslim-American Terrorism in 2013,” Triangle Center on Terrorism and Homeland Security, February 5, 2014, p. 2.

14. Scott Shane, “Homegrown Extremists Tied to Deadlier Toll than Jihadists in U.S. Since 9/11,” *The New York Times (NYT)*, June 24, 2015.

15. United Nations’ Security Council, “Action Against Threat of Foreign Terrorist Fighters Must be Ramped Up, Security Council Urges in High-Level Meeting,” 7453rd Meeting (AM), May 29, 2015.

16. Peter R. Neumann, “Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s,” The International Centre for the Study of Radicalisation and Political Violence (ICSR), January 26, 2015.

Particularly alarming are numbers from certain countries, such as the 1,200 estimated to have left France, and the 400 who left Belgium, a country of only 11 million.

The numbers in the U.S., while similarly difficult to measure precisely, are significantly lower than those in most European countries. In June 2015 the FBI stated that “upwards of 200 Americans have traveled or attempted to travel to Syria to participate in the conflict.”¹⁷ A few weeks later, the Office of the Director of National Intelligence estimated that more than 250 individuals from the U.S. had traveled or attempted to travel to the conflict area, a few dozen had joined the ranks of ISIS, and some 20 had died.¹⁸

Moreover, the surge in the number of American foreign fighters is small compared to those who sympathize with and embrace ISIS’s ideology. American authorities have consistently said that the popularity of ISIS’s propaganda, driven largely by its savvy social media tactics, wholly overshadows that of al Qaeda. Tellingly, in May 2015 FBI Director James Comey spoke of “hundreds, maybe thousands” of ISIS sympathizers and potential recruits across the country, disclosing that the Bureau had related investigations running in all 50 states.¹⁹ A few months later, in October 2015, Comey revealed that the FBI had a staggering 900 active investigations against homegrown violent extremists.²⁰

Publicly available information confirms a sharp surge of jihadist activities in the U.S., especially when compared to dynamics seen in the years since the wave of arrests following 9/11. Since March 2014, 71 individuals in one way or another linked to ISIS have been charged in the U.S. for terrorism-related activities. The number of arrests has spiked in recent months, with 56 arrested since January 2015. In the same period, a handful of attacks have occurred across the country.

Searching for Answers

What explains the recent surge in American jihadi recruits? Who are the Americans lured by the siren songs of ISIS’s propaganda? How do they embrace such radical ideology, turning their backs on their country and, in most cases, their families? Do they do so by themselves or in clusters of like-minded individuals? Once radicalized, what do they seek: to join the ISIS caliphate between Syria and Iraq or to carry out attacks in the U.S.?

Answers to these and related questions concerning ISIS mobilization in the U.S. have puzzled authorities and the public alike. To shine new light on them, the staff at the George Washington University’s Program on Extremism engaged in a six-month study of the recent surge in domestic radicalization. The result is this report, which, while unable to examine every aspect of such a complex and fluid phenomenon, provides a comprehensive overview of ISIS-related radicalization and mobilization in the United States.

The report consists of two parts. The first examines all cases of U.S. persons arrested, indicted, or convicted in the United States for ISIS-related activities since the first case in March 2014. A wide array of legal documents related to these cases provides empirical evidence for identifying several demographic factors related to the arrested individuals. This section also looks at the cases of other Americans who, while not in the legal system, are known to have engaged in ISIS-inspired behavior.

The second part of the report examines various aspects of the ISIS-related mobilization in America. Here the report analyzes the individual motivations of ISIS supporters; the role of the Internet and, in particular, social media, in their radicalization and recruitment processes; whether their radicalization took place in isolation or with other, like-minded individuals; and the degree of their tangible links to ISIS.

17. Testimony of Michael B. Steinbach, Assistant Director of the FBI, *Terrorism Gone Viral: The Attack in Garland, Texas and Beyond*, House Homeland Security Committee, June 3, 2015.

18. Barbara Starr, “A Few Dozen Americans’ in ISIS Ranks,” *CNN*, July 15, 2015.

19. Tom Vanden Brook, “ISIL Activity Drives up Pentagon Threat Level,” *USA Today*, May 8, 2015.

20. Kevin Johnson, “Comey: Feds have Roughly 900 Domestic Probes about Islamic State Operatives,” *USA Today*, October 23, 2015.

CHAPTER 1

A Snapshot of ISIS in America

IT IS APPARENT that the U.S. is home to a small but active cadre of individuals infatuated with ISIS's ideology, some of whom have decided to mobilize in its furtherance. This section attempts to provide an overview of this demographic by drawing on research that attempted to reconstruct the lives—both real and virtual—of U.S.-based ISIS supporters. The research effort was based on legal documents, media reports, social media monitoring, and interviews with a variety of individuals, though there were at times limitations to both the amount and reliability of publicly available information.

Individuals our researchers identified were classified into three categories: Legal Cases, "At-Large," and Deceased. The Legal Cases include instances where people have entered the U.S. legal system for ISIS-related activities. As of November 12, 2015, 71 individuals have been charged on ISIS-related charges. Legal documents provide a plethora of verifiable information on these individuals. As such, both the degree and the nature of these individuals' affiliations to ISIS were relatively clear, allowing researchers to draw meaningful statistical conclusions. (All those included in this category are presumed innocent until proven guilty.)

The second (in this case, non-comprehensive) category, "At Large" cases, is composed of all Americans identified by the Program on Extremism as having connections to ISIS but who, for various reasons, have not been arrested. Some of these individuals are identified by name, others only by a pseudonym.

The final (also non-comprehensive) category consists of ISIS-linked individuals who have died. This group encompasses the three people killed in the U.S.; well-identified individuals who have died under various circumstances in Syria and/or Iraq; and less clearly identified persons who are allegedly American who have died fighting in Syria and/or Iraq.

Statistics on ISIS Recruits in the U.S. Legal System

Over the course of six months, our researchers reviewed more than 7,000 pages of legal documents detailing ISIS-related legal proceedings, including criminal complaints, indictments, affidavits, and courtroom transcripts. Supplemented by original research and interviews with prosecutors, reporters, and, in some select cases, families of the charged individuals, the Program developed a snapshot of the 71 individuals who have been charged for various ISIS-related activities.

Defying any cookie-cutter profile of the American ISIS supporter, these 71 individuals constitute an incredibly heterogeneous group. In fact, they come from an array of ethnic groups and a range of socio-economic and educational statuses. A deeper analysis of some of these individuals and their radicalization and/or mobilization trajectories is provided below.

To better understand this group, researchers developed nine data points, each corresponding to a distinct demographic factor or arrest characteristic.

Age

The youngest U.S. person arrested for ISIS-related activities was an unnamed 15-year-old boy. Two others were minors, ages 16 and 17 at the time of their arrests. The oldest was Tairod Pugh, a former Air Force officer who was 47 at the time of his arrest. The average age of the American ISIS supporter at the time of charges is 26.

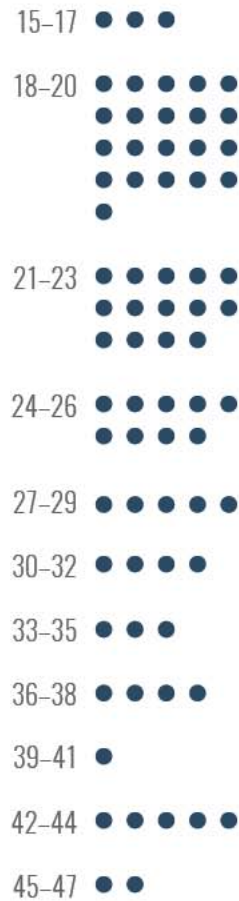
Mirroring a pattern witnessed in most Western countries, the age of those arrested in connection with ISIS is on average lower than that of individuals arrested on terrorism-related charges in the past. As U.S. Assistant Attorney General John Carlin has noted, "In over 50 percent of the cases the defendants are 25 years or younger,

FIG. 3

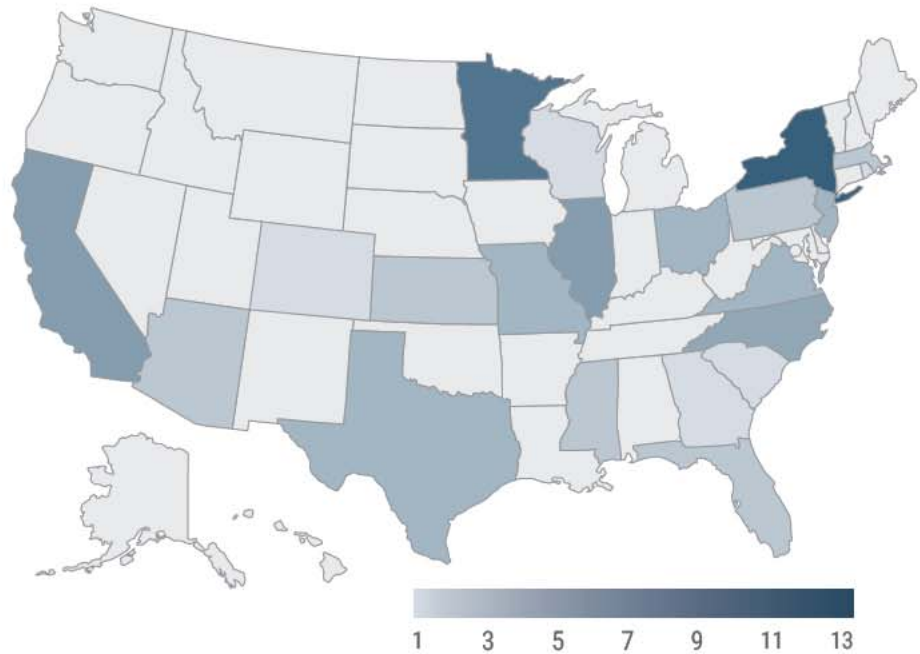
ISIS RECRUITS IN THE U.S. LEGAL SYSTEM

Age

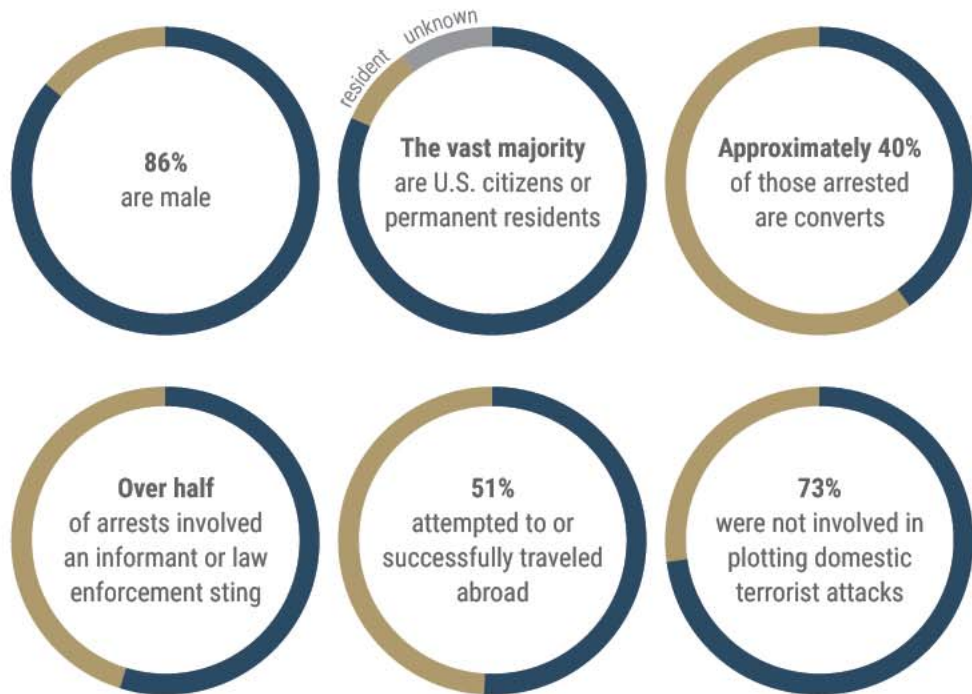
● 1 person



Numbers by State



56 individuals
were arrested in
2015, the largest
number of terrorism
arrests in a
single year since
September 2001.



and in over a third of the cases they are 21 years or younger. . . . That is different than the demographic we saw who went to support core al Qaeda in the Afghanistan FATA (Federally Administrated Tribal Areas) region.”²¹

Gender

Sixty-one of the seventy-one individuals (86%) are male. Nonetheless, women are taking an increasingly prominent role in the jihadist world. A handful of studies have attempted to identify the reasons why ISIS’s ideology attracts a growing number of Western women.²² While some of these motivations are identical to that of their male counterparts (i.e. the search for a personal identity and the desire to build a strict Islamic society), others are specific to women. The role of women in ISIS varies from propaganda disseminators and recruiters to those as the “wife of jihadist husband” and “mother to the next generation.”²³

Time Frame

The tempo of ISIS-related arrests has increased markedly in 2015. An overwhelming majority (56 individuals) were arrested for ISIS-related activities this year. This represents the largest number of terrorism arrests in a single year since September 2001.

Location

While the FBI has stated that there are active ISIS-related investigations in all 50 states, to date only 21 states have had at least one arrest within their borders. New York saw the highest number of cases (13), followed closely by Minnesota (11).

Legal Status

The vast majority of individuals charged are U.S. citizens (58) or permanent residents (6), underscoring the home-grown nature of the threat. Researchers were unable to determine the legal status of seven individuals.

Converts

Approximately 40% of those arrested are converts to Islam. Given that an estimated 23% of the American Muslim population are converts, it is evident that converts are overrepresented among American ISIS supporters.²⁴

Use of Informants/Stings

Over half (39) of the individuals were arrested after an investigation involving an informant or undercover law enforcement officer. Since 9/11, the FBI has regularly employed this tactic in terrorism investigations, with a remarkable conviction success rate. At the same time, the use of this tool has caused friction with segments of the American Muslim community.

Travel Abroad

Fifty-one percent of those charged with ISIS-related activities attempted to travel abroad or successfully departed from the U.S. In October 2015, FBI Director Comey revealed that the Bureau had noted a decline in the number of Americans seeking to travel overseas, although he did not elaborate on what elements triggered this shift.²⁵

Domestic Terror Plot

An overwhelming majority of those charged (73%) were not involved in plotting terrorist attacks in the U.S. Most U.S.-based ISIS supporters were arrested for intent to do

21. Department of Justice, “Transcript of Assistant Attorney General John P. Carlin’s Briefing at the Foreign Press Center on the Foreign Terrorist Threat and Other National Security Issues,” September 28, 2015.

22. See, for example, Saltman and Smith, “‘Till Martyrdom Do Us Part,’” ISD and ICSR, May 2015. See also Edwin Bakker and Seran de Leede, “European Female Jihadists in Syria: Exploring an Under-Researched Topic,” International Centre for Counter-Terrorism—The Hague (ICCT), April 2015.

23. Erin Marie Saltman and Melanie Smith, “‘Till Martyrdom Do Us Part’: Gender and the ISIS Phenomenon,” Institute for Strategic Dialogue (ISD) and ICSR, May 2015, p. 70.

24. Pew Research Center, “Converts to Islam,” July 21, 2007.

25. Johnson, “Comey: Feds have Roughly 900 Domestic Probes about Islamic State Operatives,” *USA Today*, October 23, 2015.

harm overseas or for providing material support—namely personnel and funds—to fighters in Syria and Iraq.

Recruits Who Remain “At-Large”

The 71 indictments are merely the tip of the iceberg, as U.S. authorities estimate that the number of individuals linked to ISIS is much larger. Our researchers identified a few dozen individuals with reported ISIS links who have not been charged. Similar to those in the legal system, the “At-Large” cohort have no common profile.

Among them, for example, are three teenage girls from the suburbs of Denver, two Somali-American sisters aged

15 and 17, and their 16-year-old friend of Sudanese descent. The trio lived a normal and comfortable life among their unsuspecting families and peers. Over a number of months, the girls engaged with ISIS supporters online, posting ISIS propaganda and expressing their desire to travel to Syria. One of their online contacts was Umm Waqqas, an influential recruiter within ISIS’s online network. The *nom de guerre* Umm Waqqas, which allegedly belongs to a woman, is one of only three accounts listed as a contact from those seeking to travel to Syria in ISIS’s 2015 guidebook *Hijrah to the Islamic State*.²⁶

One morning in October 2014 the sisters left home under the guise of going to the library while their Sudanese

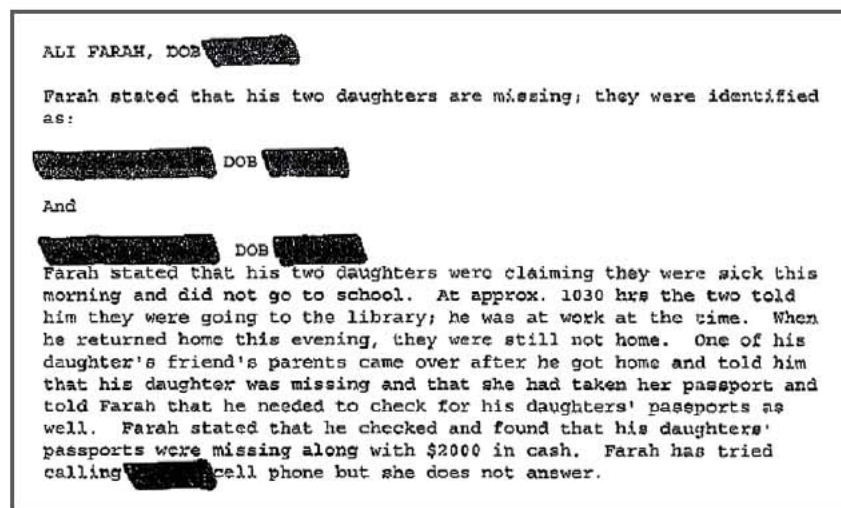


FIG. 4 Excerpt from missing persons report filed by family of the Somali-American teens



FIG. 5 Tweet posted by the 16-year-old Denver girl

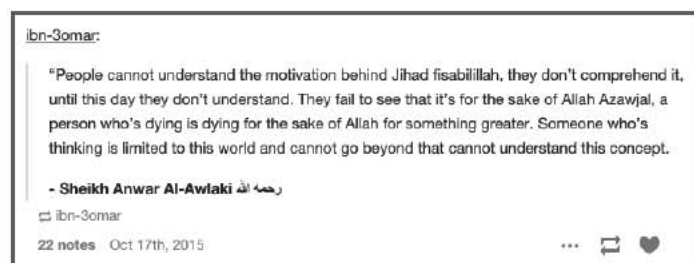


FIG. 6 Reposted by one of the Denver girls on Tumblr on the anniversary of the refined trip

26. Islamic State of Iraq and Syria (ISIS), "Hijrah to the Islamic State: What to Packup, Who to Contact, Where to Go, Stories & More," 2015.

friend boarded the bus to school. But instead of studying, the minors went to Denver International Airport, where their Syria-bound journey began. “Please make dua for us three,” the 15-year-old tweeted the morning of her departure, “It’s extremely urgent!”²⁷ Their hopes were dissipated by German authorities who—acting on a tip from the FBI that had been passed on by the sisters’ father—detained them at Frankfurt International Airport and placed them on a plane back to Denver. Upon their return, U.S. authorities released the trio to their families without charges.²⁸

The story of the Denver girls resembles that of Hoda Muthana, a young Yemeni-American woman from Hoover, Alabama.²⁹ As profiled in a *BuzzFeed* feature piece, Muthana grew up a modest, quiet girl from a conservative household.³⁰ However, at the age of 17 she began to distance herself from the local Muslim community and immersed herself in Islamic fundamentalist literature accessible online. She created an alter-ego on Twitter, gaining thousands of followers and interacting with like-minded Muslims across the world. One of them was Aqsa Mahmood, a 19-year-old from Scotland who made headlines as one of the first Western females to travel to Syria.³¹ Muthana allegedly communicated extensively with Mahmood, ultimately modeling her own departure on the example of her Scottish friend’s.³² Under the pretense of going to Atlanta for a college field trip, Muthana boarded a flight to Turkey.

Within a month of her arrival in Syria she married an Australian foreign fighter named Suhan al Rahman (a.k.a. Abu Jihad al Australi), who was later killed in an airstrike.³³ From her home in Raqqa, Muthana continues to propagate ISIS’s message online. For example, she uploaded a picture

of four Western passports with the caption, “Bonfire soon, no need for these anymore.”³⁴ On March 19, 2015—months before the Garland shooting—Muthana incited violence, tweeting: “Veterans, Patriot, Memorial etc Day parades . . . go on drive by’s + spill all of their blood or rent a big truck n drive all over them. Kill them.”³⁵

While he also planned his *bijrab* to Syria with the help of ISIS sympathizers online, 24-year-old New Yorker “Samy” (as he is referred to in legal proceedings) traveled a different path. According to his family, Samy started expressing increasingly radical religious views and became a more vocal opponent of American foreign policy in the



FIG. 7 Hoda Muthana's high school yearbook portrait



FIG. 8 Muthana on Twitter in the captioned January 2015

27. Ellie Hall, “Inside The Online World Of Three American Teens Who Allegedly Wanted To Join ISIS,” *BuzzFeed News*, October 27, 2014.

28. Jesse Paul and Bruce Finley, “Parents Reported \$2,000 Missing as Teens Headed to Join Islamic State,” *The Denver Post*, October 21, 2014.

29. Ellie Hall, “Gone Girl: An Interview With An American In ISIS,” *BuzzFeed News*, April 17, 2015. Information in the proceeding article was integrated with interviews conducted by the Program on Extremism’s staff.

30. Jon Anderson, “Hoover Woman Joins ISIS: Meet Hoda Muthana who Fled U.S. to Syria,” *AL.com*, April 20, 2015.

31. Ashley Fantz and Atika Shubert, “From Scottish Teen to ISIS Bride and Recruiter: The Aqsa Mahmood Story,” *CNN*, February 24, 2015.

32. Hall, “Gone Girl,” *BuzzFeed News*, April 17, 2015.

33. Ibid.

34. Ibid.

35. Ibid.

Middle East in 2014.³⁶ He began discussing his views online, where he engaged a fervent Muslim Brotherhood supporter from Arizona, 42-year-old Ahmed Mohammed El Gammal. Within a matter of months, El Gammal visited Samy in New York. Three months later, El Gammal allegedly facilitated the young man's journey to Syria.

Once he joined ISIS in Syria, Samy's phone and computer were temporarily confiscated to prevent contact with the outside world. During a break from his training, he reached out to his brother to apologize for his "sudden disappearance" and to reassure him that "everything is normal and safe."³⁷ After completing three weeks of intense religious training with ISIS, Samy told his brother excitedly that he would begin a month of military training, after which he would become a "regular employee [of ISIS]."³⁸ A Facebook message posted in the spring of 2015 suggests that Samy's experience with ISIS was everything he thought it would be: "I live in bilad al Islam now, the real bilad al Islam, and its [sic] beautiful."³⁹

The Deceased: Uncle Sam's Shaheed

As with the cohorts of legal cases and at-large recruits, American ISIS supporters who have been killed similarly defy a homogenous demographic profile. For clarity purposes, this cohort was organized by where the individual died.

Killed in America

Elton Simpson and **Nadir Hamid Soofi**, both residents of Phoenix, Arizona, were killed on May 4, 2015, in an attempted attack on the American Freedom Defense Initiative's Muhammad Art Exhibit and Cartoon Contest in Garland, Texas.⁴⁰ Simpson, a convert to Islam, previously served three years of probation for lying to the FBI about attempting to travel to Somalia to fight for al Shabaab.⁴¹ Before the attack, Simpson communicated online with various British and American ISIS members, who encouraged him to carry out the operation.⁴²

Usaamah Abdullah Rahim, a resident of Roslindale, Massachusetts, was shot and killed by local police officers in his hometown after charging



FIG. 9 E Gamma December 2013

26. On or about January 16, 2015, approximately eleven days before his scheduled departure from the United States, CC-1, via social media, contacted CC-2. ¹ The following exchange occurred, in substance and relevant part:		
1/16, 17:05	CC-1	As-Salamu Alaikum Ateyya my name is Samy, I'm Gammal's friend. He told me you could help me with a career opportunity in Istanbul. I'll be visiting soon to look for an internship for the summer inshaAllah. I'd really appreciate your help. Please reply whenever you get the chance. BarakAllahu feek [may Allah bless you] (emphasis added)

FIG. 10 Samy dent flies h mse f excerpt from E Gamma s cr m na comp a nt



FIG. 11 Soofi (eft) and S mpson

36. *United States of America v. Ahmed Mohammed El Gammal*, Criminal Complaint, (August 20, 2015).

37. Ibid.

38. Ibid.

39. Ibid.

40. Matt Pearce and Nigel Duara, "Texas Gunman's Mother: 'He Just had a Normal American Upbringing,'" *Los Angeles Times*, May 5, 2015.

41. Eugene Volokh, "Why Elton Simpson, One of the Texas Shooters, had Been Acquitted of an Earlier Terrorism-Related Offense," *The Washington Post*, May 4, 2015.

42. Elliott C. McLaughlin, "ISIS Jihadi Linked to Garland Attack has Long History as Hacker," *CNN*, May 7, 2015.

them with a knife.⁴³ Authorities allege that prior to the incident Rahim conspired with his nephew, David Wright, and Rhode Island resident Nicholas Rovinski, as well as additional unnamed conspirators, to assassinate individuals within the U.S. on behalf of ISIS. On the morning of June 2, 2015, Rahim changed his plans and called Wright to explain that he wanted to act imminently and target the police. Once law enforcement approached him in the parking lot of the CVS drugstore where he worked, he lunged at them with a knife and was shot and killed.⁴⁴

Killed in Syria/Iraq and Clearly Identified

Sixto Ramiro Garcia, a Houston resident, traveled to Syria in March 2014.⁴⁵ Garcia, a convert to Islam, conspired to join ISIS with fellow Houston resident Asher Abid Khan, but was left to cross the Turkey-Syria border alone after Khan returned to Texas.⁴⁶ His family was notified of his death on December 25, 2014, via a Facebook message from Garcia's account.⁴⁷ The circumstances surrounding Garcia's death remain a mystery.

Amir Farouk Ibrahim, a dual U.S.-Egyptian citizen and Pittsburgh resident, traveled to Syria in early 2013.⁴⁸ Ibrahim was reportedly killed in July 2014 in a clash with Kurdish forces. Representatives from the Syrian Observatory for Human Rights found both of his passports among the ruins of a town that had been held by ISIS.⁴⁹

Yusuf Jama, a native of Minneapolis, traveled to Syria in June 2014.⁵⁰ Prior to leaving the U.S., Jama attempted to travel to Syria in May 2014 with fellow Minneapolis

resident Guled Omar—who was later arrested and indicted on material support charges—and another individual. But the trio delayed their plans in light of pushback from Omar's family.⁵¹ Additionally, Jama lived with Mohamed Osman, whom authorities believe traveled to Somalia in July 2012 to join al Shabaab.⁵² Although the circumstances surrounding Jama's death are unknown, his family was notified of his death in December 2014.⁵³

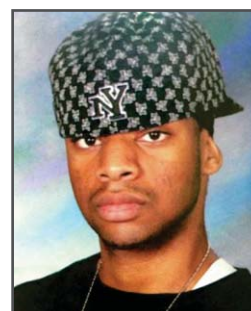


FIG. 12 Usaamah
Abdu ah Rah m



FIG. 13 Amir Farouk Ibrahim's American passport

43. *United States of America v. David Wright and Nicholas Rovinski*, Criminal Complaint, (June 12, 2015). See also Susan Zalkind and Katie Zavadski, "Boston's Wannabe Beheader 'Liked' ISIS Enough to Kill," *The Daily Beast*, June 3, 2015.

44. Ibid.

45. *United States of America v. Asher Abid Khan*, Arraignment/Detention Hearing, (June 1, 2015).

46. Ibid.

47. Ibid.

48. Betsy Hiel and Carl Prine, "Pittsburgh Man Reportedly Dead in Syria," *WPXI.com*, July 26, 2013.

49. Bill Roggio, "American Passport Found at al Qaeda Base in Northern Syria," *The Long War Journal*, July 23, 2013.

50. Laura Yuen, Mukhtar Ibrahim and Sasha Aslanian, "Called to Fight: Minnesota's ISIS Recruits," *Minnesota Public Radio (MPR) News*, March 25, 2015.

51. Ibid.

52. Yuen, Ibrahim and Aslanian, "Called to Fight," *MPR News*, March 25, 2015.

53. Ibid.

Douglas McCain, a convert to Islam raised between Chicago and Minneapolis, left the U.S. for Syria, via Turkey, in or around April 2014.⁵⁴ McCain, whose body was identified by the passport in his pocket, was reportedly killed in August 2014 during a clash between ISIS and the Free Syrian Army in the Aleppo countryside.⁵⁵

Abdirahmaan Muhumed, a dual U.S.-Somali citizen from Minneapolis, traveled to Syria in or around January 2014.⁵⁶ Muhumed's friends and family learned of his presence in Syria when he uploaded a photo of himself with a Quran and a rifle captioned "Sham."⁵⁷ Muhumed was allegedly killed in August 2014 in the same Aleppo-area

clash as McCain, whom he knew from the U.S.⁵⁸

Hanad Abdullahi Mohallim, a native of Apple Valley, Minnesota, was 18 years old when he left the U.S. for Syria on March 9, 2014.⁵⁹ Reports suggest that Mohallim was killed in action in January 2015.⁶⁰

Abdullah Ramo Pazara, a St. Louis resident of Bosnian origin, left the U.S. for Syria in May 2013, shortly after becoming a naturalized U.S. citizen.⁶¹ While in Syria, he allegedly rose to the rank of deputy to top ISIS commander Omar al Shishani and led a brigade of fighters of Balkan origin.⁶² Pazara was reportedly killed in action in the fall of 2014 near Kobane.⁶³



FIG. 14 Douglas McCain as performing rapper turned jihadist

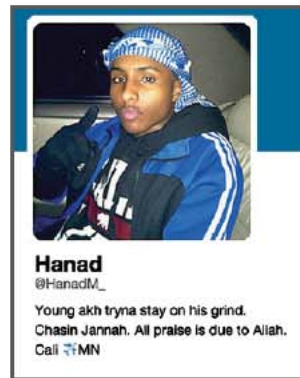


FIG. 15 Hanad Abdullahi Mohallim's Twitter profile



FIG. 16 Abdullah Ramo Pazara (right) in Syria

54. Cassandra Vinograd and Ammar Cheikh Omar, "American Douglas McArthur McCain Dies Fighting for ISIS in Syria," *NBC News*, August 26, 2014.

55. Ibid.

56. Mukhtar Ibrahim, "Jihad in Syria Lures Somalis from Minnesota," *MPR News*, June 12, 2014.

57. Ibid.

58. Michael Walsh, "ISIS Terrorist from Minnesota Worked at Major American Airport: Report," *New York Daily News*, September 3, 2014. See also Mukhtar Ibrahim and Peter Cox, "Douglas McArthur McCain, A Man with Minnesota Ties, Killed in Syria," *MPR News*, August 7, 2014.

59. Laura Yuen, Mukhtar Ibrahim and Sasha Aslanian, "From MN Suburbs, They Set out to Join ISIS," *MPR News*, March 25, 2015.

60. Andrea Huncar, "3 ISIS Recruits from Edmonton Believed Killed," *Canadian Broadcasting Corporation (CBC) News*, January 16, 2015.

61. *United States of America v. Hodzic, et al.*, Indictment, (February 5, 2015).

62. Robert Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St. Louis Today.com*, April 11, 2015. See also Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.

63. SAFF, "U Siriji Poginuo I Ramo Pazara iz Teslića," September 24, 2014.; Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.; *Slobodna Bosna*, "Ramo Abdullah Pazara: Sprski Ratnik i Islamski Fanatik," February 19, 2015.

Killed in Syria/Iraq and Not Clearly Identified

The Program on Extremism uncovered videos and information on individuals identified as Americans in ISIS propaganda who reportedly died either fighting or as suicide bombers. It was not possible to ascertain the real identity of these individuals, nor were researchers able to verify the authenticity of the information provided by ISIS. Yet some appear to have intriguing stories, having allegedly occupied important positions within ISIS or having carried out suicide attacks.

One of these individuals is a man who identified himself with the *kunya* **Abu Muhammad al Amriki** (Abu Muhammad the American) and claimed to have lived in the U.S. for “ten or eleven years” prior to leaving with his family to join Jabhat al Nusra (JN) in Syria (before changing his allegiance to ISIS). Featured in a nine minute video titled *Revealing the Treachery of Jabhat al Nusra* posted on numerous video sharing sites, Abu Muhammad al Amriki recounted how he left the al Qaeda–linked group because he believed it was working with the Free Syrian Army, as it allowed a convoy of arms bound for the outwardly secular and tacitly Western-supported rebel group to enter Syria.⁶⁴ Speaking in English in front of the black ISIS flag, the man recalled how the incident led him to switch his allegiance to ISIS, with which he became a local emir in an area near the border with Turkey. Though details are sparse, in early 2015 news of his death began circulating on ISIS-linked websites.⁶⁵

Another American to have reportedly died in Syria is **Abu Khalid al Amriki**. A known personality in the ISIS English-language social media scene, Abu Khalid al Amriki used at least five distinct Twitter accounts to spread his views. The little that is known about his offline persona comes from an interview he gave to an Australian paper, in which he revealed that his wife, whom he left behind in the U.S., was arrested on terrorism charges shortly after



FIG. 17 Abu Muhammad al Amriki explains his defection to ISIS



FIG. 18 One of Abu Khalid al Amriki's final tweets



FIG. 19 News of Abu Khalid al Amriki's death circulates on Twitter

64. YouTube, “Revealing the Treachery of Jabhat al Nusra,” February 10, 2014.

65. Alastair Jamieson, “Alleged American ISIS Commander Abu Muhammad Al-Amriki Killed: Reports,” *NBC News*, January 28, 2015.

his departure.⁶⁶ In late April 2015, Abu Khalid appeared in a video produced by one of ISIS's official media outlets, Al Hayat Media Center. Abu Khalid is dressed in camouflage and a bandana and holding an AK-47 rifle while standing next to Neil Prakash (a.k.a. Abu Khalid al Cambodi), a prominent Australian foreign fighter and ISIS propagandist.⁶⁷ Reports of Abu Khalid's death at the hands of a coalition airstrike surfaced on social media in late September 2015. In an ironic twist of fate, one of his last tweets using the Twitter handle @AK47_Backup stated, "You fly a remote control plane halfway across the world to kill an enemy that you are to [sic] coward to meet face to face."

Two unidentified individuals who used *kunyas* ending in "al Amriki" were heralded as ISIS suicide attackers by the group in 2015. One, **Abu Dawoud al Amriki**, reportedly rammed a truck packed with explosives into a gathering of soldiers in Iraq's Salahuddin province.⁶⁸ ISIS posted an image of Abu Dawoud on the Twitter page of one of its official media outlets, Al Bayan Radio, in March.⁶⁹ The other, **Abu Abdullah al Amriki**, allegedly drove an SUV laden with explosives into Iraqi army barracks near Beiji in August 2015.⁷⁰



FIG. 20 Abu Abdulah al Amriki



FIG. 21 ISIS announces Abu Abdulah al Amriki's death

66. Lauren Williams, "Meeting a Daesh jihadist in Syria," *The Saturday Paper*, July 18, 2015. Our research team attempted to identify Abu Khalid's alleged American wife but was unsuccessful. According to court records, he did at some point communicate with Keonna Thomas, an American arrested in the U.S., but there is no indication that their relationship was anything more than an online friendship.

67. Aaron Y. Zelin, "al-Hayāta Media Center Presents a New Video Message from The Islamic State: 'Stories From the Land of the Living: Abū Khālid al-Kambūdī,'" *Jihadology.net*, April 21 2015.

68. Assabah.com, "American Suicide Bomber Abu Dawoud in the Ranks of 'Daesh: The Iraqi Army Takes on the Battle to Retake Tikrit," March 4, 2015.

69. Ibid.

70. "ISIS says American suicide bomber carried out Iraq attack," *Al Arabiya*, August 19, 2015.

CHAPTER 2

From Keyboard Warriors to Battlefield Commanders: Understanding the Spectrum of ISIS in America

AS THE DATA AND ANALYSIS provided in the previous section show, the profiles of American ISIS sympathizers—from those who merely tout the group’s ideology online to those intimately involved in ISIS recruitment, financing, or fighting—are extremely diverse. Ranging from grown men who had flirted with jihadist militancy for over a decade to teenagers who have only recently converted to Islam, from the son of a Boston area police officer to a single mother of two young children, these individuals differ widely in race, age, social class, education, and family background.

Individuals with such diverse backgrounds are unlikely to be motivated by the same factors. Policymakers and academics around the world have formulated a number of explanatory theories about the underlying factors driving people to radicalize. Some focus on structural factors such as political tensions and cultural cleavages, the so-called “root causes” of radicalization. Others stress personal factors such as the shock of a life-changing event. Matt Venhaus captures the diversity of the individuals attracted to jihadist ideology, categorizing them as revenge seekers, status seekers, identity seekers, and thrill seekers.⁷¹ But it is clear that these categories are not exhaustive and that, in many cases, an individual exhibits the characteristics of more than one category. In substance, most experts agree that radicalization is a highly complex and individualized process, often shaped by a poorly understood interaction of structural and personal factors.

In many cases examined by our research team, an underlying sense of sympathy and compassion appeared to play an important role in initially motivating young Americans to become interested and invested in the Syrian conflict. Many were outraged by the appalling violence Bashar al Assad’s regime used to suppress the Syrian rebellion and the subsequent inaction on the part of the international community. Pictures and videos capturing the aftermath of civilian massacres perpetrated by the regime, displayed widely in both social and mainstream media, rocked the consciences of many—from those with an existing strong Sunni identity to those who were not Muslim—and led some to take the first steps to militancy.

A major shift began as the anti-regime rebellion in Syria came to be increasingly dominated by militant groups. By the time ISIS formally declared its caliphate in June 2014, the motivations of recruits appeared to revolve more around fulfilling perceived religious obligations, such as performing *hijrah* (migration from a non-Muslim society to a Muslim one, as per the prophet Mohammad’s migration from Mecca to Medina) and the opportunity to participate in the creation of a utopian Islamic society.

But ideological motivations are deeply intertwined with, and impossible to separate from, personal motives. The National Counterterrorism Center (NCTC) observes that those who embrace ISIS’s ideology tend to be “disenfranchised individuals seeking ideological, religious

71. Colonel John M. “Matt” Venhaus, U.S. Army, “Why Youth Join al-Qaeda,” *United States Institute of Peace*, May 2010.



FIG. 22 Moner Abu Salha aka Abu Hurayra aka Amerik

and personal fulfillment.”⁷² A search for belonging, meaning, and/or identity appears to be a crucial motivator for many Americans (and other Westerners) who embrace ISIS’s ideology.

This search for meaning was perfectly encapsulated in the words of Moner Abu Salha, the 22-year-old Floridian who is the first American known to have died in a suicide mission in Syria on behalf of Jabhat al Nusra. “I lived in America,” stated Abu Salha in a 2014 video. “I know how it is. You have all the fancy amusement parks and the restaurants and the food and all this crap and the cars. You think you’re happy. You’re not happy. You’re never happy. I was never happy. I was always sad and depressed. Life sucked.”⁷³ In contrast, he described life fighting in Syria as “the best I’ve ever lived.”⁷⁴

Despite coming from a quite different background, a fellow American who made the journey to Syria has reportedly displayed a similar malaise. Ariel Bradley was born in an underprivileged family in the Chattanooga suburb of Hixson (the same suburb where the perpetrator of the July 2015 Chattanooga shooting Mohammad Abdulazez lived). Bradley was homeschooled by her evangelical

Christian mother until she rebelled and left home as a teenager. According to friends interviewed for her extensive profile in *BuzzFeed News*, Bradley spent the following years wandering in search of something.⁷⁵

“She was definitely always looking for love,” said a former roommate “always looking for that sense of belonging.” Another friend recalled Bradley’s “clearly segmented life”: “When I first met her she was a Christian, and then she was a socialist, and then she was an atheist, and then a Muslim. As far as I could tell it was always in relation to whatever guy she was interested in, so if she meets a guy that’s an atheist then she’s an atheist, falls into that for a year. Then the guy leaves and she meets somebody new, and it starts all over again. . . . It seemed like whatever guy she was with, she would just crawl into his skin and kind of become him.”⁷⁶

At one point Bradley fell in love with a Muslim patron of the pizza parlor where she used to work. To get close to him, she converted to Islam. While things never worked out with the original love interest, Bradley began frequenting Muslim marriage websites where, in August 2011, she met an Iraqi man living in Sweden. Shortly thereafter the two married and had a child. Likely under the influence of her husband, Bradley’s faith became increasingly conservative and militant. In early 2014 the couple left for Syria, where they have reportedly been living in ISIS-controlled territory. Bradley is active online, particularly on Twitter and

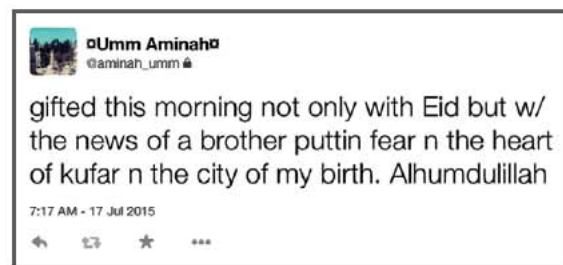


FIG. 23 Ariel Bradley celebrates the Chattanooga shootings

72. Testimony of Nicholas J. Rasmussen, Director, National Counterterrorism Center, *Countering Violent Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror*, House Homeland Security Committee, February 11, 2015.

73. Mona El-Naggar and Quynhanh Do, “Video Released of U.S. Bomber in Syria,” *New York Times*, July 31, 2014.

74. Ibid.

75. Ellie Hall, “How One Young Woman Went From Fundamentalist Christian to ISIS Bride,” *BuzzFeed News*, July 20, 2015.

76. Ibid.

Instagram, where she discusses her life and praises ISIS. In the immediate aftermath of the Chattanooga attacks, which killed five military personnel in her hometown, she tweeted: “*in sha Allah* [God willing] this will make the camps of *Emaan* [believers] and *Kuffr* [non-believers] known within Chattanooga.”⁷⁷

It is tempting to caricature Bradley as a naïve girl with personal problems whose jihadist trajectory is the outcome of an unfortunate childhood. It is also easy to assume that her actions were driven by a quest for a romantic partner. But, even in the most extreme cases, multiple factors contribute to an individual’s decision. Her friend’s analysis highlights this dynamic: “Be it religion, be it a man, be it a marriage, be it a child, be it ISIS, Ariel was always looking for something to define herself, an identity to cling to.”⁷⁸ Given her particular pattern of behavior, it is likely that Bradley might have accepted other extremist ideologies, if circumstances allowed, so long as they satiated her hunger for community, love, and identity.

Still, it is difficult to fully comprehend the complex mental processes that led Bradley, like other young Americans, to embark on such an extreme journey to the ISIS caliphate. What is apparent is that ISIS and its propaganda machine have been particularly adept at exploiting the emotions, needs, and weaknesses of young Americans, irrespective of their demographic backgrounds. What follows is an examination of the online and physical world dynamics that influence U.S.-based ISIS sympathizers.

The Role of Social Media

Extremist groups inspired by a range of ideologies have embraced the Internet for a variety of purposes. As a 2009 report by the International Centre for the Study of Radicalisation at King’s College London observes:

The Internet can be used by extremists to illustrate and reinforce ideological messages and/or narratives. Through the Internet, potential recruits can

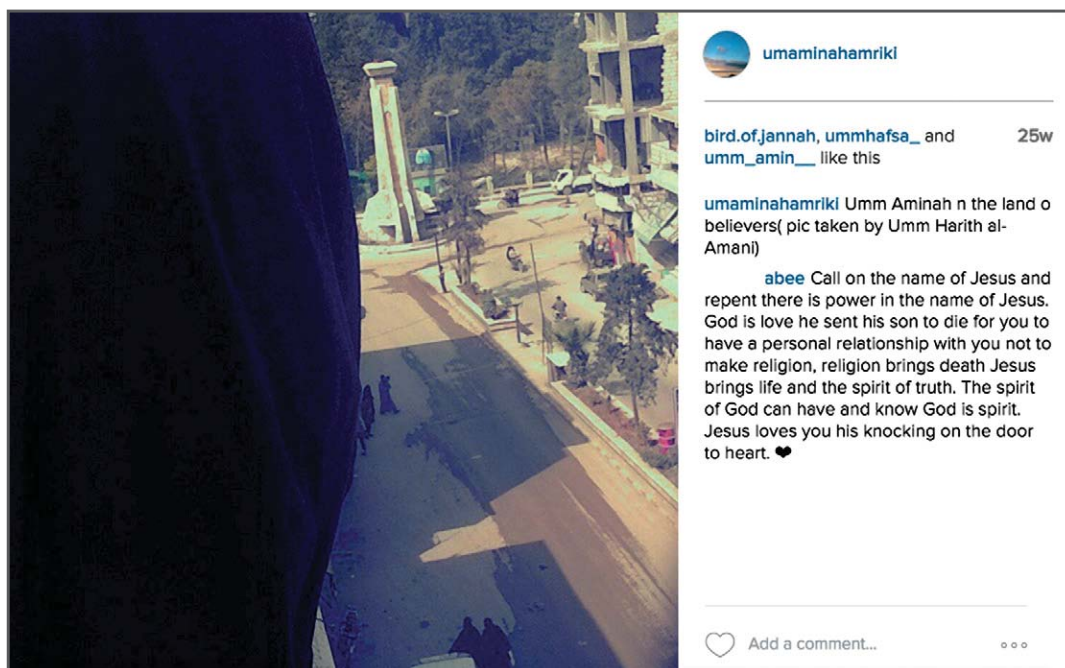


FIG. 24 Snapshot of life in the caliphate image from Ariel Bradley's Instagram account

77. Hall, “How One Young Woman Went From Fundamentalist Christian to ISIS Bride,” *BuzzFeed News*, July 20, 2015.

78. Ibid.

gain near-instantaneous access to visually powerful video and imagery which appear to substantiate the extremists' political claims. . . . The Internet makes it easier to join and integrate into more formal organizations. It provides a comparatively risk-free way for potential recruits to find like-minded individuals and network amongst them, enabling them to reach beyond an isolated core group of conspirators. . . . It creates a new social environment in which otherwise unacceptable views and behaviour are normalised. Surrounded by other radicals, the Internet becomes a virtual 'echo chamber' in which the most extreme ideas and suggestions receive the most encouragement and support.⁷⁹

Western governments tend to agree on the importance of the Internet in radicalization processes. The dynamic has been described with clarity by the Netherlands' domestic intelligence agency (AIVD) in an extensive report that calls the Internet "the turbocharger of the jihadi movement." The report argues:

There is a large group of Muslims, mostly young people, in non-Muslim Western countries, who feel isolated within the societies in which they live. Because these youngsters see their future in the West, unlike their parents, while at the same time experiencing a strong element of distrust for Western society, they are looking for their own identity and for a position to adopt in Western society. . . . When hunting for answers to these questions, they may end up in an environment with which they are familiar and which is easily accessible, namely the Internet. Not only can they find a great deal of information there, but

they can also become part of a virtual (Muslim) community, exchanging ideas and blowing off steam by expressing their frustration with other like-minded individuals who share their fate.⁸⁰

Officials in the U.S. have expressed similar concerns. The 2007 National Intelligence Estimate, titled *The Terrorist Threat to the US Homeland*, observes:

The spread of radical—especially Salafi—Internet sites, increasingly aggressive anti-U.S. rhetoric and actions, and the growing number of radical, self-generating cells in Western countries indicate that the radical and violent segment of the West's Muslim population is expanding, including in the United States. The arrest and prosecution by law enforcement of a small number of violent Islamic extremists inside the U.S.—who are becoming more connected ideologically, virtually, and/or in a physical sense to the global extremist movement—points to the possibility that others may become sufficiently radicalized that they will view the use of violence here as legitimate.⁸¹

In May 2008, the U.S. Senate Committee on Homeland Security and Governmental Affairs published a report titled *Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat* in which the committee warns about the increased frequency with which U.S.-based militants are active online.⁸² A 2010 report by NCTC contends that "the Internet and related information technologies—such as Web forums, blogs, social networking sites, and e-mail—that serve as platforms for extremist propaganda and discourse can enable and advance the radicalization process and help mobilize

79. Tim Stevens and Peter R. Neumann, "Countering Online Radicalisation: A Strategy for Action," ICSR, March 16, 2009, p. 12.

80. Netherlands' Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministry of International Affairs and Kingdom Relations), "Jihadis and the Internet," Netherlands' National Coordinator for Counterterrorism, February 2007, p. 91.

81. United States Office of the Director of National Intelligence, National Intelligence Council, "The Terrorist Threat to the US Homeland," *National Intelligence Estimate*, July 2007.

82. U.S. Senate Committee on Homeland Security and Governmental Affairs (HSGAC), "Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat," May 8, 2008.

individuals who may not be geographically near key extremist figures or significant events.”⁸³

U.S. officials have repeatedly highlighted how ISIS uses social media to reach a significantly wider audience much faster than any group in the past. “ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds,” argued FBI Director Comey in a July 2015 testimony before the U.S. Senate. “No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.”⁸⁴ He continued, “Social media has allowed groups, such as ISIL, to use the Internet to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.”⁸⁵ Comey further elaborated on the novelty of ISIS social media use:

Your grandfather’s al Qaeda, if you wanted to get propaganda, you had to go find it. Find where *Inspire* magazine was and read it. If you want to talk to a terrorist, you had to send an email into *Inspire* magazine and hope that Anwar al Awlaki would email you back. Now all that’s in your pocket. All that propaganda is in your pocket, and the terrorist is in your pocket. You can have direct communication with a terrorist in Syria all day and night, and so the effect of that—especially on troubled minds and kids—it works! It’s buzz,

buzz, buzz, buzz, buzz. It’s the constant feed, the constant touching, so it’s very, very different and much more effective at radicalizing than your grandfather’s al Qaeda model.⁸⁶

Indeed, ISIS’s ability to directly and constantly reach Americans through social media has manifested itself in a number of ways: 1) triggering or advancing their radicalization process; 2) helping them mobilize to leave for Syria to join the group; and 3) inciting them to carry out attacks in America. The following examples illustrate this three-fold manifestation.

Grooming from Afar

An archetypal case of ISIS’s online radicalization and recruitment campaign was chronicled in an illuminating *New York Times* story on “Alex,” a 23-year-old girl from rural Washington state.⁸⁷ Alex lived with her grandparents from an early age, after her mother lost custody due to drug addiction. A college dropout who, in her own words, lived “in the middle of nowhere” and had no connection to Islam, Alex was motivated by a “horrificed curiosity” to seek out ISIS supporters after reading news of the execution of American journalist James Foley.⁸⁸

Within several months, she was exchanging messages and conversing over Skype with various ISIS-linked recruiters.⁸⁹ Over time, Alex, who had previously expressed a desire to “live a faith more fully,” was meticulously groomed online, her new friends showering her with money, books, gift cards, and chocolate. She soon converted to Islam and slowly embraced ISIS’s ideology. Her new friends offered Alex a previously lacking sense of

83. Similar findings were reached in this report. See also National Counterterrorism Center, “Radicalization Dynamics: A Primer,” September 2010, p. 18; HSGAC, “Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism,” February 16, 2012.

84. Testimony of James B. Comey, Director, Federal Bureau of Investigation (FBI), Senate Select Committee on Intelligence, *Counterterrorism, Counterintelligence, and the Challenges of “Going Dark,”* July 8, 2015.

85. Ibid.

86. Ryan J. Reilly, “If You’re Trying To Join ISIS Through Twitter, The FBI Probably Knows About It,” *Huffington Post*, July 9, 2015.

87. Rukmini Callimachi, “ISIS and the Lonely Young American,” *NYT*, July 27, 2015.

88. Ibid.

89. Ibid.



FIG. 25 Mohammed Hamzah Khan on Twitter

belonging: hours after declaring her conversion online, the number of individuals following her on Twitter doubled, prompting her to tweet, “I actually have brothers and sisters. I am crying.”⁹⁰ Alex began to live what the *Times* categorizes as a double life. In public, she continued teaching Sunday school classes at her grandparents’ church. But, behind closed doors, she was a full-fledged believer in ISIS’s ideology.

An ISIS supporter from the U.K.—who turned out to be a married middle-aged father with a criminal record of multiple arrests—spent hours each day grooming Alex. He eventually told her that it is a sin for Muslims to live among non-believers, and extended an invitation for her to travel to Austria, marry a 45-year-old ISIS supporter, and then move to Syria.

Realizing that Alex was spending an inordinate amount of time on her computer, her grandmother confiscated her electronics and confronted her online contacts via Skype. With her double life exposed, Alex promised to stop communications with ISIS sympathizers and allowed her grandmother

to change her Twitter and email passwords. But the companionship her like-minded friends provided was apparently too good to give up. The *Times* claims that, despite her promise, Alex has continued to be active in the online ISIS scene.⁹¹

Travel Agents

In addition to helping radicalize individuals, online ISIS supporters have been instrumental in providing both advice and logistical support to Americans attempting to travel to Syria. This dynamic played out in October 2014 when three siblings from Chicago were stopped at O’Hare International Airport on their way to Syria.

The journey had been meticulously planned by the eldest sibling, 19-year-old engineering student Mohammed Hamzah Khan. Khan, a graduate of an Islamic school in the Chicago suburbs, had been active online and met a man known as Abu Qaqa on Twitter, whom he soon communicated with using personal messaging platforms such as Kik and WhatsApp.⁹² According to authorities, it was Abu Qaqa who provided Khan with the phone number of an individual to call upon landing in Turkey. Khan’s 17-year-old sister had also been active online, trying to find ways to travel to Syria. Using the Twitter name “Umm Bara,” she communicated with an English-speaking ISIS fighter who went by the name Abu Hud—known on Twitter as the “Paladin of Jihad”—and popular as result of his Tumblr series #DustyFeet, a de facto travel guide for would-be recruits.⁹³ A search of the siblings’ home found a step-by-step guide to crossing the Turkish border, contact information for four individuals involved in smuggling ISIS volunteers, including Abu Qaqa, and handwritten farewell letters addressed to their parents.⁹⁴

Another aspect of the Khans’ story is noteworthy. While “Alex” and many other ISIS sympathizers are individuals with limited or no knowledge of Islam, the Khan siblings grew up steeped in religious studies. All three attended

90. Rukmini Callimachi, “ISIS and the Lonely Young American,” *NYT*, July 27, 2015.

91. Ibid.

92. Janet Reitman, “The Children of ISIS,” *The Rolling Stone*, March 25, 2015.

93. Ibid.

94. *United States of America v. Mohammed Hamzah Khan*, Criminal Complaint (October 6, 2014).

Islamic schools and had become *hafiz* or *hafiza*, a term given to those who have memorized the entire Quran.⁹⁵ The eldest even taught youth at a local mosque.⁹⁶

Devil on the Shoulder

While the case dynamics remain somewhat murky, ISIS social media appears to have played a role in pushing Americans Elton Simpson and Nadir Soofi to attack the Muhammad Art Exhibit and Cartoon Contest in Garland, Texas. A few months before the attack Simpson, who had been involved in jihadist activities for over a decade, became an active participant in the community of U.S.-based ISIS sympathizers on social media. Simpson also made contact with a well-known British foreign fighter, Abu Hussain al Britani, and Mohamed Abdullahi Hassan (a.k.a. Mujahid Miski), a prominent Somali-American English-speaking propagandist.⁹⁷ Ten days before the attack, Miski posted about the Garland event with a clear exhortation: “The brothers from the Charlie Hebdo attack did their part. It’s time for the brothers in the #US to do their part.”⁹⁸

Simpson, via a Twitter account with the username “Shariah is Light” and an avatar of the late al Qaeda propagandist Anwar al Awlaki, responded to Miski’s call to arms, publicly asking his friend in Somalia to “dm” (Direct Message, a private message on Twitter) him.⁹⁹ Simpson and Soofi then drove from Arizona to Garland in a vehicle loaded with assault rifles, body armor, and hundreds of rounds of ammunition. Prior to the attack, Simpson tweeted a final time, using a hashtag #texasattack. The hashtag was quickly picked up by Abu Hussain al Britani and circulated throughout the

pro-ISIS community on Twitter in an effort to encourage others to commit similar acts.¹⁰⁰

The Echo Chamber

U.S. authorities estimate that several thousand Americans consume ISIS propaganda online creating what has been described as a “radicalization echo chamber.”¹⁰¹ American ISIS activists and sympathizers are active on a variety of platforms, from open forums like Facebook, Google+, and Tumblr to more discrete messaging applications such as Kik, Telegram, surespot, and the dark web. But Twitter is by far the platform of choice of this informal echo chamber. For this reason, our researchers focused on the Twitter activities of approximately 300 individuals identified as American supporters of ISIS.

Identifying the 300 individuals was challenging because most online ISIS sympathizers seek anonymity. Individuals were coded as Americans if they self-identified as such; if Twitter’s geo-location software placed them within the U.S.; or if they used a variation of the *kunya* “al

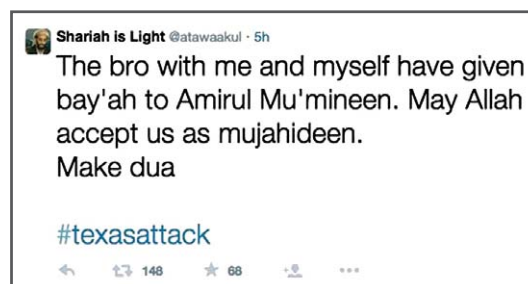


FIG. 26 Elton Simpson pledges allegiance to ISIS before his attack

95. Kevin Sullivan, “Three American Teens, Recruited Online, Are Caught Trying to Join the Islamic State,” *The Washington Post*, December 8, 2014.

96. Jethro Mullens and Ted Rowland, “Who is Mohammed Hamzah Khan?,” *CNN*, October 7, 2014.

97. Scott Shane, “Texas Attacker Left Trail of Extremist Ideas on Twitter,” *NYT*, May 5, 2015.

98. Jim Sciutto, Pamela Brown, Paul Cruickshank and Paul Murphy, Texas attacker tweeted with overseas terrorists, *CNN*, May 5, 2015.

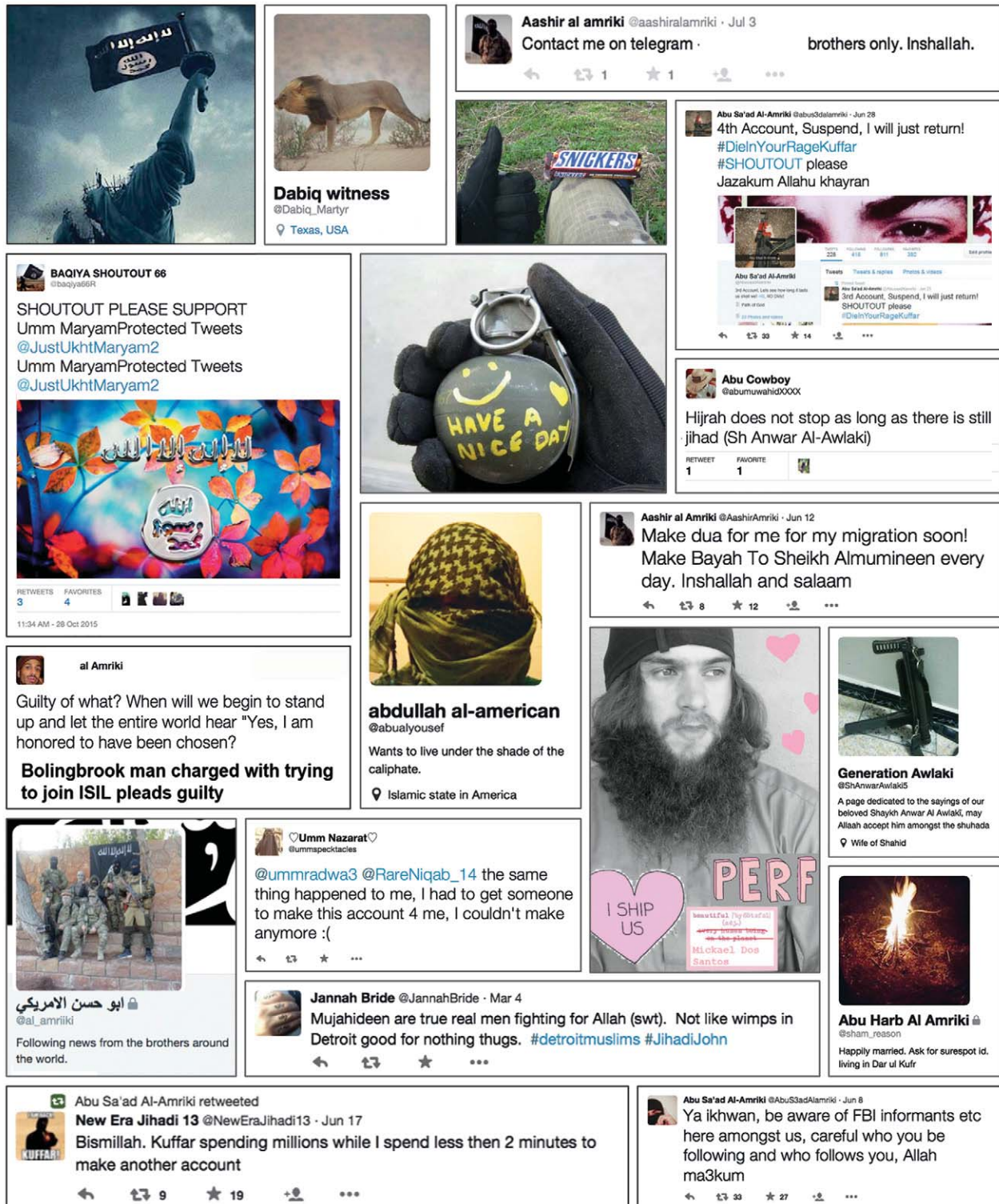
99. Rita Katz, “The Power of a Tweet: Elton Simpson and the #TexasAttack,” *SITE Intelligence Group (SITE)*, May 5, 2015.

100. Katz, “The Power of a Tweet” *SITE*, May 5, 2015.

101. Pierre Thomas, Mike Levine, Jack Date and Jack Cloherty, “ISIS: Potentially ‘Thousands’ of Online Followers Inside US Homeland, FBI Chief Warns,” *ABC News*, May 7, 2015. The term has also been used by Assistant Attorney General John Carlin: United States Department of Justice, “Assistant Attorney General John P. Carlin Delivers Remarks on Domestic Terrorism at an Event Co-Sponsored by the Southern Poverty Law Center and the George Washington University Center for Cyber and Homeland Security’s Program on Extremism,” October 14, 2015.

FIG. 27

THE RADICALIZATION ECHO CHAMBER



Amriki” in their Twitter username or handle. Additionally, researchers analyzed the content of English-speaking ISIS sympathizers for syntax, spelling, word selection, and cultural context and cross-referenced lists of followers to isolate Americans from the much larger English-speaking ISIS community on Twitter. The categorization of an account as belonging to an American was reaffirmed on a few occasions, most frequently when an individual’s criminal complaint and/or indictment made reference to social media accounts. In at least one case—that of Terrence McNeil—a technical mistake by an ISIS supporter on social media revealed their identity as an American.¹⁰²

While American ISIS supporters tend to be male, nearly one third of the accounts examined are purportedly operated by women. Additionally, supporters broadly divided into two sets: those who locate themselves in Syria and Iraq and those still in America but aspiring to assist ISIS in a number of ways. Those in the former group often maintain their network of friends in the U.S. after arriving in ISIS territory. They post near real-time updates of ISIS-led attacks and life in the caliphate, encouraging their fellow Americans to make the trek and, at times, scolding their real-world and online friends for their lack of commitment to the cause.

A significant number of American ISIS supporters use avatars of black flags, lions, and green birds.¹⁰³ A particularly clever account uses a picture of the Detroit Lions, combining a distinctly American pride in an NFL team and the popular Islamic symbol of bravery very frequently used by ISIS supporters. Images, quotes, and links to lectures of the deceased radical cleric Anwar al Awlaki are favorites of the American ISIS scene. Increasingly photos of other Americans who have been arrested on terrorism charges, killed waging *jihad* abroad, or were responsible for homegrown terrorist attacks are used as avatars.

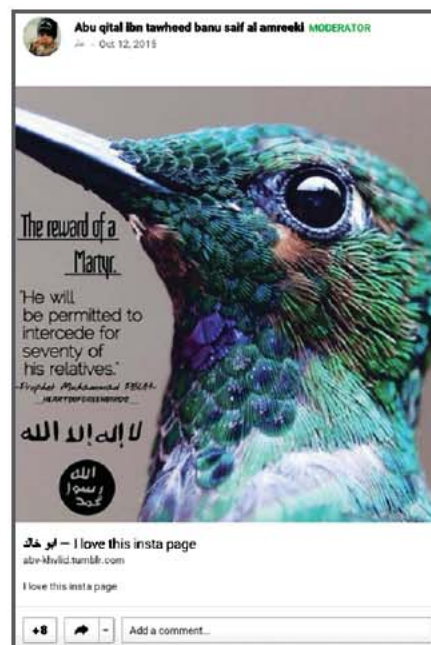
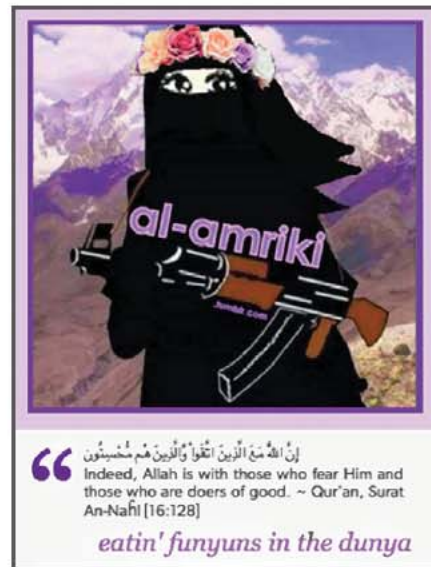


FIG. 28 Examples of ISIS supporters' imagery on social media

102. McNeil tweeted a screenshot of his Twitter suspension (at the time, his 14th suspension). He neglected to remove a small part of his Google ID, which led to a number of Google+ pages. After reviewing the videos on each page, a link was found to a video posted on YouTube, which was subsequently linked to a Facebook profile with his real name and location. One of his Facebook status updates from last year matched with materials from his 10th Twitter account prior to suspension.

103. The term “green bird” indicates a status one reaches when he or she dies (becomes a *shaheed*, or martyr) and reaches *jannah*, or heaven. It is a scriptural reference from a *hadith*, or reported saying from the prophet Mohammad, that celebrates the virtues of martyrdom. Jihadists term fallen comrades “green birds” to eulogize them as pious, faithful Muslims.

As with many online communities, participants in the American ISIS Twitter scene exhibit distinct styles, roles, personalities, and degrees of commitment, which often fluctuate over time. Reflecting these dynamics, their accounts can be divided into three categories: nodes, amplifiers, and shout-outs.

The **nodes** are the leading voices that enjoy a prominent status within the larger community and are the primary content creators for the network. A group of two or three clustered users will often swap comedic memes, news articles, and official ISIS tweets, allowing them to pool followers and more easily spread content both to new audiences and throughout their network.

Amplifiers largely do not generate new content but rather retweet and “favorite” material from popular users. Ultimately, because they post little, if any, original content, it is often unclear whether these accounts correspond to real-life ISIS sympathizers or are programmed to post automatically.

Finally, **shout-out** accounts are a unique innovation and vital to the survival of the ISIS online scene. They

primarily introduce new, pro-ISIS accounts to the community and promote newly created accounts of previously suspended users, allowing them to quickly regain their pre-suspension status. Although they tweet little substantive content, shout-out accounts tend to have the largest followings in the Twitter landscape and therefore play a pivotal role in the resilience of ISIS’s Twitter community.

While American ISIS accounts are suspended with some frequency, these suspensions have become a badge of honor and a means by which an aspirant can bolster his or her legitimacy. In most suspension cases, a new (and often more than one) account with a variation of the previous username is created within hours. As American ISIS supporters are continuously suspended from Twitter, creating a new account becomes increasingly difficult, leading some to turn to others for assistance. The user’s first tweet is often an image of the Twitter notification of suspension, proving that they are the owner of the previous account, along with a request for shout-outs. The new accounts are then retweeted by others, allowing the user to regain his or her previous online following.

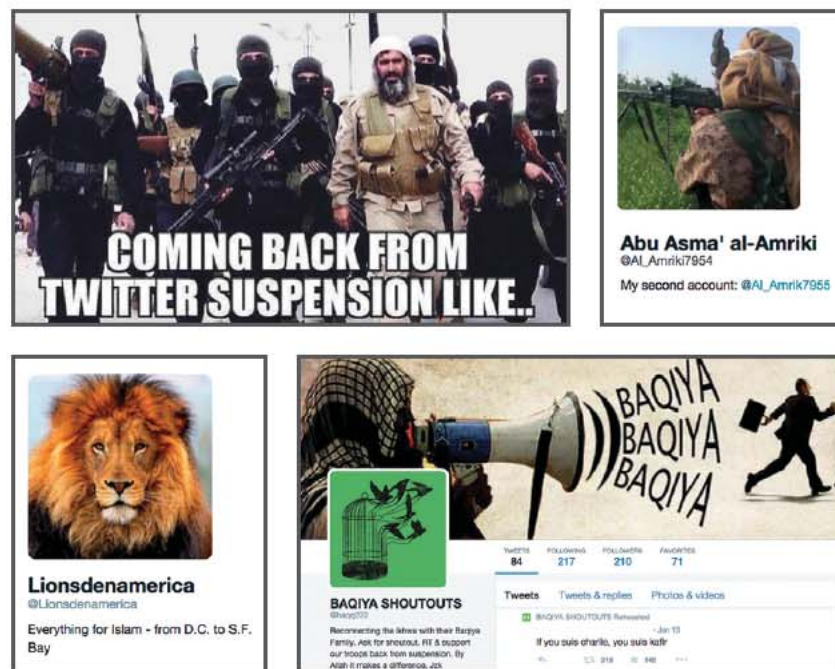


FIG. 29 Clockwise from top left: A user announces a new account; examples of node, shout-out, and amplifier accounts.

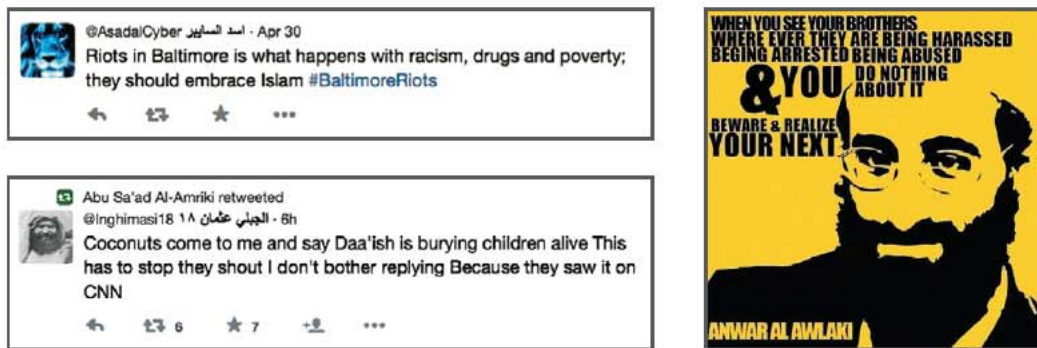


FIG. 30 Cockswort interjecting in the #BlackLivesMatter conversation sharing a quote from Anwar al-Awlaki dismissing Muslims as “coconuts”

Shout-out accounts have further bolstered connectivity by employing Twitter’s List function, which allows users to view all tweets by list members on a single page, gain access to full member lists, and weed out suspicious or contrarian accounts. American ISIS supporters have begun sharing ever-expansive lists of individuals to block through the website Block Together, a task that was previously un-delegated and decentralized. In the past individual accounts would collect a handful of accounts to block and share the list with peers via a series of tweets or posts from the website JustPaste.it. While it is unclear who is curating these lists, American ISIS supporters constantly capitalize on new tools to extend the tenure of their accounts.

Communicating primarily in English, American ISIS supporters discuss a wide range of topics, from open support for gruesome acts of terror to boringly benign banter.¹⁰⁴ When ISIS releases propaganda materials in foreign languages (namely Arabic), members of the American community often ask the larger online ISIS echo chamber for translation assistance. Popular content for American ISIS supporters’ posts include photos, videos, and discussion of human rights abuses committed by the Syrian, American, Israeli, and various Arab governments; news of ISIS’s military victories and provision of social services; photos of deceased ISIS militants

commemorating their status as martyrs; and mocking of Western (and now also Russian) leaders’ perceived weakness and ignorance.

On occasion, American ISIS supporters exploit hashtags related to U.S. policies and political movements. For example, some tried interjecting in the #BlackLivesMatter conversation in an attempt to bolster their support among African American Muslims and spread their propaganda to unsuspecting Americans of all backgrounds. Using Black Lives Matter–related hashtags, American ISIS supporters and globally based ISIS recruiters alike have sought to capitalize on unrest in Ferguson, Missouri, and Baltimore, trying to tailor their U.S.-targeted propaganda to resonate with segments of the African American community.¹⁰⁵

American accounts, like the larger ISIS echo chamber, tend not to tolerate dissent and silence attempts at nuance. Muslim religious leaders, particularly those living in the West, who condemn ISIS are routinely dismissed as “coconuts,” a derogatory term used to insult those accused of denying their Muslim identity. Many U.S.-based Muslim scholars and activists, even those from conservative backgrounds, are subject to routine death threats.

American ISIS supporters also act as “spotters” for future recruits. Our researchers observed real-time cases of

104. Our researchers include a number of Arabic speakers who reviewed Arabic-language accounts for individual who self-identified as American and found a small contingent of Americans using Arabic as their primary language.

105. Justine Drennan, “Islamic State Supporters Urge Baltimore Rioters to Join Extremist Cause,” *Foreign Policy*, April 28, 2015.

recently converted Americans pulled into the ISIS echo chamber. In one case the seemingly naïve individual posted general questions about religion, to which ISIS supporters quickly responded in a calm and authoritative manner. After a few weeks, the accounts of hardened ISIS supporters slowly introduced increasingly ardent views into the conversation. The new recruit was then invited to continue the conversion privately, often via Twitter's Direct Message feature or on other private messaging platforms such as surespot.

Real-World Clusters: ISIS's Den in America

The role of social media in recent developments in the jihadist scene in America, as elsewhere, is central. Yet, it would be incorrect to overemphasize the impact of social media by considering it the sole medium of radicalization and mobilization for American ISIS supporters. A close examination of the individuals analyzed for this study reveals a significantly more nuanced reality in which the importance of social media, while present in virtually all cases, differs substantially from case to case.

To be sure, cases of web-driven, individual radicalization have increased in frequency with the rise of ISIS. Individuals like Shannon Conley and Christopher Cornell (discussed below) are quintessential examples of individuals whose radicalization was confined to the virtual space, completely devoid of contact with like-minded individuals in the physical world.

Yet, in other cases the role of the Internet is not as all-encompassing, but rather complementary to equally, if not more, important dynamics in the physical world. In these cases, individual ISIS sympathizers did not begin their radicalization trajectories alone in front of a computer screen, but rather via face-to-face interactions through preexisting social contacts who already embraced jihadist ideology. Over time, these individuals tend to form a cluster: a small informal group of like-minded individuals whose internal dynamics reinforce the beliefs of its members. Just as the virtual community of ISIS supporters acts

as an echo chamber, these real-life connections reinforce and strengthen individual commitment to ISIS.

Individuals who belong to these informal clusters typically become consumers of jihadist propaganda on the Internet. While the online echo chamber undoubtedly contributes to the individual's and thus the cluster's radicalization, the one-on-one and group dynamics cultivated in the physical world sometimes play a greater role. In these scenarios, online and offline dynamics complement one another, both contributing to and accelerating the cluster's members' radicalization.

These group dynamics are also common in several European countries, where informal clusters often form at the margins of radical mosques, Salafist organizations, or student groups, or simply through the interaction of like-minded acquaintances in the neighborhoods of many European cities and towns. As with other radicalization-related dynamics, this phenomenon, typical of the European reality, occurs on a significantly smaller scale and less frequently than in the U.S. Yet, our analysis revealed that while some individuals fit the profile of the "lone actor," others were part of a cluster of individuals of varying sophistication who radicalized and mobilized together.

The U.S. case that most closely resembles these European dynamics is that of the Minneapolis cluster. Americans traveling to fight in conflict zones is not a new phenomenon for the Minneapolis–St. Paul area. From 2007 to approximately 2009, nearly two dozen individuals, mostly ethnic Somalis, absconded from the U.S. to join the terrorist group al Shabaab.¹⁰⁶ The departing left in small groups, the first wave providing moral and logistical support to those who followed. In response, the FBI began a massive investigation, dubbed Operation Rhino, in an attempt to stem travel to conflict areas.

At the time, some analysts argued that the wave from Minneapolis was unique to the Somali conflict. This contention was challenged in 2014, when a number of Somali Americans shifted their focus from Somalia to Syria. Since

106. B. Todd Jones, "Operation Rhino," *Office of the United States Attorneys*, July 8, 2015.

then, at least 15 individuals have traveled or attempted to travel to join ISIS.¹⁰⁷ They relied on a well-worn recruiting apparatus that leveraged deep personal, familial, and community relations. Chief among that recruiting network was Mohamed Abdullahi Hassan, one of the first to leave Minneapolis to join al Shabaab, becoming a linchpin who recruited others to follow his example. A similar dynamic occurred with Abdi Nur who, after joining ISIS in 2014, sent messages back to his friends in Minneapolis offering contact information and fake passports.¹⁰⁸ Many of the Somali-American ISIS recruits grew up in the same community, attended the same schools, and worshiped at the same mosque. Several of these individuals inherited connections to al Shabaab, including one individual whose older brother joined the group and another who lived with a friend who later departed for Somalia to join the fight.¹⁰⁹

While the Minneapolis cohort has received significant media attention, a less known but equally revealing case unfolded in St. Louis, Missouri. At the center of the cluster is a charismatic Bosnian immigrant, Abdullah Ramo Pazara. A veteran of the Bosnian civil war, Pazara came to America in the second half of the 1990s and lived a seemingly unremarkable life. He married, worked as a truck driver and developed a passion for motorcycles. But in 2011, after both his marriage and trucking business unraveled, he developed an interest in a literalist interpretation of Islam.¹¹⁰ In 2013, just days after obtaining U.S. citizenship, Pazara left for Syria, where he quickly rose to the rank of *emir* (commander) of a Balkan-dominated battalion working under well-known top ISIS commander Omar al Shishani.¹¹¹

Pazara's actions were supported by the efforts of a small group of Bosnian Americans. The men and women lived in St. Louis (home to America's largest Bosnian population) and suburban Illinois towns, but a handful originally hailed from the Bosnian town of Teslic. The group collected almost eight thousand dollars, which they sent to Pazara and families of ISIS fighters in the Balkans.¹¹² Coordinating their activities through Facebook and



FIG. 31 From the U.S. to Syria, Abdullah Ramo Pazara

107. Paul McEnroe, Abby Simons and Libor Jany, "From the Heartland to Jihad: How a Group of Young Men from Minnesota Were Drawn Into ISIL's Campaign of Terror," *Minnesota StarTribune*, September 20, 2015.

108. McEnroe, Simons and Jany, "From the Heartland to Jihad," *Minnesota StarTribune*, September 20, 2015.

109. Yuen, Ibrahim and Aslanian, "Called to Fight," *MPR*, March 25, 2015.

110. Robert Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St. Louis Post-Dispatch*, April 11, 2015.

111. Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St. Louis Post-Dispatch*, April 11, 2015. See also Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.

112. Robert Patrick, "Woman Pleads Guilty in Terror Funding Case with St. Louis Ties," *St. Louis Post-Dispatch*, September 28, 2015.

email, the group also purchased “United States military uniforms, tactical combat boots, surplus military goods, tactical gear and clothing, firearms accessories, optical equipment and range finders, rifle scopes, equipment, and supplies” for Pazara’s battalion in Syria.¹¹³ Authorities dismantled the ring in February 2015, arresting six individuals (three men and three women) on terrorism-related charges. Pazara was reported killed while fighting against Kurdish forces in Kobane in the fall of 2014.¹¹⁴

While the Minneapolis and St. Louis clusters each revolved around an ethnic bond, a separate cluster in the greater New York City area came together in a different

way and had a more heterogeneous makeup. The group initially connected as early as November 2012, when the then-teenage Nader Saadeh, a New Jersey resident of Jordanian/Palestinian descent, shared his jihadist sympathies with the like-minded Munther Omar Saleh, a teenager from Queens.¹¹⁵ In late 2014, Nader involved his older brother Alaa Saadeh and Samuel Topaz, a high school friend of mixed Jewish/Dominican descent from Fort Lee who had converted to Islam. In addition, Saleh soon incorporated Staten Island’s Fareed Mumuni into the group. The five spent their days absorbing, discussing, and sharing ISIS propaganda—both online and in the physical world. The FBI, which had the group under surveillance for months, listened in as the young men discussed building a “small army” and traveling to the Middle East.¹¹⁶

By the spring of 2015 the group had cemented their plans to join ISIS. Despite Nader’s initially successful travel to Amman, he was arrested by Jordanian authorities in the days following his arrival. In the wake of Nader’s arrest, the FBI swooped in, arresting the four remaining members of the cluster in the New York area. The arrest of Mumuni escalated, as the native of Ghana used a kitchen knife to attack FBI agents attempting to execute a search warrant of his home.

The Program on Extremism’s research has uncovered the presence of other small groups of apparent ISIS sympathizers in various American cities.¹¹⁷ One of them, located in Texas, revolves around a few charismatic individuals and an Islamic studies group. Another, based in the suburbs of a large Midwestern city, appears to be composed of former high school friends and a handful of their



FIG. 32 Nader Saadeh



FIG. 33 Alaa Saadeh



FIG. 34 Samuel Topaz on Facebook

113. *United States of America v. Ramiz Zijad Hodzic, et. al.*, Indictment (February 5, 2015).

114. Associated Press (AP), “Bosnian Immigrants Plead Not Guilty in Terror Financing Case,” *Yahoo! News*, February 11, 2015; Radio Sarajevo, “U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH,” September 25, 2014.; SAFE, “U Siriji Poginuo i Ramo Pazara iz Teslića,” September 24, 2015.; Slobodna Bosna, “Ramo Abdullah Pazara: Srpski Ratnik i Islamski Fanatik,” February 18, 2015.

115. *United States of America v. Alaa Saadeh*, Criminal Complaint (June 26, 2015).

116. *Ibid.*

117. The Program on Extremism has decided not to disclose details about these cases so as not to compromise any potential investigation.

acquaintances. As in most small clusters throughout the U.S., members of both come from diverse ethnic backgrounds and reinforce an active online life with regular interactions in the physical space.

Wide Spectrum of Support Roles

The diversity of American ISIS recruits also extends to the roles they take on in support of the cause. At one end of the spectrum is a small yet alarming number of Americans who have managed to establish deep, real world connections to ISIS. In addition to the aforementioned example of Abdullah Ramo Pazara, researchers identified a number of cases in which Americans traveled to Syria and Iraq and developed important connections to the organization.

One such case that received relatively little media attention is that of the Kodaimati clan, a Syrian-American father and his two sons who became enmeshed in shifting dynamics of two terrorist organizations. One of the sons, Mohamed Saeed Kodaimati, moved to the U.S. in 2001 where he lived for years and became an American citizen.¹¹⁸ In December 2012, Saeed (as he is referred to in the criminal complaint) traveled from San Diego to Istanbul.¹¹⁹ After three months in Turkey, Saeed was arrested by authorities and spent 35 days in prison, where he

met and interacted with a bevy of Syrian rebels, criminals, and jihadists.¹²⁰

Following his release, he travelled to Syria and began working in the JN-run Sharia Authority of Hanano district in the Aleppo governorate. In his own words, Saeed became their “media person,” posting updates on the Authority’s work on various Facebook pages.¹²¹ Sometime later, his association with JN took a much more operational role. Saeed, his father, and his younger brother—whom he refers to as “Rahmo”—began participating in combat operations with JN against the Syrian army.¹²² Saeed’s father was injured on a return trip from the frontlines, apparently by a rocket attack resulting in “shrapnel that went through his side and out through his back.”¹²³ After ISIS seized control of parts of his neighborhood from JN, Saeed became an interlocutor between the two terrorist organizations. He told a friend via Facebook that his “role is more of reconciliatory one . . . I am a mediator for those who have a problem with Da’ish [ISIL].”¹²⁴ He was allowed

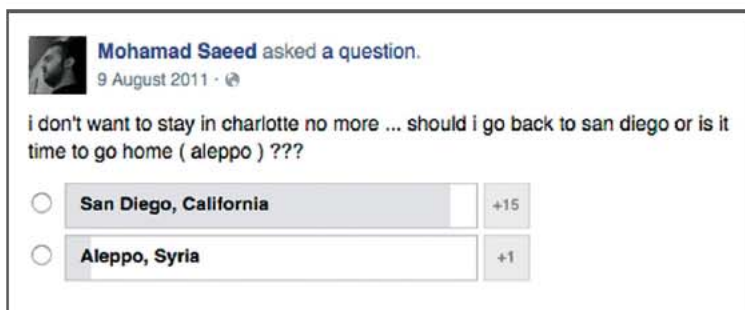


FIG. 35 Facebook post by Mohamed Saeed Kodaimati

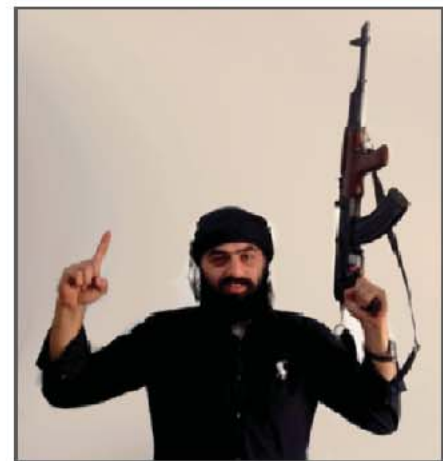


FIG. 36 Mohamed Saeed Kodaimati

118. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).

119. Kristina Davis, “San Diegan Accused of Hiding ISIS Links,” *The San Diego Union-Tribune*, April 23, 2015.

120. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).

121. Ibid.

122. Ibid.

123. Ibid.

124. Ibid.

to keep his weapons and, while stating to the FBI he never swore allegiance to ISIS, he claimed that “they know me, who I am, and I don’t have any problems with them.”¹²⁵

After three years in Syria, Saeed attempted to return to the U.S. but was prevented from boarding his flight in Turkey.¹²⁶ Local authorities sent him to the U.S. embassy, where law enforcement and diplomatic security questioned him regarding his activities in Syria.¹²⁷ Over the course of several discussions, he grossly mischaracterized his time in Syria, contending that he did not participate in any violent activity.¹²⁸ Confronted with his Facebook messages and photos corroborating authorities’ belief that he served in the ranks of terrorist groups, Saeed returned to the U.S. and pled guilty to providing false statements to the FBI.¹²⁹

On the opposite end of the mobilization spectrum, a more common typology is those whose contributions to ISIS fail to exceed online declarations of support and personal fantasies of joining the group. These are the cases of people, most often indicted for attempting to provide material support to ISIS, whose links to ISIS are largely limited to the virtual realm.

A prime example of the disturbed wannabe ISIS recruit is Shannon Conley, a Colorado native who first appeared on the radar of the FBI Denver Field Office following a confrontation with a local church.¹³⁰ During the several months she attended the church, Conley complained she was being treated unfairly due to her Muslim views and dress, making her feel like a “terrorist.”¹³¹



FIG. 37 Shannon Maureen Conley

Conley showed up one day and began sketching the layout of the church’s campus, causing church officials to ban her from the premises.¹³²

In one of her many interviews with law enforcement, Conley stated she wanted to wage jihad against “kafir” in order to protect Muslim lands.¹³³ A certified nurse, she expressed the desire to become a “housewife and camp nurse” for ISIS militants in Syria.¹³⁴ Obsessed with guerrilla warfare, she became a U.S. Army Explorer to learn American combat tactics that she could then teach to ISIS fighters and admitted to owning *Al Qaida’s Doctrine for Insurgency: Abd Al-Aziz Al-Muqrin’s A Practical Course for Guerilla War*.¹³⁵ She began communicating with a Tunisian ISIS fighter on Skype, who pushed her to join him in Syria as his wife.¹³⁶ The invitation prompted the FBI to contact

125. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).

126. *Ibid.*

127. *Ibid.*

128. *Ibid.*

129. *Ibid.*

130. *United States of America v. Shannon Maureen Conley*, Criminal Complaint (April 9, 2014).

131. *Ibid.*

132. *Ibid.*

133. *Ibid.*

134. *Ibid.*

135. *Ibid.*

136. *Ibid.*

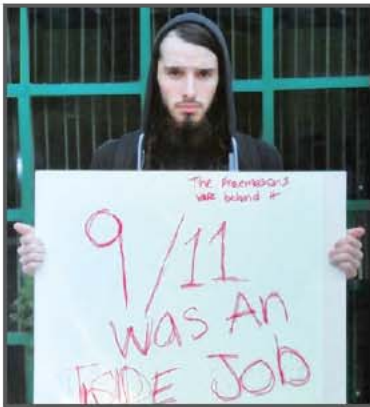


FIG. 38 Christopher Lee Cornell

Conley's parents, who joined authorities in an effort to keep Conley in the U.S. Despite their efforts, Conley's father discovered a one-way plane ticket to Turkey and contacted the FBI. The following day, his daughter was arrested while attempting to board a flight to Germany at Denver International Airport.¹³⁷

A similar case is that of Christopher Lee Cornell. Born in a Cincinnati suburb, Cornell wrestled in high school and is remembered by teachers as a "typical student."¹³⁸ After graduating in 2012, Cornell, described by his father as a "big mama's boy" whose best friend was a cat, lived with his parents and was unemployed.¹³⁹ In the summer of 2014 Cornell converted to Islam, growing his beard

and donning traditional Muslim clothing.¹⁴⁰ He became increasingly angry, isolated, and withdrawn, often attracting harassment from neighbors.¹⁴¹ Cornell developed an online persona as Raheel Mahrus Ubaydah and a network of contacts—among them an FBI undercover operative.¹⁴² Cornell informed the operative of his plans to attack the U.S. Capitol and set off a series of pipe bombs.¹⁴³ He was arrested in January 2015 after purchasing several semi-automatic rifles and approximately 600 rounds of ammunition as part of an FBI sting.¹⁴⁴

Determining a link to ISIS has proven challenging in a few recent cases. The most prominent is that of Mohammad Abdulazez, the shooter whose attacks on two military installations in Chattanooga in July 2015 left five dead. Following the incident, investigators discovered Abdulazez operated a blog focusing on Islamist themes, and downloaded copies of Anwar al Awlaki's sermons. Yet authorities were unable to determine a link to or a demonstrated interest in ISIS.¹⁴⁵ Suggesting additional or concurrent potential explanations for his actions, before the attack Abdulazez allegedly stopped taking his anti-depression medication and regularly consumed illegal narcotics.¹⁴⁶

A second incident that escapes easy categorizations took place in Oklahoma in September 2014, when 31-year-old convert Alton Nolen beheaded a former coworker. Nolen carried out the gruesome act shortly after having been suspended from his job, potentially indicating that he was motivated by personal reasons.¹⁴⁷ On the other hand,

137. Michael Martinez, Ana Cabrera and Sara Weisfeldt, "Colorado Woman Gets 4 Years for Wanting to Join ISIS," *CNN*, January 24, 2015.

138. AP, "Teachers: Ohio Man Accused in Terror Plot a Typical Student," *WHSV.com*, January 15, 2015.

139. Ben Brumfield, Pamela Brown and Dana Ford, "FBI Says Plot to Attack U.S. Capitol was Ready to Go," *CNN*, January 15, 2015.

140. Brumfield, Brown and Ford, "FBI Says Plot to Attack U.S. Capitol was Ready to Go," *CNN*, January 15, 2015.

141. Kimball Perry and Patrick Brennan, "Father: Terror Plot Suspect was a 'Momma's Boy,'" *Cincinnati.com*, January 23, 2015.

142. *United States of America v. Christopher Lee Cornell*, Criminal Complaint (January 14, 2015).

143. *Ibid.*

144. *Ibid.*

145. Jonathan Dienst and Miguel Almaguer, "Mohammad Youssef Abdulazez Downloaded Recordings from Radical Cleric, Officials Say," *NCB News*, July 21, 2015.

146. Greg Jaffe, Cari Wade Gervin and Thomas Gibbons-Neff, "Tenn. Gunman Used Drugs, Struggled with Clash of Faith," *The Washington Post*, July 18, 2015.

147. Abby Ohlheiser, "What we Know about Alton Nolen, Who as been Charged with Murder in the Oklahoma Beheading Case," *The Washington Post*, September 30, 2014.

the act's modalities and the fact that Nolen, while having no known contact with ISIS, was an avid consumer of jihadist propaganda online, suggest that the case could be more than an ordinary incident of workplace violence.¹⁴⁸

Similarly unclear is the case of Zale Thompson, who attacked four New York Police Department officers with a hatchet in October 2014.¹⁴⁹ His online search history shows an interest in jihadist videos, some of which included ISIS material.¹⁵⁰ However, Thompson, who was described by law enforcement as a loner with possible mental problems, also consumed black nationalist and other anti-government propaganda online, making an

even inspirational link to ISIS uncertain at best.

Perhaps the most puzzling is the case of Joshua Ryne Goldberg, a 20-year-old Jewish Floridian who was arrested in September 2015 for distributing information relating to a bomb plot targeting a 9/11 memorial ceremony in Kansas City.¹⁵¹ Goldberg had multiple online personas: an ISIS-affiliated Australian jihadist, a white supremacist, a feminist, and a free-speech radical.¹⁵² Regardless of his life as a virtual troll, Goldberg did nonetheless provide an individual, who unbeknownst to Goldberg was an FBI informant, with instructions for constructing a bomb from a pressure cooker filled with nails.¹⁵³

148. Michael Pearson, "Who is Oklahoma Beheading Suspect Alton Nolen?," *CNN*, September 30, 2014.

149. Agence France-Presse, "New York Police Brand Hatchet Attack 'Terrorist' Act," *Yahoo News!*, October 24, 2015.

150. Caitlin Nolan, Kerry Burke, Rocco Parascandola, Joseph Stepansky and Thomas Tracy, "Hatchet-wielding Man Shot Dead by NYPD Cops in Queens; Police Eye Possible Terrorism Motive," *New York Daily News*, October 24, 2014.

151. Garrett Pelican, "Orange Park Man, 20, Indicted in 9/11 Memorial Bomb Plot," *First Coast News*, September 15, 2015.

152. Katie Zavadski, "'Terrorist' Troll Pretended to be ISIS, White Supremacist, and Jewish Lawyer," *The Daily Beast*, September 11, 2015.

153. *United States of America v. Joshua Ryne Goldberg*, Criminal Complaint (September 10, 2015).

CONCLUSION

Countering ISIS's American Recruits

THIS REPORT has provided a look inside the bubble of American ISIS sympathizers, a diverse and diffuse scene that the FBI estimates include hundreds, if not thousands, of individuals. To be sure, most of the participants in this counter-culture will never make the leap from talk to action, from being keyboard warriors to actual militancy. Some will mature out of what is just an awkward adolescent phase. Others simply lack the personality traits necessary for committing terror attacks or setting out for ISIS territory. On a more mundane level, others find themselves restrained by the practical commitments of their daily lives.

Nonetheless, a subset of the Americans inside the domestic ISIS bubble, whether they operate individually or in small clusters, will at some point move from chatter to action. For some that will mean boarding a flight to the Middle East. For others, it will entail gathering the equipment needed to carry out an attack inside the United States. The decision to attack the home front may follow unsuccessful attempts to link up with recruiters overseas. In other cases, the attacker's horizon remains focused on targeting the "infidels" inside America.

The diversity of ISIS's American recruits and the wide range of ways they demonstrate their support requires careful consideration prior to any potential policy response. Because there is no standard recruit profile, there is also no silver bullet that will blunt ISIS's allure. Recognizing this complexity is a vital initial step for policymakers, law enforcement officials, civic leaders, teachers, and parents when crafting effective solutions.

Stepping back to consider the implications of the demographic data and personality profiles surveyed in this report, several essential policy recommendations emerge:

First, the number of ISIS recruits in America and the

complex scene they comprise poses a challenge that cannot be solved solely by arrests. Law enforcement vigilance is vital but insufficient on its own. Moreover, many early-stage ISIS sympathizers have not necessarily broken any laws. A comprehensive preventive approach to radicalization is necessary. Unfortunately, the resources devoted to countering violent extremism (CVE) by the U.S. government remain woefully inadequate for the task at hand.¹⁵⁴ Robust funding and dynamic programs are needed immediately.

Second, an effective alternative to arrest is intervention to help sway individuals from the path of radicalization. Our research identified 71 ISIS recruits in the U.S. legal system—a figure far short of the 250-plus Americans who, according to government officials, have attempted to or actually traveled to Syria and Iraq. Why those 180 individuals are not in the legal system has several explanations, including the fact that many cases fail to meet the legal threshold for arrest. This factor reinforces the need for the government to create a framework for targeted interventions with radicalized individuals by non-law enforcement groups, as well as legal parameters so that interveners are not at risk of civil and criminal liability if their efforts fail.

Third, while interventions are a potential solution for Americans already on the path to radicalization, it would be even more effective to prevent citizens from even starting that perilous journey. Researchers and civic leaders should empirically analyze which messaging resonates best with audiences commonly targeted by ISIS, recognizing that a range of narratives deployed for unique audiences will likely be necessary.

Fourth, there are individuals and organizations that would like to implement counter-ISIS messaging online, yet worry that their activities might inadvertently attract the attention of law enforcement. For instance, several

154. Lorenzo Vidino and Seamus Hughes, "Countering Violent Extremism in America," Program on Extremism, June 2015.

American Muslims consulted for this report expressed willingness to engage ISIS supporters online yet hesitated to do so for fear of falling onto the FBI's radar by engaging in dialogue with radicals. The government should provide legal guidance and recommend best practices so that potential counter-messengers can make informed decisions on whether and how to engage.

Finally, there is a largely untapped opportunity to leverage American ISIS recruits who have become disillusioned with the cause. These individuals have dropped out for a variety of reasons, whether experiencing the brutality of life under ISIS firsthand or finding a more positive outlet for the quest that led them to ISIS in the first place. U.S. officials would do well to provide avenues for their stories to be amplified to help dissuade would-be recruits.

The government should consider, within reason, limited immunity for some returning foreign fighters, as their messages are more likely to resonate than those delivered by most other counter-messaging programs.

While jihadist causes have lured American recruits for several decades, the surge spurred by the rise of ISIS and its sophisticated marketing of its counter-culture to impressionable Americans is unprecedented. The data and vignettes provided in this report illuminate the complexity of the threat and caution against simple solutions. In their response to this challenge, American political and civic leaders will need to be bold, experimental, and receptive to novel policies and initiatives in order to defeat ISIS and protect some of our fellow citizens from falling into its clutches.

APPENDIX

The 71 individuals charged for ISIS-related activities (as of November 12, 2015)

Abdi Nur	John T Booker
Abdirahman Yasin Daud	Jonas ‘Yunus’ Edmonds
Abdul Malik Abdul Kareem	Joshua Ray Van Haften
Abdullahi Mohamud Yusuf	Justin Nojan Sullivan
Abdurasul Hasanovich Juraboev	Keonna Thomas
Abror Habibov	Leon Nathan Davis III
Adam Dandach	Mediha Medy Salkicevic
Adnan Abdihamad Farah	Michael Todd Wolfe
Ahmed Mohammed El Gammal	Miguel Moran Diaz
Akba Jihad Jordan	Mohamad Saeed Kodaimati
Akhror Saidakhmetov	Mohamed Abdihamid Farah
Akmal Zakirov	Mohamed Abdullahi Hassan
Alaa Saadeh	Mohammad Hamza Khan
Alexander Ciccolo	Mufid Elfgeeh
Alexander E Blair	Muhammad Oda Dakhalla
Ali Saleh	Muhanad Badawi
Ali Shukri Amin	Munther Omar Saleh
Arafat Nagi	Nader Elhuzayel
Armin Harcevic	Nader Saadeh
Asher Abid Khan	Nicholas Rovinski
Asia Siddiqui	Nicholas Teausant
Avin Marsalis Brown	Nihad Rosic
Bilal Abood	Noelle Velentzas
Christopher Lee Cornell	Ramiz Zijad Hodzic
David Wright	Reza Niknejad
Dilkhayot Kasmiov	Robert C. McCollum
Donald Ray Morgan	Samuel Rahamin Topaz
Fareed Mumini	Sedina Unkic Hodzic
Guled Ali Omar	Shannon Maureen Conley
Hamza Naj Ahmed	Tairod Nathan Webster Pugh
Hanad Mustafe Musse	Terrence McNeil
Harlem Suarez	Unnamed minor (PA)
Hasan Edmonds	Unnamed minor (SC)
Heather Elizabeth Coffman	Yusra Ismail
Jaelyn Delshaun	Zacharia Yusuf Abdurahman
Jasminka Ramic	

What explains the recent surge in American jihadi recruits? Who are the Americans lured by the siren songs of ISIS's propaganda? How do they embrace such radical ideology? What do they seek?

This report provides a comprehensive overview of ISIS-related radicalization and mobilization in the United States.

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

www.cchs.gwu.edu/program-extremism ■ @gwupoe

From: (b) (6)
To: (b) (6)
Subject: RE: DHS CVE Corodinator for Boston
Date: Thursday, September 03, 2015 12:17:50 PM
Attachments: [image001.jpg](#)

(b) (6)

Just looping back on this. I spoke with (b) (6) for about an hour today via phone. He is going out to LA to get some OJT with another CVE person for DHS to see how it is working out west. He seems to understand I&A's authorities pretty well and wants to coordinate / work with us when appropriate. I will be setting up a get together with him in late Sept.

Vr/

(b) (6)

(b) (6)
Regional Director, New England
Field Operations
Office of Intelligence and Analysis
U.S. Department of Homeland Security

(b) (6)

WARNING: This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you received this message in error, please reply immediately to the sender and delete this message.

From: (b) (6)
Sent: Monday, August 31, 2015 4:27 PM
To: (b) (6)
Subject: RE: DHS CVE Corodinator for Boston

(b) (5)

From: (b) (6)
Sent: Monday, August 31, 2015 3:17 PM
To: (b) (6)
Subject: RE: DHS CVE Corodinator for Boston

(b) (5)

Thanks for tracking all this down!

■

From: [REDACTED]
Sent: Monday, August 31, 2015 2:54 PM
To: (b) (6)
Subject: RE: DHS CVE Corodinator for Boston

Just got off the phone with my colleague at NPPD, he has the name, is sending to me.

The Boston CVE coordinator is (b) (6). He does not have a cellphone listed in global yet.

(b) (6)

[REDACTED]

Evidently, there is one in your AOR and one in LA (CVE Coordinator). They work under the Office of Strategic Engagement within NPPD.

(b) (5)

[REDACTED]

From: (b) (6)
Sent: Monday, August 31, 2015 2:22 PM
To: (b) (6)
Cc: [REDACTED]
Subject: RE: DHS CVE Corodinator for Boston

(b) (5)

[REDACTED]

(b) (6)
Regional Director, New England
Field Operations
Office of Intelligence and Analysis
U.S. Department of Homeland Security

(b) (6)

[REDACTED]

WARNING: This communication, along with any attachments, is covered by federal and

state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you received this message in error, please reply immediately to the sender and delete this message.

From: [REDACTED]
Sent: Monday, August 31, 2015 2:21 PM
To: (b) (6)
Cc: [REDACTED]
Subject: RE: DHS CVE Corodinator for Boston

Checking with NPPD

From: [REDACTED]
Sent: Monday, August 31, 2015 2:18 PM
To: [REDACTED]
Cc: (b) (6)
Subject: RE: DHS CVE Corodinator for Boston

First I have heard of it.

[REDACTED]
Regional Director, New England
Field Operations
Office of Intelligence and Analysis
U.S. Department of Homeland Security
(b) (6)

WARNING: This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you received this message in error, please reply immediately to the sender and delete this message.

From: [REDACTED]
Sent: Monday, August 31, 2015 1:46 PM
To: (b) (6)
Subject: DHS CVE Corodinator for Boston

All,
So apparently there is a new DHS CVE coordinator who has been hired and deployed to Boston (thru NPPD?). Also there is apparently a big CVE meeting tomorrow with this person with all the agency heads here. (b) (5)

[REDACTED]
(b) (5)
Thank you

[REDACTED]

[REDACTED]

Office of Intelligence & Analysis
Department of Homeland Security
Commonwealth of Massachusetts

(b) (6) [REDACTED]

[REDACTED]

(b) (6) [REDACTED]

[REDACTED]



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**COUNTERING ISLAMIC RADICALIZATION AND
AL SHABAAB RECRUITMENT WITHIN THE ETHNIC
SOMALI POPULATION OF THE UNITED STATES: AN
ARGUMENT FOR APPLYING BEST PRACTICES FOR
STEMMING YOUTH GANG RECRUITMENT AND
INITIATION**

by

Jeffrey J. Jones

December 2010

Thesis Advisor:

Second Reader:

John Rollins

Javed Ali

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2010	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Countering Islamic Radicalization and Al Shabaab Recruitment Within the Ethnic Somali Population of the United States: An Argument for Applying Best Practices for Stemming Youth Gang Recruitment and Initiation			5. FUNDING NUMBERS	
6. AUTHOR(S) Jeffrey J. Jones				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) Over the past few years, a spate of attempted plots, lethal attacks, and arrests of American Muslims both at home and overseas has created the perception of a more worrisome development regarding the issue of domestic radicalization and homegrown violent extremism. The individuals involved in these developments have come from a broad cross-section of various ethnic, socioeconomic, cultural, and geographic backgrounds in the United States, making it difficult for law enforcement and the intelligence community to focus their efforts to predict or determine where violent extremists will emerge. This thesis focuses on the Somali-American community in particular and the threat posed by a very small percentage of that community that has, in recent years, been drawn to violent extremist agendas in Somalia. This thesis examines existing best practices that might be leveraged or utilized to combat the radicalizing influences that have affected some Somali-Americans in the past, with the hope that those practices can prevent similar effects in the future.				
14. SUBJECT TERMS Al Shabaab, Al Qaeda East Africa, Somalia, Somali-American, Radicalization, Community mobilization, Social capital, Trust, Socioeconomic, Spengel model, Disaffection			15. NUMBER OF PAGES 105	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**COUNTERING ISLAMIC RADICALIZATION AND AL SHABAAB
RECRUITMENT WITHIN THE ETHNIC SOMALI POPULATION OF THE
UNITED STATES: AN ARGUMENT FOR APPLYING BEST PRACTICES FOR
STEMMING YOUTH GANG RECRUITMENT AND INITIATION**

Jeffrey J. Jones
Supervisory Special Agent, Federal Bureau of Investigation
B.A., Mary Washington College, 1992

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2010**

Author: Jeffrey J. Jones

Approved by: John Rollins
Thesis Advisor

Javed Ali
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT¹

Over the past few years, a spate of attempted plots, lethal attacks, and arrests of American Muslims both at home and overseas has created the perception of a more worrisome development regarding the issue of domestic radicalization and homegrown violent extremism. The individuals involved in these developments have come from a broad cross-section of various ethnic, socioeconomic, cultural, and geographic backgrounds in the United States, making it difficult for law enforcement and the intelligence community to focus their efforts to predict or determine where violent extremists will emerge. This thesis focuses on the Somali-American community in particular and the threat posed by a very small percentage of that community that has, in recent years, been drawn to violent extremist agendas in Somalia. This thesis examines existing best practices that might be leveraged or utilized to combat the radicalizing influences that have affected some Somali-Americans in the past, with the hope that those practices can prevent similar effects in the future.

¹ The opinions expressed in this thesis are those of Jeffrey J. Jones and do not necessarily reflect those of the Federal Bureau of Investigation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND AND PROBLEM STATEMENT	1
B.	RESEARCH QUESTION	4
C.	METHODOLOGY	4
1.	Comparative Study	4
2.	Appreciative Inquiry	5
D.	LITERATURE REVIEW	5
1.	Al Shabaab’s Rise to Power	6
2.	Al Shabaab and Al Qaeda: A Dual Threat to the United States	8
3.	The Threat Posed by Radicalized Americans Supporting Al Shabaab.....	10
4.	The Way Forward: Applying Counter-Gang Program Best Practices in Countering the Radicalization of Ethnic Somali-Americans	12
II.	A STUDY OF THE UNITED KINGDOM’S COUNTERRADICALIZATION PROGRAM AND ASSESSMENT OF THE VIABILITY OF ITS APPLICATION IN THE UNITED STATES	17
A.	THE UK’S NATIONAL COUNTERRADICALIZATION PLAN	17
B.	THE VIABILITY OF THE UK PREVENT MODEL’S APPLICATION IN THE UNITED STATES.....	24
C.	CONCLUSION	28
III.	COUNTERGANG BEST PRACTICES	29
A.	A “GANG” DEFINED.....	29
B.	A BRIEF HISTORY OF GANGS IN THE UNITED STATES	30
C.	COMMUNITY MOBILIZATION INITIATIVES.....	31
D.	CONCLUSION	39
IV.	ANALYSIS	43
A.	SOCIOECONOMIC FACTORS CONTRIBUTING TO YOUTH GANG RECRUITMENT.....	44
B.	SOCIOECONOMIC FACTORS CONTRIBUTING TO SOMALI-AMERICAN AL SHABAAB RECRUITMENT.....	48
C.	CONCLUSION	60
V.	FINDINGS AND RECOMMENDATIONS	63
A.	FINDINGS	63
B.	NATIONAL POLICY GUIDANCE.....	65
C.	BUILDING TRUST	66
D.	DECENTRALIZING THE EFFORT	68
E.	PROPOSAL.....	69
	LIST OF REFERENCES	75
	INITIAL DISTRIBUTION LIST	87

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Comprehensive Gang Program Model.....	35
Figure 2.	Framework of Multiple Marginality: “Act and React”.....	47

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Law Enforcement Strategies and Perceived Effectiveness	33
Table 2.	Effectiveness of Comprehensive Gang Model	36
Table 3.	Somali-Americans Supporting Al Shabaab	52
Table 4.	Non-Somali-American Converts Supporting Al Shabaab	53

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIAI	al-Ittihad al-Islami
AQEA	Al Qaeda East Africa
CAP	Chicago Area Project
CBRN	Chemical, Biological, Radiological, Nuclear
CLG	Communities and Local Government
DHS	Department of Homeland Security
DOJ	Department of Justice
FATA	Federally Administered Tribal Area
FBI	Federal Bureau of Investigation
GRP	Gang Reduction Program
HOA	Horn of Africa
IC	Intelligence Community
ICC	Islamic Courts Council
ICU	Islamic Courts Union
ISC	Intelligence and Security Committee
NCTC	National Counter-Terrorism Center
NGO	Non-Governmental Organizations
NGTA	National Gang Threat Assessment
OJJDP	Office of Juvenile Justice and Delinquency Prevention
OSCT	Office of Security and Counter-Terrorism
QHSR	Quadrennial Homeland Security Review
RICU	Research, Information and Communications Unit
TFG	Transitional Federal Government
UK	United Kingdom
US	United States
USG	United States Government
USPER	United States Person

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the faculty of the Naval Postgraduate School's Center for Homeland Defense and Security and the Federal Bureau of Investigation's Counterterrorism Division for selecting me to participate in what has been the most rewarding educational experience of my career. I would also like to give a special thanks to Assistant Section Chief C. Bryan Paarmann, who afforded me time to participate in this extraordinary professional development experience alongside colleagues from municipal, state, and other federal agencies.

I would like to thank my thesis advisors, John Rollins, and Javed Ali. Their wisdom and insight borne from years of experience serving our nation was instrumental in my successful completion of this thesis.

I would like to reserve my most sincere and heartfelt thanks for my wife and daughters. I can never sufficiently express in words how thankful I am for your patience, love, and support, which make possible all personal or professional success I enjoy.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The President's national security strategy explicitly recognizes the threat to the United States posed by individuals radicalized here at home.

-Eli Lake

East Africa-based al-Qa'ida leaders or al-Shabaab may elect to redirect to the Homeland some of the Westerners, including North Americans, now training and fighting in Somalia.

-Dennis Blair

A. BACKGROUND AND PROBLEM STATEMENT

In December 2006 the Ethiopian military invaded Somalia and overthrew the governing Islamic Courts Council (ICC). During the ensuing conflict several citizens were discovered fighting against the Ethiopians alongside Al Shabaab Al-Mujahidin (Al Shabaab), the largest and best organized armed militia in Somalia. Since that time, Al Shabaab has been designated by the United States as a terrorist organization because it has "committed, or poses a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States" (United States Department of State [USDOS], 2008). This designation was made largely due to the threat posed by Al Shabaab's close association with the Al Qaeda terrorist organization (Brennan, 2010), but its pronouncement was likely spurred on by incidents of support of Al Shabaab by Somali-Americans and other radicalized Americans, including travel by those individuals to Somalia for the purposes of engaging in jihad. Al Shabaab's ties to Al Qaeda are rooted in Al Shabaab's close relationship in recent years with Al Qaeda East Africa (AQEA) operative Saleh Nabhan (Mudd, 2009). Nabhan was an unindicted co-conspirator involved in the planning of the 1998 bombing of the U.S. embassies in Kenya and Tanzania and was an active supporter of Al Shabaab, providing militaristic training to the terrorist group until his recent death at the hands of the U.S. military (Roggio, 2009). Prior to his death, the FBI had been actively seeking to indict Nabhan for his role in the 1998 embassy bombings, which resulted in the deaths of

U.S. citizens. Horn of Africa (HOA) expert Dr. David Shinn notes that Al Shabaab's current leader, Muktar Robow, continues Al Shabaab's affiliation with Al Qaeda, as he reinforced in a 2008 statement:

We will take our orders from Shayk Usama bin Ladin because we are his students.... Most of our leaders were in trained in al-Qa'ida camps. We get our tactics and guidelines from them. Many have spent time with Usama bin Ladin. (Shinn, 2009, p. 3)

Despite the U.S. Department of State's designation of Al Shabaab as a terrorist organization, U.S. citizens continue to travel to Somalia to fight alongside Al Shabaab (Mueller, 2009) against the Somali Transitional Federal Government (TFG), which was installed to replace the ICC. To date dozens of radicalized² U.S. citizens have since been identified as having traveled to the region to engage in jihad against the TFG government and military forces in place to protect that government. The FBI believes that other U.S. citizens have yet to be identified. The reasons behind these citizens' support of Al Shabaab will be examined later in this paper. Al Shabaab's close alignment with Al Qaeda (Associated Press, 2009), currently the gravest terrorist threat to U.S. national security, is made worse by the fact that Al Shabaab is the most prolific trainer currently known of American citizens seeking to become jihadists. In 2008, the world witnessed the first American citizen die as a suicide bomber inside Somalia in support of Al Shabaab operations (Mudd, 2009). The threat to the United States posed by Al Shabaab and by the American citizens now trained by Al Shabaab has garnered the attention of the U.S. national leadership, which has declared that the radicalization of such Americans is a threat to our national security (Simmons, 2006, p.1; Lieberman, 2009, Blair, 2010, p.11; Mueller, 2009). While no ethnic Somali-Americans have yet returned to the United States

² Broadly defined, radicalization is the process by which an individual or group assumes extremist beliefs and/or behaviors. (Homeland Security Institute, 2006, p. 1) Within the context of this problem, however, radicalization is more specifically defined as the process whereby an individual comes to accept an extreme and militant interpretation of Islam in which Western and Western-affiliated powers are seen as aggressors against Islam. This version of Islam defines society in terms of Muslims and non-Muslims, or as Muslims and infidels, and espouses the necessity of 'jihad' and violent action as a means to defend Islam from the infidels (Mullins, 2008, para. 3).

and conducted terrorist attacks, those returning upon completing their jihadist training (and in some cases fighting) pose a real and present danger to the security of the United States.

There is general agreement among leaders within Islamic communities in the United States and experts in the field of Horn of Africa (HOA) studies (Anwar, 2006) that law enforcement agencies in the United States must proactively engage in community outreach within ethnic Somali communities in order to stem the tide of Somali-American radicalization and recruitment at the hands of extremist Islamists. To stem the occurrence of radicalization among the ethnic Somali population in the United States and therefore reduce the likelihood that radicalized American Somalis would, at the behest of the Al Shabaab terrorist organization, engage in terrorist attacks within the United States, local, state, and federal law enforcement agencies, including the FBI, public welfare entities, and private sector organizations have initiated efforts to counter radicalization occurring within ethnic Somali communities. Current counterradicalization policies and practices are a necessary and positive step toward both improving government relations with Somali-Americans and reducing radicalization among that segment of the population, but the degree to which they have been effective in achieving these goals is not known. However, it is clear that in their current state these efforts do not fully address the underlying socioeconomic factors (Mukhtar, 2009, p.7) that foster an environment in which American Somali youth are likely to become radicalized and thus be susceptible to Al Shabaab recruitment. This is evidenced by the continued radicalization of Somali-American males who continue to travel to the Horn of Africa region to train with, and fight alongside, the Al Shabaab terrorist organization (Hsu, 2009).

While the radicalization and Al Shabaab recruitment of Somali-Americans is a relatively new problem, many of the causative socioeconomic factors are nearly identical to those at the root of the decades-old problem of youth gang formation in the United States. For decades, law enforcement and social welfare agencies in the United States have addressed the problem of youth gangs and the proliferation of such gangs in our society, and over time they have identified best practices for countering youth gang

recruitment and initiation. The success of these best practices is attributable in part to these agencies' incorporation of policies and procedures cognizant of, and sensitive to, the aforementioned underlying socioeconomic factors contributing to the formation of youth gangs. The adoption of such best practices by law enforcement and social welfare agencies and organizations, if applicable, would allow such agencies to conserve valuable resources currently dedicated to identifying, largely through trial and error, the most effective and efficient means of conducting community outreach to the Somali-American community in an effort to counter the radicalization occurring in that community.

B. RESEARCH QUESTION

Understanding that programs focused on countering radicalization among Somali-American youth are only a first step to addressing this nationwide problem and that similar programs are needed to address this problem within other communities in the United States, the U.S. government must nonetheless act quickly to address radicalization within the U.S. Somali diaspora communities.

What, if any, best practices can be derived from law enforcement and public welfare agency efforts over the last four decades to stem youth gang recruitment and initiation and then be applied to the U.S. government's efforts to counter radicalization and Al Shabaab recruitment within the ethnic Somali diaspora in the United States?

C. METHODOLOGY

1. Comparative Study

In an effort to ascertain counterradicalization best practices to be utilized by the United States, a review of the current counterradicalization program utilized by the United Kingdom—a country of similar cultural and governmental construct as the United States—demonstrates both the positive and negative effects of such a comprehensive, nationwide program. This study examines these positive and negative aspects and offers an assessment of the likelihood of such a program's being implemented in the United States. This study begins with the assertion there is currently no unified national strategy for countering radicalization.

2. Appreciative Inquiry

Through a secondary analysis of the primary source material regarding counter-gang best practices in the United States, the viability of the application of these best practices to the USG's counter-radicalization efforts among Somali-American communities was examined after reviewing and comparing the underlying socioeconomic factors contributing to both gang recruitment and Somali-American radicalization.

D. LITERATURE REVIEW

The literature addressing the ongoing conflict in Somalia, Al Shabaab's role in that conflict, and the threat arising from radicalized American citizens traveling to Somalia to fight alongside Al Shabaab is understandably limited, given the relatively short time span of this issue. While there are books written prior to the December 2006 Ethiopian invasion of Somali that tangentially address Al Qaeda's interests in the Horn of Africa (HOA) region (e.g., Lewis, 2003; Emerson, 2002; Kepel, 2004), these works do not address the specific issues of the radicalization of ethnic Somali-Americans, their support to Al Shabaab, and the threat they pose to the homeland. The bulk of the publications addressing these issues thus far have been periodicals, research reports, and proceedings of meetings and other forums, such as symposiums and Congressional testimony. These are dominated by the commentary of a few frequently quoted and cited experts on matters related to the HOA region. There is also government research as well as analysis conducted by nongovernmental organizations such as the Somali Justice Advocacy Center and the Somali Family Care Network. These offer insight into both the government's perception of the threat posed to the United States by Al Shabaab and its supporters in the United States, as well the perception of civic organizations focused on providing aid to the Somali diaspora. Additionally, there are also sources that address the issue of gang recruitment and initiation, the relevance of which I will discuss later in this proposal. All of these sources have been organized according to which of the following key categories they address. Some sources cover more than one of these topics:

- Al Shabaab's rise to power;
- Al Shabaab and Al Qaeda: a dual threat to the United States;
- The threat to the homeland posed by radicalized Americans supporting Al Shabaab;
- The way forward: applying counter-gang program best practices in countering radicalization of ethnic Somali-Americans.

1. Al Shabaab's Rise to Power

One of the most prolific writers on the topic of Somalia's political instability and societal turmoil is Dr. Ken Menkhaus, professor of political science at Davidson College and noted expert on HOA issues. In March 2009, Menkhaus testified in a hearing entitled "Violent Islamist Extremism: Al Shabaab Recruitment in America" before the U.S. Senate Committee on Homeland Security and Governmental Affairs. Menkhaus's testimony focused on how the ongoing societal instability in Somalia has led to the emergence of the nationalistic-focused group Al Shabaab, which has inspired the Somali diaspora globally. Menkhaus attributes the rise of Al Shabaab to the intense nationalistic feelings of the Somali people and their dissatisfaction with the United Nations–installed Transitional Federal Government in Somalia. Menkhaus also attributes the newly discovered radicalization of young ethnic Somali-Americans to similar nationalistic feelings, which coupled with feelings of alienation and disenfranchisement in their U.S. communities, make this segment of the population especially susceptible to radicalization and recruitment by Al Shabaab. In his testimony Menkhaus also spoke of the cultural obstacles that law enforcement must overcome in order to conduct effective outreach to the Somali communities in the United States, obstacles that include an innate fear of authority, a history of victimization, and the all-too-frequent lack of positive male role models for impressionable young ethnic Somali men—sentiments expressed by a clear majority of writers on this subject. This subject will be addressed further in another segment of this review.

Echoing many of the same sentiments as Menkhaus is former U.S. Ambassador to Ethiopia and Deputy Director of the U.S. Department of State Somalia Task Force Dr.

David H. Shinn. In a paper he submitted to the Combating Terrorism Center at the U.S. Military Academy at West Point, Shinn provides an overview of the history of Al Qaeda in Somalia, the rise of Al Shabaab, and its recruitment of Americans and other Westerners, and he offers suggestions as to how best to stabilize the internal conditions in Somalia. Shinn asserts that Al Shabaab's genesis can be traced to the 1998 bombings of the U.S. embassies in Kenya and Tanzania committed by al-Ittihad al-Islami (AIAI) (Shinn, 2009, p. 2). Shinn asserts that Aden Hashi Ayro, a former member of the Somali Islamic Courts Union (ICU) who had trained with Al Qaeda in Afghanistan and who was inspired by the 1998 AIAI embassy attacks, formed Al Shabaab in 2004 (Shinn, 2009, p. 2). Shinn notes that Ayro employed nationalistic and Islamic rhetoric to energize "disaffected young Somalis" as he led them into battle against the Ethiopians who had invaded Somalia to depose the ICU (Shinn, 2009, p.2). Shinn's work borrows heavily from news accounts of the Ethiopian invasion of Somalia, as well as from his peer, Dr. Ken Menkhaus. Shinn's paper, however, unlike the works by Menkhaus, offers no solutions as to how the United States should address the problem of the radicalization of its ethnic Somali population.

On the theme of how best to address the crisis in Somalia, Ted Dagne, a specialist in African affairs and a writer for the Congressional Research Service, wrote a February 2009 report to Congress entitled "Somalia: Current Conditions and Prospects for a Lasting Peace." In that report, which focused heavily on the issue of Somali piracy on the high seas, Dagne spoke to the current security conditions in Somalia, specifically the instability caused by the ongoing attacks by Al Shabaab against the TFG and its protective forces. Dagne, like Roque and Menkhaus, notes that while Al Shabaab was at least partially responsible for the relative peace enjoyed by Somalis prior to the 2006 invasion by the Ethiopians, Al Shabaab was also responsible for the current continued societal unrest. Dagne makes note of the fact that American citizens have traveled to Somali, but he does not address the fact that these Americans traveled to Somalia to fight in support of Al Shabaab and the TFG. Dagne acknowledges that one American has martyred himself as a suicide bomber inside Somalia, but he paints the occurrence as an anomaly and delves no further into the issue. Dagne seeks to inform his audience—in this

case the Congress—about the current security situation in Somalia, and his work is informative with regard to the current security environment in Somalia and the threat posed by Al Shabaab. However, Dagne’s work, like many in this field, offers little insight into why Americans are fighting alongside Al Shabaab within Somalia and offers no suggestions as to how best to address this phenomenon.

In summary, the literature covering the history of Somalia and the rise of Al Shabaab is largely homogeneous, as authors on this topic tend not to stray far from commonly accepted facts derived from historical accounts. While informative and necessary for building the foundation for any plan of action to address radicalization of ethnic Somalis in the United States, this subject matter offers little in the way of constructive guidance as to how to achieve this goal. To find this information we must examine other sources.

2. Al Shabaab and Al Qaeda: A Dual Threat to the United States

Sources containing historical accounts of Al Qaeda’s footprint in Somalia consistently point to the early 1990s as being the time that the terrorist organization first took an interest in the region. One such source, a policy paper written by the International Crisis Group, places Al Qaeda’s emergence in Somalia between 1992 and 1995, during the United Nations humanitarian intervention in that country. (International Crisis Group, 2005, pp. 6–7) This paper examines the rise of militant Islam in Somalia as seen in the ascension of AIAI in the early 1990s and that group’s close relationship with Al Qaeda. The paper also examines the present-day tensions between Al Shabaab and the TFG in Somalia and U.S. efforts to kill or capture Al Qaeda and Al Shabaab leadership in that country. The paper’s utility to counterradicalization efforts is found in its coverage of the early years of Al Qaeda in the HOA region, as well as its examination of Al Qaeda’s continued ties to the region, and Al Shabaab specifically. The connectivity between these two terrorist organizations is the primary reason for the FBI’s concern with the radicalization of Americans and their subsequent travel to Somalia to train and fight in support of Al Shabaab.

In a hearing before the Senate Homeland Security and Governmental Affairs Committee in March 2009, FBI National Security Branch Associate Executive Assistant Director Phillip Mudd provided testimony regarding Al Shabaab's ties to Al Qaeda. Mudd specifically addressed Al Shabaab's ties to those responsible for the 1998 attacks on the U.S. embassies in Kenya and Tanzania, referring to East Africa Al Qaeda (EAAQ) facilitator Saleh Nabhan, as well as that organization's ties to the Al Qaeda leadership currently in hiding in Pakistan's federally administered tribal areas (FATA) (Mudd, 2009, p. 2). Mudd opined that Al Qaeda could be recruiting operatives to conduct terrorist operations both within and outside Somalia; while there is currently no evidence to suggest that this is occurring, the FBI remains concerned that it is a very real possibility (Mudd, 2009, p. 2). Mudd noted Al Shabaab's successful recruitment of a U.S. person (USPER) from Minneapolis, Minnesota, and his subsequent use as a suicide bomber inside Somalia in 2008 has only heightened the FBI's concern that other Al Shabaab trained USPERS could become operational within the United States (Mudd, 2009, p. 2).

Mudd's concerns were echoed by testimony given the same day by Andrew Liepman, Deputy Director of Intelligence at the National Counterterrorism Center (NCTC) who spoke to the continued interest by Al Qaeda's senior leadership in the events in Somalia. Liepman's testimony, as the head of the nation's primary intelligence fusion center, which examines the intelligence disseminated from all members of the intelligence community (IC), bolsters Mudd's testimony. Liepman's testimony further demonstrates the collective IC's fear that Al Qaeda and Al Shabaab could be planning and coordinating attacks against the homeland. As evidence to his claim, Liepman references a February 2009 video, in which Al Qaeda's second-in-command, Ayman al-Zawahiri, praised Al Shabaab, and another video in August 2008, in which Saleh Nabhan welcomes Muslims around the world to travel to Somalia, attend Nabhan's training camp, and join Al Shabaab in jihad (Liepman, 2009, pp. 4–5).

Mudd's and Liepman's testimony are derived largely from U.S. intelligence community (IC) reporting, which cannot be covered here due to classification issues, but which is supported and corroborated by media and nongovernmental organization (NGO) reporting. One such article, written by Bill Roggio and appearing in the *Long War*

Journal, discusses the recent death of Saleh Nabhan at the hands of U.S. military forces (Roggio, 2009). In that article Roggio discusses how, prior to his death, Nabhan was an unindicted co-conspirator involved in the planning of the 1998 bombing of the U.S. embassies in Kenya and Tanzania. Roggio also highlights the fact that Nabhan was additionally an active supporter of Al Shabaab who provided militaristic training to the terrorist group until his death. Reinforcing these claims is previously noted HOA expert Dr. David Shinn whose recent work outlines how Al Shabaab's current leader, Muktar Robow, continues Al Shabaab's affiliation with Al Qaeda as Robow reinforced in a 2008 statement in which he claimed that Al Shabaab receives guidance and orders from Usama bin Ladin (Roggio, 2009, p. 3). Additionally, a recent article in the *Washington Times* reported the surfacing of a video, entitled "Labaik ya Osama" in which Al Shabaab formally pledges allegiance to Osama bin Ladin (Waterman, 2009, p.1). The article goes on to address the issue of the symbiotic relationship between Al Qaeda and Al Shabaab and quotes an unnamed U.S. government official who confirms this relationship by saying, "That's why [al Shabab is] on the terrorism list" (Waterman, 2009, p. A14).

In summary, while the extent of the intertwining of Al Qaeda and Al Shabaab can be debated, there is little doubt left that the two terrorist organizations are at least engaged in an ongoing dialogue.

3. The Threat Posed by Radicalized Americans Supporting Al Shabaab

The bulk of the writing on the topic of the radicalization of Americans is found in news articles, both in print and online. These articles often lack any great depth of analysis, but they provide snapshots of the FBI's investigation of American citizens who have been radicalized and traveled to Somalia to fight alongside Al Shabaab. One recent article from the *Washington Post* noted that, while Al Qaeda is under increasing international pressure, the threat from homegrown extremists who travel abroad for jihadist training under the Al Qaeda banner is growing and represents a real threat to the United States and its allies. The article identified seven U.S. citizens who have died while fighting alongside Al Shabaab in Somalia and three additional citizens whom the FBI recently charged with terrorism violations related to those U.S. citizens' support to Al

Shabaab (Hsu, 2009). Additionally, a June 2009 *New York Times* article highlighted the radicalization of several Minneapolis Somali-American youth, including Shirwa Ahmed, the first American known to die as a suicide bomber in Somalia, and Mohamoud Hassan, among others (A. Elliott, 2009). This article was followed by a January 2010 article highlighting the path to radicalization for American citizen Omar Hammami, now known by his pseudonym Abu Mansoor Al-Amriki, or “the American,” who has become one of the best-known public faces of Al Shabaab (A. Elliott, 2010). Articles such as these make up much of the open-source information regarding Al Shabaab’s American recruits.

Rafaello Pantucci, a researcher at the Australian Strategic Policy Institute, authored a study that examined the threat posed by Al Shabaab. In that study Pantucci focused on the fear held by several countries, primarily the United States, the United Kingdom, Canada, and Australia, that radicalized and jihadist-trained ethnic Somalis will return to their home countries and carry out terrorist attacks, as has already occurred in the United Kingdom and Canada (Pantucci, 2009, p. 5). Pantucci notes that previous such attacks were self-inspired and did not require an attack order from Al Shabaab leadership (Pantucci, 2009, p. 6). In a hearing before the Senate Homeland Security and Governmental Affairs Committee in March 2009, FBI National Security Branch Associate Executive Assistant Director Phillip Mudd provided testimony in which he expressed the FBI’s concern regarding the threat posed by radicalized American citizens returning to the United States after training and fighting in jihad overseas (Mudd, 2009, pg. 2). Mudd’s sentiments were echoed by Senator Joseph Lieberman, who identified the radicalization of American citizens and their subsequent travel to Somalia to engage in jihad fighting alongside Al Shabaab as a threat to U.S. national security (Lieberman, 2009, p.6).

The preponderance of online and print articles on this subject focus on the comings and goings of suspected foreign fighters, primarily Americans, who are believed or known to be traveling overseas to train and fight alongside Al Shabaab. While many of these articles imply the threat to the United States associated with such actions of American citizens, the tenor and tone of the reporting is not yet alarmist in nature.

Nonetheless, these articles account for the majority of the unclassified reporting regarding the movement of radicalized Americans into and out of Somalia.

4. The Way Forward: Applying Counter-Gang Program Best Practices in Countering the Radicalization of Ethnic Somali-Americans

From a review of the various sources related to radicalization and the ongoing tribulations in Somalia, it appears that there are many barriers that all levels of government must overcome in order to effectively address the radicalization of the U.S. Somali diaspora. Menkhaus identified six such barriers between law enforcement outreach efforts and Somali-Americans. These barriers include Somali-Americans' distrust of law enforcement due to harsh treatment endured in Somalia at the hands of security services, the illegal status of some Somalis residing in America, Somali customary laws that conflict with U.S. laws, the Somali peoples' history of persecution, and ignorance of U.S. laws (Menkhaus, 2009, pp.13–14).

In developing a program to counter radicalization among ethnic Somalis living in the U.S., local, state, and federal government agencies should look to historical examples of law enforcement community outreach to disaffected segments of society. One prime example of such outreach efforts that have greatly contributed to the decline of crime committed by this segment of society is outreach to youth susceptible to violent gang initiation. There are numerous studies that demonstrate how active law enforcement and community outreach to disaffected, disenfranchised, and at-risk youth can greatly reduce the incidence of youth gang membership, as well as reduce the incidence of violent crime committed by youths.

One such study, written by Finn-Aage Esbensen and found in the September 2000 *Juvenile Justice Bulletin*, a product of the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention, attempts to outline methods that help communities identify youth at risk for joining gangs and then identify methods for preventing youths from joining gangs. The central tenets of the bulletin are that, while youths of various ages and from all segments and strata of society join gangs, the vast majority of youth gang members tend to be between the ages of 12 and 24 (Esbensen, 2000, p. 3) and come

from “socially disorganized and socially marginalized communities” (Esbensen, 2000, p. 9) The study more specifically defined the average youth gang member as being a “minority youth residing in single-parent households” (Esbensen, 2000, p. 4). The study further posited that any program designed to reduce youth gang recruitment and participation that only focused on one solution or approach was doomed to failure. The study pointed to the need for a multipronged approach that addressed the multiple underlying problems making youth more susceptible to gang involvement (Esbensen, 2000, p. 9).

In his comprehensive online book concerning street gangs, Dr. Mike Carlie addresses the full spectrum of issues related to gangs. Carlie examines every facet of gangs, from how and why they form, to how they recruit and maintain members, to how municipalities can combat gang violence and address the familial and societal issues that lead to gang formation and expansion. Carlie’s study draws on a massive body of work compiled by hundreds of professionals and spanning the fields of academia, law enforcement, government, and private agencies that addresses gangs of all types on a daily basis. Some of Carlie’s findings speak to the importance of healthy and stable home lives in the socialization process and the ability of Somali youths to avoid becoming involved in criminal behavior, the negative impact of the absence of positive male role models, and the lack of discipline at home as being key factors in determining whether youths will join gangs. (Carlie, 2009, pp. 2–8)

Mary H. Lees, Mary Deen, and Dr. Louise Parker of Washington State University confirm Carlie’s assertions in their review concerning gang violence and prevention. The three authors outline the reasons that youths join gangs, their risk factors for joining, and methods to prevent youths from joining gangs. Similar to the reasons cited by the authors addressing the radicalization of ethnic Somali youth in the U.S., these three authors have determined that youths most often join gangs out of a need for positive emotional reinforcement, structure, discipline, a sense of belonging, acceptance, and recognition, among other needs (Lees, Deen, & Parker, 1994, para. 2). The primary risk factors determining youth susceptibility to gang recruitment are racism, poverty, lack of a support network, and media influences (Lees, Deen, & Parker, 1994, para. 4). The 2008

U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention (OJJDP) Comprehensive Gang Model, authored by noted gang researcher Irving A. Spergel, summarizes the findings of all these authors. The Comprehensive Gang Model serves as a guide to best practices for addressing community gang problems and is based on five strategies that, when combined, allow government agencies and private-sector entities to effectively address gang problems wherever they arise nationally (United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention [USDOJ, OJJDP], 2008). This is a seminal work that thoroughly encapsulates decades of gang research and proffers a real-world-tested model for local communities to implement in an effort to address their specific gang problems.

The conclusions of these studies, primarily the demographic analyses and the corresponding socioeconomic factors identified as being at the root of gang recruitment and initiation, are nearly identical to those associated with the segment of the ethnic Somali diaspora residing in the United States, which is radicalizing and being recruited by Al Shabaab. All five individuals who testified in the hearing before the Senate Homeland Security and Governmental Affairs Committee in March 2009 provided testimony in which they pointed to the same familial and societal factors mentioned in the Juvenile Justice bulletin as being responsible for the disproportionate number of young ethnic Somali males radicalizing in the United States. Abdirahman Mukhtar, Youth Program Manager for the Brian Coyle Center, a community center in Minneapolis, Minnesota, perhaps best summarized the consensus beliefs of those providing testimony. Mukhtar attributed the rise in radicalization among young Somali-Americans to their sense of being torn between their new American identity and customs and those of their parents and grandparents who have not assimilated into American culture. Mukhtar also noted the lack of jobs for Somali youths, the relative poverty of their families, and the lack of positive male role models as all being factors allowing Somali-American youth to be susceptible to radicalization (Mukhtar, 2009, p. 3).

From this cursory examination of works addressing the issue of youth gang recruitment and participation, it is evident that there is good reason to further study the parallels between this topic and the radicalization of ethnic Somali youths residing in the

United States. By understanding and applying best practices already utilized to address youth gang recruitment and participation to the problem of radicalization, the FBI and other governmental and nongovernmental agencies could, it is hoped, increase their chances of successfully countering radicalization within ethnic Somali communities in the United States, thereby greatly reducing the threat posed by such radicalization.

THIS PAGE INTENTIONALLY LEFT BLANK

II. A STUDY OF THE UNITED KINGDOM'S COUNTERRADICALIZATION PROGRAM AND ASSESSMENT OF THE VIABILITY OF ITS APPLICATION IN THE UNITED STATES

In addressing a problem of such magnitude as radicalization, it might prove beneficial for domestic intelligence and law enforcement agencies and social welfare partners to look to foreign governments of similar construct as the United States, having similar laws and a similar appreciation of civil liberties and basic human rights, in order to identify those best practices which could, with modification, be applied here in the United States. One such foreign government counterradicalization program, the United Kingdom's (UK's) "PREVENT" program, hereafter referred to as "Prevent," shows significant promise as being a "lessons learned" resource for the United States. Currently that program is under review by the British government, and a full assessment is due in January 2011 (Home Office.gov.UK, 2010). This chapter provides the results of a study of the UK's Prevent program in an attempt to highlight both the positive and negative aspects of this program and to assess the viability of such a program in the United States.

A. THE UK'S NATIONAL COUNTERRADICALIZATION PLAN

Since 2003, the UK has had in place a comprehensive national counterterrorism strategy known as CONTEST, which is currently comprised of the following four component plans, or pillars:

PURSUE: to stop terrorist attacks;

PREVENT: to stop people from becoming terrorists or supporting violent extremism;

PROTECT: to strengthen protection against terrorist attack; and

PREPARE: where an attack cannot be stopped, to mitigate its impact. (Pursue Prevent Protect Prepare, 2009, p. 13)

Together these plans under the CONTEST umbrella seek to "reduce the risk to the United Kingdom and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence" (Pursue Prevent Protect Prepare, 2009, p. 12). This strategy grew in part out of the September 11, 2001 (9/11) terrorist

attacks in the United States, but the strategy's importance was not fully realized in the UK until a group of homegrown radicalized Muslims conducted orchestrated terrorist attacks within London's subway and city bus systems on July 7, 2005 (7/7) (Pursue Prevent Protect Prepare, 2009, p. 82). Both 9/11 and 7/7 demonstrated the continued global reach, determination, influence, and lethality of the Al Qaeda (AQ) terrorist organization and the threat posed by radicalization at the hands of militant Islamist ideologies. In 2008, UK authorities proclaimed that at any given moment they were contending with approximately 30 terrorist plots, 200 terrorist groups or networks, and 2,000 individuals that UK authorities judge to be a terrorist threat to the UK (National Security Strategy of the UK, 2008, p. 10). While such details are absent in the UK's 2010 National Security Strategy, the strategy does make clear that Al Qaeda continues to be the most significant terrorist threat to the UK, and authorities there uncover terrorist plots on a "regular basis" (National Security Strategy of the UK, 2010, p. 14). For the UK such threats highlight the importance and necessity of an overarching strategy like CONTEST. In crafting its CONTEST program, the government has made it clear that it alone cannot solve this problem but instead must have the support and participation of a diverse swath of society—including community and social groups, law enforcement, education, faith-based groups, the media and many others—and must be a cross-government program (National Security Strategy of the UK, 2010, p. 26). The CONTEST program is run by the Home Office's Office of Security and Counter-Terrorism (OSCT), which is made up of the following six directorates:

- Research, Information, and Communications Unit (RICU);
- Strategy, Planning and Change;
- Prepare, Protect, CT Science & CBRN;
- Law, Security and International;
- Communications Capabilities; and
- 2012 Olympic Safety and Security. (homeoffice.uk.gov, 2010)

In an effort to address the underlying problem of radicalization, the UK initiated in October 2007 the Prevent component of its strategy (Pursue Prevent Protect Prepare, 2009, p. 80). This program seeks to reduce popular support for terrorism and stymie

terrorist recruitment efforts among the population of the UK (Pursue Prevent Protect Prepare, 2009, p. 82)—efforts that UK authorities label as “winning hearts and minds” (Communities and Local Government [CLG], 2007). At the heart of the Prevent program is the government’s message crafted by the RICU, which was established in 2007 when the Prevent program was launched (Pursue Prevent Protect Prepare, 2009, p. 153). The RICU works to counter the violent extremist narrative of Al Qaeda and other like-minded groups through a variety of means. Perhaps the pivotal role played by RICU is its mission to help government agencies craft the content and language of their counterradicalization messages and provide an assessment of how they are likely to be received by the target audience (Pursue Prevent Protect Prepare, 2009, p. 154). In order to do this, the RICU leverages the skills of media specialists, anthropologists, pan-Arab media, marketing advisors, and other specialists (Pursue Prevent Protect Prepare, 2009, p. 154). RICU, like all UK government agencies, operates under the assumption that “contemporary terrorism is driven by an ideology and not a theology” (Pursue Prevent Protect Prepare, 2009, p. 154), but RICU understands that Muslim communities are the ones most intensely targeted by Al Qaeda and other violent extremist Islamist groups. For this reason RICU strives to promote alternative voices to the violent extremist narrative being focused at Muslim communities and works with foreign government partners in order to ensure that a shared and consistent message is passed to the global Muslim community. Following RICU’s carefully planned strategy, the UK government has publicized its intent to not betray its core values of “human rights, the rule of law, legitimate and accountable government, justice, freedom, tolerance, and opportunity for all” (National Security Strategy of the United Kingdom, p. 6), while still openly identifying the perpetuation of corrupted interpretations of Islam by violent extremists as being the nation’s primary terrorism threat (National Security Strategy of the United Kingdom, p.10).

As identified and updated in 2009, the specific objectives of the Prevent strategy over the next three years are “to challenge the ideology behind violent extremism and support mainstream voices; disrupt those who promote violent extremism and support the places where they operate; support individuals who are vulnerable to recruitment, or have already been recruited by violent extremists; increase the resilience of communities to

violent extremism, and address the grievances which ideologues are exploiting” (Pursue Prevent Protect Prepare, 2009, p. 14). Currently, the UK government finances the Prevent program to the sum of £140 million, or roughly \$200 million U.S. dollars. These monies go toward financing the numerous initiatives managed under the Prevent umbrella. A few of the more high-profile of these initiatives include the “OSCT’s efforts to remove unlawful terrorism-related content from the Internet while also working to counter the messages of violent extremists propagated on the Internet” (Pursue Prevent Protect Prepare, 2009, p. 94); the “OSCT’s creation of a ‘Young Muslims Advisory Group’, which gives a voice and a means of peacefully effecting societal change to young Muslims” (Pursue Prevent Protect Prepare, 2009, p. 90); the “efforts of local authorities working with the police under the umbrella of the ‘Channel’ program to identify youth deemed to be at risk of radicalization and then arranging for non-law enforcement, community-based interventions intended to help steer at-risk youth from the path to radicalization” (Pursue Prevent Protect Prepare, 2009,); the “government’s efforts to provide schools with resources to modify their curriculum in such a manner as to give students the tools to understand and challenge violent extremist narratives” (Pursue Prevent Protect Prepare, 2009, p. 88); and the “government’s efforts to reduce inequalities amongst the religions and races in the areas of housing, education, the criminal justice system, health, and the labor market and its endeavors to promote inter-faith harmony and shared sense of what it means to be a citizen of the U.K.” (Pursue Prevent Protect Prepare, 2009, p. 91). These are but a few of the many programs being funded by the central government, but they reflect the scope of the problem that the UK government seeks to address and the ambitiousness of the government’s response to that problem.

In trying to assess the success of the Prevent program to date, the UK government, by way of its Intelligence and Security Committee’s (ISC) 2008–2009 Annual Report, noted that it had been advised by the Home Office that progress within the Prevent program is now being measured against three key outcomes. These outcomes focus on the degree of resistance to violent extremism within UK Muslim communities, within key sectors such as universities and prisons, and within the communities of key

international partner nations (Intelligence and Security Committee [ISC], n.d., p.28). However, the ISC voiced concern over the lack of measurable progress in these efforts to date (ISC, n.d.). Supporting the ISC's concerns is the Communities and Local Government Committee (hereafter referred to as "the Committee"). Within the UK Parliament, the House of Commons maintains government oversight responsibilities and, like the U.S. Congress, has multiple committees focused on reviewing various government programs and services, one of which is the Committee. The Committee has budget, policy, and administrative oversight of the OSCT's Department of Communities and Local Government (CLG). The CLG, a UK government-created entity seeks to better society by improving public services, fostering community cohesion, and addressing malign behaviors (House of Commons, CLG, 2010), with the latter being the reason that the CLG was given program management responsibility for the Prevent program. In March 2010, the Committee, facing an increasingly unsettled and media-incited Muslim population, produced a report in which it stated, "The current overall approach to *Prevent* is contentious and unlikely ever to be fully accepted in its existing form by those it is most important to engage" (House of Commons, CLG, 2010, p. 3). The report outlined several issues that the Committee identified as being the basis for its assessment. The following represent the more contentious of these issues, as well as the Committee's recommendations as to how the government should address them.

Role of the CLG: While the Committee generally accepted the premise of, and need for, the four component elements of CONTEST (Pursue, Prevent, Protect, and Prepare), it agreed with the sentiments of those citizens it interviewed in the course of their investigation: the CLG should not be involved in Prevent, because the program has led to widespread feelings of exclusion and alienation among Muslims in the UK (House of Commons, CLG, 2010, p. 3). Consequently, the Committee recommended that the CLG's role in the government's counterterrorism agenda be reduced so that the CLG could then focus more on its role of building cohesion among and across communities (House of Commons, CLG, 2010, p. 62).

Focus on Muslims: Perhaps the most contentious of all the issues addressed, the perceived focus by the UK government on Muslims, was found by the Committee to be perhaps the single greatest impediment to the success of the Prevent program. The Committee referenced a report produced in 2005 from the findings of seven different government-initiated working groups. The working groups were comprised of members of the UK's Muslim population, who were asked in the wake of 7/7 to help the government determine the best courses of action for successfully preventing extremism. That report specifically warned that government efforts "targeting only Muslim communities would result in further stigmatizing them as being the 'problem', which could potentially lead to increased alienation whilst society at large plays little or no role in the two-way integration process" (Preventing Extremism Together Working Group, 2005, p. 48).

To date, the government has experienced difficulty in convincing a segment of the Muslim population that the government's intent is to focus on Al Qaeda-inspired terrorism and is not simply a tool for spying on all Muslims per se (House of Commons, CLG, 2010, p.11). The result of this has been that a portion of UK Muslims now harbors "feelings of alienation and stigma" while non-Muslim communities harbor resentment for Muslim communities because they are receiving government funding via the Prevent program (House of Commons, CLG, 2010, p.22). The Committee found that these factors together have kept Prevent from being able to sustain meaningful interfaith dialogue and community cohesion for the purposes of countering violent extremism (House of Commons, CLG, 2010). As a possible solution, the Committee proposed that the government consider utilizing the framework of the CLG's Connecting Communities program, which gives those communities that feel they have no voice or say in societal and government affairs a forum in which to peacefully air grievances in an effort to promote societal change (Connecting Communities, 2010). Such a program within Prevent would allow the government to continue to address at the national level the specific threat posed by Al Qaeda-inspired violent extremism, while also providing

Muslims suffering feelings of alienation and frustration a forum through which they could peacefully voice their concerns and seek reconciliation (House of Commons, CLG, 2010, p. 23).

Fears of government surveillance: Of equal contentiousness as the claims of Prevent's spotlight-like focus on Muslims alone are the allegations that the government, via Prevent, is unjustly and unlawfully surveilling law-abiding Muslims. Fanning the flames of the hysteria surrounding this issue, the Committee contends, are media reports that sensationalize the issue. One such article, which the Committee referenced, points to a government-funded youth center in which the government sought to contain free Internet access so that it could monitor the websites visited by the youth (House of Commons, CLG, 2010, p. 12). While a subsequent government investigation into these allegations found no evidence to support the claims, the damage had nonetheless already been done, and the idea that the government sought to spy on Muslims was already etched into the psyche of the Muslim populace. In defense of government efforts to promote community-based outreach to persons susceptible to radicalization and violent extremist messages, one of the panelists consulted by the Committee for its report highlighted the case of former UK citizen Hasib Hussain, who died while perpetrating the 7/7 attacks. Prior to his death, Hussain, by all accounts, was an average UK citizen except for his apparent interest in and support for Al Qaeda, as evidenced by his scribbles on his school books. The panelist opined that the outcome of 7/7 could have been different had someone conducted outreach to Hussain prior to his becoming a suicide bomber. The Committee, itself unsure as to how the government could dispel public fears of government spying of Muslims, ultimately recommended that the government commission an independent investigation into the allegations (House of Commons, CLG, 2010, p.18).

In the end, the Committee found that, while the Prevent program was necessary and has been effective to some degree, it has in many cases had the opposite effect from that intended by the government. In addition to recommendations for addressing the problems identified in the preceding paragraphs, the Committee emphasized the need for greater local government control of Prevent funding but less involvement of local

government community outreach agencies in the counterterrorism agenda (House of Commons, CLG, 2010, p. 67). Additionally, the Committee found that there needed to be “greater clarity as to what the programme aims to achieve” and a “proportionate and risk-based approach to delivering Prevent” before much-needed performance measures can be adopted by the government (House of Commons, CLG, 2010, p.66). It is clear that the Committee’s findings and recommendations were heavily influenced by sentiments of anger, outrage, and alienation emanating from the UK’s Muslim population. Did the Committee then cave to the overwhelmingly negative response from the Muslim populace? The truth is complicated and nuanced, but it is evident that the government’s negative assessment of its own Prevent program was shaped by public perception.

B. THE VIABILITY OF THE UK PREVENT MODEL’S APPLICATION IN THE UNITED STATES

In assessing the viability of enacting a UK Prevent-like program within the United States, we must examine the experiences of the UK and endeavor to avoid Prevent’s shortcomings and pitfalls. In doing this, we must acknowledge that, while there are many similarities between the two nations, there are also substantial differences that must be considered. Examining first the similarities, both the UK and the United States have a representative forms of government—the UK having a democratic constitutional monarchy, and the United States a democratic representative republic. Both have increasing populations due in large part to growing immigrant diasporas. Both are free-market economies engaged in international trade and therefore dependent upon positive foreign relations with nation-state trading partners and their diaspora populations residing within their borders. Both have robust legislatures that have enacted dynamic laws intended to protect their citizenry from terrorists and terrorist acts. Our nations’ commonalities are perhaps best captured in a description of UK society found in the UK’s National Security Strategy 2009 update;

We have a markedly pluralistic society, with a tradition of open debate supported by a lively free press, and a very long-standing tradition of the rule of law. We have a strong belief in values which should guide our

government's actions. But we also have a tradition of individualism which means that our values and identity are not easily captured in a single narrative. (p. 38)

Despite these similarities, however, there are differences that could make the implementation of many elements of the PREVENT program difficult in the United States.

One difference is the way in which Muslims are treated and are, or are not, assimilated into the native culture. American Muslims occupy predominantly the middle class, whereas 20 percent or more of European Muslims live in poverty (PEW Research Center, 2007, p. 54) and suffer from a “failed integration” (Ruffer, 2008). This “failed integration” seems to largely have its roots in the way in which Muslims are, or are not, embraced by their host nation. European nations, whether fairly or not, are perceived as displaying national biases which exclude anyone who does not reflect the image of the individual nations (i.e., Englishness, French-ness, etc.), whereas the United States still enjoys its “melting pot” image in the eyes of the world (Sageman, 2007, p. 2). Perhaps the most notable difference between the United States and the UK, however, is that the UK's system of constitutional monarchy allows for much greater national government direction and control of a program such as Prevent, whereas the federal system of government in the United States empowers the states to largely govern themselves, while traditionally limiting the role of the federal government to only those duties not assumed by the states. In the UK the national government has been able to implement the Prevent program with little resistance from the kingdoms and localities within the UK, and in fact it has enjoyed widespread acceptance and embrace of the program. In the United States such federally directed and led implementation of Prevent would meet with substantial resistance from the states if such a program were not methodically coordinated beforehand. Even then, there is no guarantee that the federal government could secure the acceptance of all 50 states. In order to obtain the support and participation of the states, the federal government would likely be required to provide funding to assist the states in implementing a counterradicalization program and would additionally need to clearly demonstrate how such a program would benefit the states and their citizenry. This could be done, and should be done, by demonstrating how a well-structured

counterradicalization program could be utilized to address at-risk youth from across a wide spectrum of socioeconomic and cultural backgrounds that are susceptible to adopting violent antisocial behaviors of all kinds—not just violent Islamist extremist behavior. States will want to participate in such a program because it will help them provide much-needed social services to their citizenry and will, when applied properly, affirmatively address violent criminal behavior stemming from real and perceived socioeconomic inequalities among the population. Obtaining the consensus of the states will prove to be one of the greatest hurdles the federal government will face when implementing a U.S. counterradicalization program. However, by focusing on the benefits of such a program—including improved social services to the respective constituencies of the states, federal funding streams for all counterradicalization programs and services, and improved security through the targeted reduction of radicalization and its negative side effects—it is feasible that the federal government could obtain the buy-in of the states.

Once the federal government has the states' acceptance of the program, it must then work to provide specific and detailed guidance regarding implementation. This will likely prove taxing due to the sheer complexity of implementing such a massive cross-government program servicing the immense U.S. population. Unlike the UK, which has approximately 50 law enforcement agencies (Association of Chief Police Officers, 2010), serving a total population of approximately 62 million people (Office for National Statistics, 2010), the United States has approximately 17,000 law enforcement agencies (Federal Bureau of Investigation, 2010), serving a total population of approximately 309 million people (U.S. Census, 2010). The staggering numbers of both law enforcement agencies in the United States (not to mention the bevy of other local, state, and private sector agencies) and the civilians that they serve and protect makes a nationally designed and locally applied program like Prevent a daunting task. The federal government must drive the counterradicalization message via a RICU-like entity that formulates the countermesssage and then assists the states with adapting the message so that it reaches the widest possible audience within each state's diverse population. Working together, however, this can be accomplished in the same way that other federally initiated and

state-managed social-welfare programs, such as Medicaid, have been accomplished. The immense geographic and population size of the United States need not be an impediment to implementation of a successful counterradicalization program.

Similar to the UK's stance that "the most significant international terrorist threat to the UK continues to come from groups who claim to act in the name of Islam and who try to recruit people of Muslim faith to the cause of violent extremism" (Pursue Prevent Protect Prepare, 2009, p. 12), the previous U.S. presidential administration identified violent ideologies that "twisted" Islam to serve its own terrorist goals (National Security Strategy of the United States, 2006, p.12) as being the gravest threat to the national security of the United States. However, the current administration is reticent to associate Islam with terrorism (Apuzzo, 2010) and has engaged in proactive outreach to Muslim communities in both the United States and abroad in an attempt to dispel the notion that the United States is at war with Islam (White House, 2009). Given the administration's aversion to linking terrorism with radical Islam or violent Islamist extremists, it is likely that a phased approach will be required when acclimating the American public to the dangers associated with radicalization. Although the UK and the United States currently differ with regard to the language they utilize in describing the threat posed by radicalization, nonetheless they each acknowledge that it is a very real threat to national security. By studying and learning from the UK's Prevent program, the United States will be better positioned to avoid such issues as perceived government spying on, and undue focused scrutiny of, law-abiding Muslims. The establishment of a robust RICU-like organization that manages the national counterradicalization message will likewise be key in ensuring the viability of the government's program. The number of media outlets in the United States is exponentially larger than in the UK, a fact that will make it all the more important that the government make it clear that the media is an integral part of the solution to the problem of radicalization and has a duty to help educate, as well as to inform the public. This can be accomplished as long as the government ensures that its message is consistent and focused on empowering communities to help at-risk youth and others susceptible to those peddling messages of hate and violence.

C. CONCLUSION

In summation, it is entirely feasible that a Prevent-like program could be applied within the United States so long as the states and their component agencies are brought in early to the planning and coordination of such a program. There will be a need for collective discussions as to how the counterradicalization message will be crafted, what it will be, and how it will be disseminated. Additionally, the media's assistance will need to be formally enlisted to help with what will be a massive information campaign. The focus of such a campaign would be educating the public about the objective of the program—which is to empower communities to reject violent extremism—and in so doing helping to protect Americans from future terrorist attacks.

III. COUNTERGANG BEST PRACTICES

Street gangs are an amalgam of racism, of urban underclass poverty, of minority and youth culture, of fatalism in the face of rampant deprivation, of political insensitivity, and the gross ignorance of inner-city (and inner-town) America on the part of most of us who don't have to survive there.

-M. W. Klein

Having examined the counterradicalization practices instituted in the United Kingdom, a nation of similar governmental and social construct as the United States, and having observed the both the benefits and pitfalls of such a program, let us now examine how the United States has dealt with a similar social problem—the problem of youth gangs. Such an examination may allow us to ascertain what practices, if any, can be applied. For nearly 100 years, gangs have existed in one form or another in the United States, but gangs as we understand them today came to the forefront of the criminal world within the last 50 years. In this period of time, law enforcement and social welfare organizations have developed methods of addressing this problem—some effective and some not. However, within the last decade there has arisen a set of countergang best practices, that might be suitable with modification for application to the problem of radicalization among the ethnic Somali-American populace, thus avoiding the need to “reinvent the wheel” when creating a counterradicalization program.

A. A “GANG” DEFINED

In analyzing countergang best practices, it is important to note that there are several different types of gangs. The 2009 National Gang Threat Assessment (NGTA), prepared by the U.S. Department of Justice-Sponsored National Gang Intelligence Center, identifies three basic types of gangs: street gangs, prison gangs, and outlaw motorcycle gangs, with street gangs being the most prevalent (National Gang Intelligence Center, 2009, p. 7). Street gangs are further broken down into three subgroups: national-level, regional-level, and local street gangs. Local street gangs are in turn predominantly comprised of youth gangs (National Gang Intelligence Center [NGIC], 2009, p. 7). In this context youth gangs are defined as having more than two members who are between the

ages of 12 and 24, sharing a sense of identity, have been in existence for a year or more, and are involved in criminal activity (Esbenson, 2000, pp. 2–3). Due to the fact that street gangs represent the broadest set of gang membership and also best mirror the demographic of Somali-American's current radicalizing of ages 17 and 27 (Ephron & Hosenball 2009), countergang programs targeting such gangs are the most useful for purposes of comparison with potential counterradicalization practices. In Chapter IV we will examine further the demographic within Somali-American communities that is most susceptible to radicalization and Al Shabaab recruitment.

B. A BRIEF HISTORY OF GANGS IN THE UNITED STATES

While the exact origins of youth gangs in the United States are unclear, it is known that in the 1800s during the Industrial Revolution there was a proliferation of youth gangs (largely made up of members from multiple immigrant diasporas) throughout New England, which may have arisen due to the difficult urban conditions of industrialized America (Howell, 1998, p. 2). Since that time the United States has experienced three additional periods of gang expansion, with the most recent period occurring in the 1990s (Howell, 1998). Early gang research described gangs in terms of nationality and/or ethnicity versus race-based descriptors until around the 1950s (Esbensen, 2000, p. 4). Historically, gangs were made up of members who were almost exclusively males residing in the inner city and who were members of an ethnic or racial minority (Esbensen, 2000, p. 3). While current data demonstrate that gangs have migrated in recent years from urban areas to suburban areas and even rural communities (NGIC, 2009, p. iii), the data also suggest that a majority of gang members are still from racial and ethnic minorities (Ogletree, 2008, p. 41). The exact number of youth gangs in the United States is not known; however, the 2009 National Gang Threat Assessment estimated that there were approximately 1 million gang members belonging to more than 20,000 criminally active gangs within the United States, and 58 percent of state and local law enforcement agencies reported having active criminal gangs in their jurisdictions (NGIC, 2009, p. iii).

C. COMMUNITY MOBILIZATION INITIATIVES

In the last three decades there have been numerous countergang programs and initiatives applied to addressing the issue of criminal gangs in the United States. A study commissioned by the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Programs (OJJDP) in 2000 examined the history of these programs. This study notes that modern countergang efforts began with programs that simply attempted to prevent youth from joining gangs, but by the mid-1930s these efforts had transitioned to programs that sought to organize and mobilize communities in an effort to reduce crime and to counter gang formation (Howell, 2000, p. 5). This is due to the widespread acceptance of the notion that cohesive, organized, and engaged communities were the key to reducing crime as well as mitigating gang problems since the social environment and not the individual were the cause of maladaptive behavior—a concept known as “social disorganization” theory (Esbensen, 2000, p. 6).

What is perhaps the best known delinquency prevention program in the United States to date (Esbensen, 2000)—the Chicago Area Project (CAP)—was established in 1934 by two early gang researchers, Clifford Shaw and Henry McKay, who, following social disorganization theory, directed the implementation of CAP (Howell & Curry 2009, p. 2). The goal of CAP was to reintegrate gang members into society through such methods as the use of “detached workers,” who were members of a government agency or government-sponsored agency, assigned to embed within local gangs where they could more directly counsel gang members in an attempt to reintegrate them into society (Howell & Curry, 2009, p. 2). Additionally, CAP engaged preexisting community groups, such as church groups and labor unions (Esbensen, 2000, p. 6) in an effort to improve the conditions in neighborhoods, including offering afterschool programs and other activities in an effort to fill youths’ time with positive activities and divert them from entering gangs (Esbensen, 2000). CAP spawned numerous other similar programs in other cities in other states. However, subsequent research called into question the efficacy of the detached-worker concept due to the fact that such programs focused

almost solely on affecting individual behavior, while at the same time failing to address shortcomings in community structure and capacity (Esbensen, 2000, p. 7), the concept at the heart of social disorganization theory.

As countergang efforts progressed, a transition occurred in which law enforcement, with the support of legislative initiatives, began to initiate suppression programs designed to target areas with high gang concentrations for intensified enforcement efforts (Howell, 2000, p. 5). While enforcement activities are an essential aspect of any effective countergang program, such activities only treat symptoms and do not address shortcomings in a community's structure or capacity; thus they cannot be expected to be the sole solution to the problem (Esbensen, 2000, p. 7). Today, many jurisdictions prefer to adopt programs incorporating aspects of these and other countergang approaches (Esbensen, 2000, p. 7). These approaches can be separated into seven distinct types of programs: prevention, intervention, suppression, multiple technique programs, multiagency programs, comprehensive programs, and legislative initiatives (Esbensen, 2000, p. 7).

Of the recommendations cited in the 2000 OJJDP study, which examined the implementation of these types of programs within multiple jurisdictions across the nation, two of the cited recommendations are the most relevant for the purpose of addressing the problem of youth radicalization within Somali-American communities. The first recommendation is that all elements of a community, not just law enforcement, should work together to address this problem. The second recommendation is that communities must provide gang members with alternatives to being in a gang, since no consistently successful program for preventing youth from joining gangs has yet been identified. Those programs which have thus far shown great promise involve helping youth with family, peer, and school problems, as well as community conditions (Howell, 2000, p. 54). Further, the 2000 OJJDP study examined a 1995 national gang migration study in which respondents from 211 surveyed cities assessed the effectiveness of multiple countergang practices (Howell, 2000, p. 46). The results showed that nearly two-thirds of cities surveyed utilized some type of community engagement strategy, and 54 percent found such practices to be effective, as the table below illustrates (Howell, 2000, p. 46).

Table 1. Law Enforcement Strategies and Perceived Effectiveness

Strategy	Used	Judged Effective (if used)
Some or a lot of use		
Targeting entry points	14%	17%
Gang laws	40	19
Selected violations	76	42
Out-of-State information exchange	53	16
In-State information exchange	90	17
In-city information exchange	55	18
Federal agency operational coordination	40	16
State agency operational coordination	50	13
Local agency operational coordination	78	16
Community collaboration	64	54
Any use		
Street sweeps	40%	62%
Other suppression tactics	44	63
Crime prevention activities	15	56

^a Percentage of cities, *n*=211. The number of cities responding to each question varied slightly.

Source: Maxson, Woods, and Klein, 1995.

Source: Howell, 2000, p. 46.

The aforementioned 2000 OJJDP study concluded that the most effective counter-youth gang program will likely prove to be a combination of strategies, including prevention, intervention, and suppression, initiated in a collaborative, community-engaging fashion (Howell, 2000, p. 55).

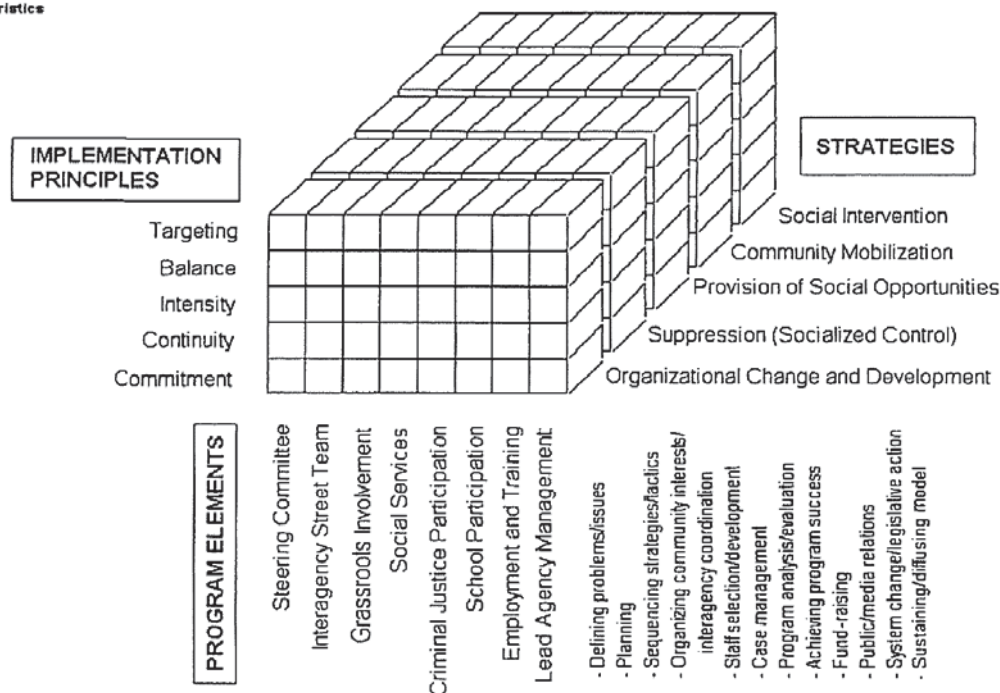
Contemporary countergang strategies, as well as the aforementioned 2000 OJJDP gang study, reflect the research and field work of noted gang researcher and University of Chicago sociologist and professor, Dr. Irving A. Spergel, who has spent more than three decades studying the problem of gangs and their negative effects on society. A prolific writer on the topic of gangs, Dr. Spergel is perhaps most renowned for what is now known as the “Spergel model” (2010 Canada, 2010, p. 9), or the “community-wide, comprehensive gang program model,” which the U.S. Department of Justice adopted and renamed simply the “comprehensive gang model.” Key assumptions of the model are that the youth gang problem is the result of fragmented communities and the failure of public agencies in those communities to tend to the social development needs of youth and that youth gangs are generally attractors of youth “between childhood and adulthood,

particularly youth from disorganized or deviant families in socially and economically marginal neighborhoods (Spergel, Wa, & Sosa, 2006, p. 203).

Dr. Spergel, with DOJ funding, first implemented his comprehensive gang model in Chicago's Little Village neighborhood in a program that lasted from 1992 to 1997 (Spergel, Wa, & Sosa, 2006, p. 203). This first implementation of the model suffered from several catastrophic failures, including the local police department's lack of interest in entering into joint relationships with other key program agencies and community groups and, perhaps most damningly, the ultimate dissolution of the crucial neighborhood advisory group, due largely to petty squabbling and the inability to communicate effectively (Spergel, Wa, & Sosa, 2006, p. 211). The neighborhood advisory panel, consisting of members from several local places of worship, Boys and Girls clubs, a community organization, social welfare agencies, local residents, the local alderman, and a business group, were key elements of the comprehensive countergang program and the failure of these elements to work together for the betterment of the community was cited as one of the primary reasons why the Little Village program did not achieve its full potential in countering youth gang formation and gang violence (Spergel, Wa, & Sosa, 2006, p. 217). Despite the failure of the Little Village community to fully implement all strategies and program elements of the comprehensive, community-wide gang program model, the program nonetheless demonstrated the necessity of, and power of, community engagement and mobilization.

Community Context
Social Disorganization Factors:

- Demographic
- Socioeconomic
- Family Characteristics
- Ecological
- Cultural



Source: Spergel, Wa, & Sosa, 2006, p. 206

Figure 1. Comprehensive Gang Program Model

Following the implementation of the Little Village program, OJJDP conducted a demonstration to measure the effectiveness of the comprehensive gang model and initiated the program in five separate localities across the United States from 1995 to 2000. The results from those five sites—Mesa, Arizona; Riverside, California; Bloomington-Normal, Illinois; San Antonio, Texas; and Tucson, Arizona—were combined with the results of the Little Village program (Table 2). The outcome showed three of the six localities making significant planning mistakes that kept them from seeing positive results. The other three localities experienced reductions in both gang violence and drug-related offenses due to their successful implementation of programs focusing on prevention, intervention, and suppression (USDOJ, OJJDP, 2008, p. 44). However, the study made clear the fact that when communities come together collectively to address a shared problem, they are more likely to enjoy success than they would working in an uncoordinated fashion.

Table 2. Effectiveness of Comprehensive Gang Model

Program Implementation Characteristics		Degree of Importance to Program Success [†]	Levels of Implementation by Project Site [‡]					
			Chicago	Mesa	Riverside	Bloomington-Normal	San Antonio	Tucson
Program Elements (Structure)	City/County Leadership	***	2	4	4	1	1	1
	Steering Committee	**	1	4	3	1	1	0
	Interagency Street Team/Coordination	***	4	4	3	0	0	0
	Grassroots Involvement	*	3	1	1	0	1	0
	Social Services: Youth Work, Individual Counseling, Family Treatment, and Recreation	**	3	3	3	2	3	3
	Criminal Justice Participation	***	4	4	4	1	1	0
	School Participation	**	1	3	3	3	2	0
	Employment and Training	**	3	1	4	3	1	0
	Lead Agency/Management/Commitment	***	4	4	4	0	0	0
Strategies	Social Intervention: Outreach and Crisis Intervention	**	4	3	3	1	1	0
	Community Mobilization: Interagency and Grassroots	**	1	3	2	1	0	0
	Provision of Social Opportunities: Education, Job, and Culture	**	3	2	2	2	1	0
	Suppression	***	4	4	3	0	0	0
	Organizational Change and Development	***	2	4	4	0	0	0
Operating Principles	Targeting Gang Members/ At-Risk Gang Youth	***	4	2	3	1	3	3
	Balance of Service	***	4	3	3	0	0	0
	Intensity of Service	*	4	3	3	1	0	0
	Continuity of Service	**	2	1	2	2	0	2

Source: Spergel, Wa, and Sosa, 2006, pp. 216–217

[†]Importance of characteristic to success: ***=extremely, **moderately, *=somewhat

[‡]Levels of implementation: 4=excellent, 3=good, 2=fair, 1=poor, 0=none

The 2008 U.S. Department of Justice’s Office of Juvenile Justice and Delinquency Prevention (OJJDP) Best Practices to Address Community Gang Problems encapsulates, supports, and summarizes the findings of Dr. Spergel’s work, as well as the OJJDP’s 1995–2000 implementation of Dr. Spergel’s comprehensive, community-wide gang program model. The OJJDP has sought, through multiagency collaboration across all levels of government, to replace the false promise of “safety, belonging, economic opportunity, and a sense of identity” (USDOJ, OJJDP, 2008, p. iii) that gangs use to lure recruits. Based on decades of analysis of the gang problem, primarily strategies developed largely through the research and field work of Dr. Spergel, the OJJDP’s formula for success is based on five strategies that when combined allow government

agencies and private-sector entities to effectively address gang problems wherever they arise nationally. The five strategies are community mobilization, opportunities provision, social intervention, suppression, and organizational change and development.

Community mobilization entails leveraging the involvement of the citizenry, including rehabilitated gang members, community organizations, and government agencies in addressing gang recruitment and initiation, and also coordinating and synchronizing programs across all participating agencies (USDOJ, OJJDP, 2008, p. 2). The opportunities provision entails developing tailored training, education, and employment programs to provide gang-involved youth alternatives to gang participation (USDOJ, OJJDP, 2008, p. 2). Social intervention entails conducting outreach to, and providing services to gang-involved youth and their families with the assistance of youth-serving agencies, faith-based organizations, schools, grassroots organizations, law enforcement, and other juvenile/criminal justice organizations (USDOJ, OJJDP, 2008, p. 2). Suppression entails utilizing a system of both formal and informal social control procedures to address gang violence and other criminal activity. Formal procedures might include community-oriented policing-style gang suppression operations, while informal procedures could include monitoring and supervision of gang-involved youth by juvenile/criminal justice agencies, community-based agencies, schools, and grassroots organizations (USDOJ, OJJDP, 2008, p. 2). And finally, organizational change and development entails maximizing the effective utilization of available resources by developing and implementing dynamic and forward-thinking policies and procedures within and across participating agencies (USDOJ, OJJDP, 2008, p. 2).

Implementation of these strategies can come after a community experiences a tragic event, such as a gang-related death or other violence that shocks the conscience, but it can also occur in the absence of any such catalyst and can be merely the result of a gradual building of public support to address a gang problem (USDOJ, OJJDP, 2008, p. 6). In whatever fashion a community comes together to address its gang problem, the community's next step toward addressing the problem is the convening of an organizational structure (identified by OJJDP as a steering committee) to plan and coordinate community response efforts (USDOJ, OJJDP, 2008, p. 6). Experience has

demonstrated that successful implementation of the comprehensive, community-wide gang program model is determined by the effectiveness of the steering committee (USDOJ, OJJDP, 2008, p. 6), which works best when made up of a mix of upper-level management from participating agencies, as well as influential individuals from the community, including residents, grassroots community group representatives, neighborhood associations, faith-based organizations, and advocacy groups (USDOJ, OJJDP, 2008, pp. 6–7).

The OJJDP’s comprehensive gang model outlines five steps through which communities should implement the aforementioned five core strategies in order to address a gang problem. Step one: the community, including community leadership, acknowledges the existence of a youth gang problem (USDOJ, OJJDP, 2008, p. 3). Step two: the community assesses the scope of its gang problem (USDOJ, OJJDP, 2008, p. 3). Step three: the community, through a steering committee, sets goals and objectives to address the problem (USDOJ, OJJDP, 2008, p. 3). Step four: the steering committee provides the community with relevant programs, services, and strategies to address the problem and does so in a manner consistent with the aforementioned five core strategies (USDOJ, OJJDP, 2008, p. 3). And finally step five: the steering committee evaluates the effectiveness of the community’s response to the problem and makes modifications to the program as required (USDOJ, OJJDP, 2008, p. 3).

In order to test its comprehensive gang model, in 2003 OJJDP implemented the Gang Reduction Program (GRP) in four U.S. cities: Los Angeles, California; Milwaukee, Wisconsin; North Miami Beach, Florida; and Richmond, Virginia (USDOJ, OJJDP, 2008, p.3). The GRP sought to assist communities in addressing their gang problems by teaching those communities to utilize the five core strategies derived from Dr. Spengel’s body of work regarding gangs. In each of the cities, the GRP model was modified so as to be most effective in addressing the unique “local needs and problem-solving approaches” of that locale (Cahill et al, 2008, p. 356). The findings from that study were compiled and presented in 2008 by the Urban Institute’s Justice Policy Center in coordination with the OJJDP. With regard to community engagement and collaboration, the study found that there was successful steering committee formation and function, including program

planning and implementation, at all of the program sites, which as previously noted is a criterium for successful implementation of the comprehensive gang model (Cahill et al, 2008, p. 359). And while the study found varying levels of collaboration and communication among program participants, with agencies focusing on suppression strategies collaborating more quickly and more closely at the start than did agencies focusing on the intervention and outreach strategies, in the end those individuals and agencies comprising the community engagement and outreach arm of the GRP improved their levels of communication and collaboration (Cahill et al., 2008, pp. 359–60).

D. CONCLUSION

The last two decades of gang research and countergang program testing has demonstrated that the most effective counter–youth gang program will likely prove to be a combination of strategies, including prevention, intervention, and suppression, initiated in a collaborative, community-engaging fashion (Howell, 2000, p. 55). Fortunately, this fact has been recognized by our national leadership. The Honorable Robert C. Scott, Chairman of the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, U.S. House of Representatives of the 110th Congress, in addressing a 2007 hearing on effective countergang practices spoke to the need for a “continuum of services for youth” involving the educational, law enforcement, social welfare, mental health, not-for-profit, business, and faith-based sectors working together (Scott, 2007, p. 3). Similarly, in 2008, the U.S. House of Representatives held one of several hearings in which it heard from numerous expert witnesses in the field of gang research, as well as gang suppression, who testified regarding what constitutes an effective practice for addressing gangs. Referenced in that hearing was a study in which three common characteristics of programs that successfully address gangs and gang violence was identified. These characteristics can be found repeated throughout the extensive body of work concerning gangs and have come to be accepted almost as universal truths. The first of these characteristics of successful countergang programs is their inclusion of families, schools, and other components of communities (Ogletree, 2008, p. 12). Only with the inclusion of these elements of the community can a program be truly successful. The second characteristic of successful countergang programs is their

focus on individual development, especially teaching youth social and cultural skills needed by youth in order for them to be effective and contributing members of their community (Ogletree, 2008, p. 12). The third and final characteristic of successful countergang programs is that they begin in preschool and continue throughout primary and secondary education. Such programs have shown that they are effective in reducing criminal behavior among male youth—especially those from economically challenged families (Ogletree, 2008, p. 12).

Why then are such programs often not implemented, or if implemented why are they not always successful? There are many reasons why a particular countergang program might not be initiated, or perhaps ultimately fail if initiated. These reasons can range from the failure of a community to recognize its gang problem, the failure of communities to effectively communicate and collaborate in the planning or implementation phases of a countergang program, or the failure of government agencies to focus adequate resources on the gang problem, to name only a few. Unfortunately, authorized funding from Congress for countergang programs is typically not provided in full and has been declining in recent years (Scott, 2007, p. 1). Additionally, many of those programs that do receive funding, at both the national and local levels, are unproven programs with questionable methodologies and outcomes (D. Elliott, 2007, p. 8).

The fact that many U.S. communities have yet to implement the comprehensive gang model and the fact that several of those communities that have implemented the model have not fully solved their gang problem need not be reasons to abandon examination of this model as a viable method for addressing radicalization occurring within Somali-American communities. The comprehensive gang model, if accepted, modified, and then applied to a program addressing radicalization among ethnic Somali males, who are generally of the same demographic as youths most susceptible to gang recruitment, would not only save the government valuable time in addressing this threat but might serve to help Somalis better assimilate into American culture. Perhaps a test case in one American city containing an ethnic Somali enclave might serve to establish the effectiveness of such a program in reducing the sense of non-belonging that many

second-generation Somali youth harbor; this is a topic that will be discussed in greater depth in Chapter IV. By reducing or eliminating this sense of non-belonging, it may be possible to reduce the risk of radicalization and Al Shabaab recruitment among these youth.

The general consensus of gang researchers and experts is that the gang problem requires national-level funding and direction, but local, community-based solutions (Howell & Curry, 2009; Esbensen, 2000; Spergel, Wa, & Sosa, 2006; Fernandez, 2007, p. 49). Further, study after study reiterates the need that countergang programs focus not only on correcting individual behavior through multiple community-based intervention programs, but also that such programs work to reshape the communities, including the families, in which gang members live (Esbensen, 2000, p. 7; Hill, Liu, & Hawkins, 2001, p. 3; Kennedy, 2007, p. 33). This is not only because gangs are the by-products of fractured families and communities (Esbensen, 2000, p. 7), but more importantly because gangs are more likely than not to come from “socially disorganized or marginalized communities” (Esbensen, 2000, p. 9).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

For the early gang researchers, the quest for an understanding of urban gangs began when researchers started following peasants and sharecroppers into cities. Thus, immigration and the experiences of immigrants adapting and adjusting to city life form the basis for all else that follows, including and especially the maladaptation that so often occurs among them. In this vein, there are multiple areas in which immigrants and especially their children find themselves betwixt and between, beginning with where they settle, what jobs they fill, and how and why their social and cultural values and practices are challenged and typically undermined and revamped. It also takes into account when the social environment shapes personal identities with whom the individuals interact. As noted above, no more than 10% of the youths become gang members in most affected neighborhoods, and the most marginalized families and children in each of these neighborhoods tend to fall into this category.

-J. D. Vigil

So what causes the radicalization of a small but significant number of Somali-American youth? The answer is complex: sophisticated extremist recruiters target vulnerable individuals, young men—many of them refugees who came here as small children or who are children of immigrants—torn between their parents’ traditional ethnic, tribal, and clan identities and the new cultures and traditions offered by American society. Caught between two worlds, and lacking structure and definition in their lives at home, some youth become susceptible to the draw of gangs and criminality, and in some cases religious or nationalistic extremism.

- Andrew Liepman

The above quotes, the first concerning the problem of gangs in the United States and the second concerning the problem of radicalization and Al Shabaab recruitment in the United States, both speak to the trials and tribulations that certain communities in this country have experienced as a result of their migration, or their ancestors’ migration. The two problem sets interestingly share numerous commonalities. Both problem sets demonstrate a propensity to attract youth, especially male youth from socioeconomically

challenged communities, who must fight against social and cultural norms that are often in conflict with those of their families and or communities—an issue to be examined in this chapter.

In Chapter II we examined the efforts of the government of the United Kingdom to counter radicalization primarily among its Islamic population. If we are to accept that the UK counterradicalization practices would not be acceptable given the much greater size of the United States' populace, its more decentralized federal system of government, its corresponding exponentially greater number of law enforcement and intelligence agencies that would need to be involved, as well as the politically unpalatable nature of such a program as PREVENT, singularly focused on Muslims, then we must look to other methods to counter radicalization occurring among Somali-Americans. In Chapter III we examined the problem of youth gangs in the United States and a corresponding set of best practices that have been adopted by the U.S. Department of Justice as being the nation's best hope of countering youth gang formation. In this chapter we will examine both the socioeconomic drivers of youth gang formation and the socioeconomic drivers of radicalization and Al Shabaab recruitment occurring among Somali-American youth. Such a juxtaposition is intended to illuminate the similarities of the socioeconomic drivers of both problem sets, thereby making a case for the need to conduct a test-case study of the application of identified countergang best practices against the problem of Somali-American radicalization and Al Shabaab recruitment.

A. SOCIOECONOMIC FACTORS CONTRIBUTING TO YOUTH GANG RECRUITMENT

For as long as communities and governments have sought to combat gangs and gang crime, there have been theories proposed and studies initiated to identify the reasons that youth join gangs. The findings point to a range of causes, from lack of societal integration, racism, poverty, and political isolation. While these factors alone cannot be said to be the sole indicators of potential gang affiliation, gang-study findings indicate that minority youth from single-parent households are at greater risk for joining gangs than are their counterparts from Caucasian two-parent households (Esbensen, 2000, p. 4). Lending credence to this statistic is the work of renowned family therapist Michael

Gurian, who has studied the troubling contemporary trend of male youth scholastically falling behind females of the same age. Gurian points to the lack of positive male role models as a primary reason for the learning gap between the genders, especially when examining male youths in the junior-high-school and high-school age range (Tyre, 2006). Gurian notes that boys learn healthy work habits and self restraint from older male role models (Tyre, 2006), and in the absence of such role models, young males easily fall prey to negative influences.

In American society today 40 percent of boys are raised in the absence of their biological fathers, and more than half of African-American males who begin high school never graduate (Tyre, 2006). Social ecologist James D. Vigil supports the theory of the negative effects of absentee positive male role models and offers additional explanation as to why certain youth join gangs. Vigil notes that the typical age range of youth involved in violent gang activity is the very age range in which youth are transitioning from childhood to adulthood; this is a time typically characterized by ambivalence and unpredictability, and for many teenagers living in stressful conditions, it is an especially difficult stage in their development (Vigil, 2003, p. 227). Beyond the lack of male role models, gang researchers point to socioeconomic deprivation, especially among urban youth, as being one of the leading predictors of youths susceptible to gang recruitment (Esbensen, 2000, p. 5).

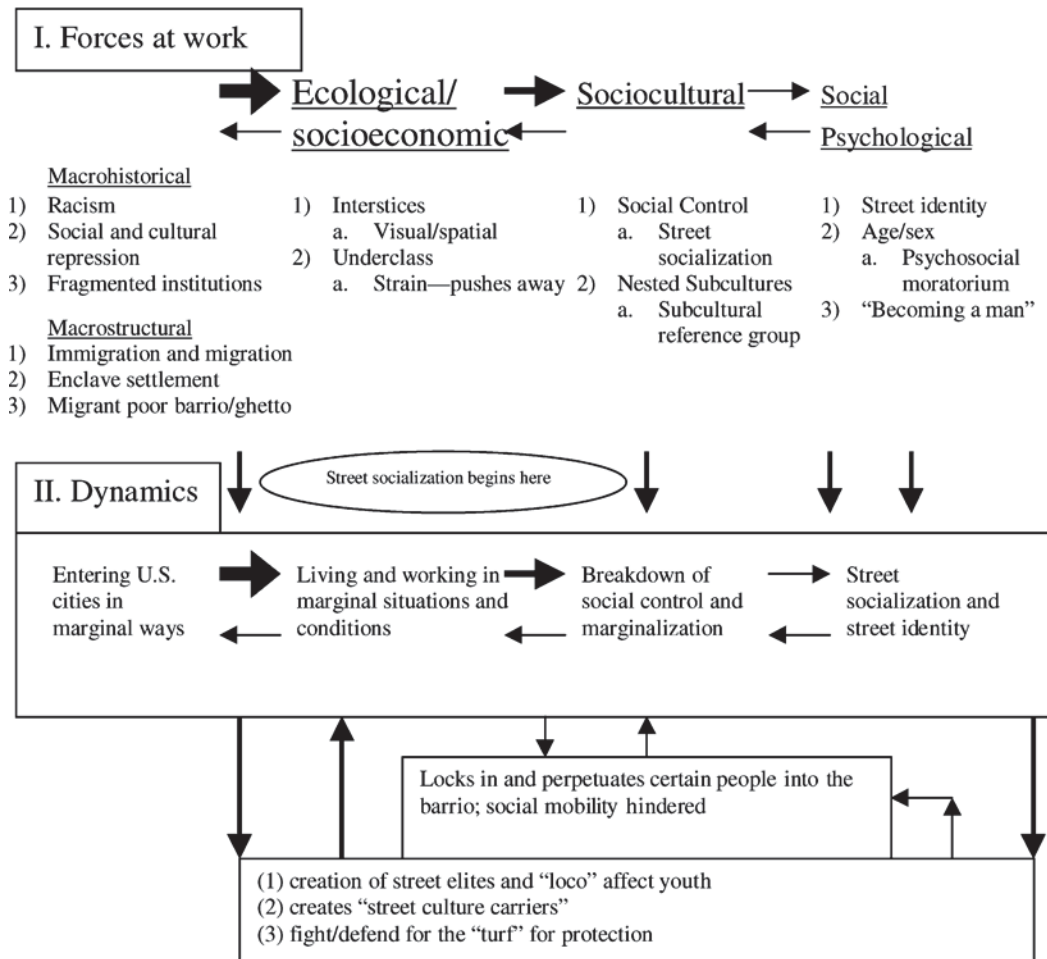
One prime example of such outreach efforts that have greatly contributed to the decline of crime committed by this segment of society is outreach to youth susceptible to violent gang initiation. There are numerous studies that demonstrate how active law enforcement and community outreach to disaffected, disenfranchised, and at-risk youth can greatly reduce the incidence of youth gang membership, as well as reduce the incidence of violent crime committed by youths. One such study in a bulletin by the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention, attempts to outline methods that help communities identify youth at risk for joining gangs and then identify methods for preventing youths from joining gangs. The central tenets of the bulletin are that, while youths of various ages and from all segments and strata of society join gangs, the vast majority of youth gang members tend to be between the ages of 12

and 24 (Esbensen, 2000, p. 3) and come from “socially disorganized and socially marginalized communities” (Esbensen, 2000, p. 9). The study more specifically defined the average youth gang member as being a “minority youth residing in single-parent households” (Esbensen, 2000, p. 4). The study further proffered that any program designed to reduce youth gang recruitment and participation that only focused on one solution or approach was doomed to failure. The study pointed to the need for a multipronged approach that addresses the multiple underlying problems making youth more susceptible to gang involvement (Esbensen, 2000, p. 9).

Corroborating these findings are individuals from community outreach groups across the country, such as the director of the Latin American Youth Center in Washington, D.C., Mai Fernandez. Speaking before Congress, Fernandez pointed to the plight of immigrant families who came to the United States to find better lives for their families; in so doing many of the parents discovered that they needed to have multiple jobs outside of the home, leaving them precious little time to spend rearing children and providing them the time and attention required to keep them from seeking a sense of belonging with gangs and falling prey to negative influences (Fernandez, 2007, p. 48). Speaking before the same House of Representatives subcommittee the following year, former Los Angeles gang member Ely Flores spoke of his path to recruitment by a gang and his subsequent life of delinquency and crime. Flores spoke of coming from a single-parent household, where he was raised by his mother in an economically depressed neighborhood, where many of his peers were frequent visitors to youth detention facilities and prisons as a result of joining gangs in order to fill a need for belonging (Flores, 2008, p. 80). Flores identified the lack of resources and alternatives to gang life as the reason for his ever-growing sense of anger and disenfranchisement.

Still other gang researchers point to even more complex and interwoven socioeconomic predictors for gang initiation. One such framework, known as multiple marginality (Vigil, 2003, p. 230), takes a collective assessment of such factors as the effect of the neighborhood dynamic, sociocultural marginalization, poverty, social control, and other gang membership predictors. This framework seeks to examine the interconnectivity of multiple factors to include what constitutes a gang, where the gang

resides/exists, how the gang operates, and how their behavior is in part determined by societal factors, why gangs act the way they do, when gangs will act out with violence, and with whom gang members engage in unlawful and/or socially destructive behavior (Vigil, 2003, p. 232).



Source: Vigil, 2003, p. 231.

Figure 2. Framework of Multiple Marginality: “Act and React”

Vigil discusses the process of acculturation—the process of learning a new culture—as a key element of marginalization because the conflict between learning one’s own culture while at the same time having to learn a new culture often leads youth, especially minority youth, to identify with life on the street (Vigil, 2003, p. 235–36.) Vigil notes that, in studying urban street gangs, early gang researchers at the turn of the

century examined the movement of sharecroppers and other immigrants into urban settings. It was from this migration into the cities of socioeconomically deprived immigrants and the resulting hardships of urban life, including the lack of integration with mainstream society, that set the stage for the creation of gangs (Vigil, 2003, pp. 232–33). Pointing specifically to African American youth, Vigil notes that the acculturation process has been ongoing for this segment of society since their ancestors were uprooted from Africa and transplanted in foreign lands such as the United States (Vigil, 2003, p. 236).

These same tenets are shared by literally hundreds of professionals spanning the fields of academia, law enforcement, government, and private agencies who address gangs of all types on a daily basis. Some key findings in this body of study speak to the importance of healthy and stable home lives in the socialization process and the ability of youths to avoid becoming involved in criminal behavior, the negative impact of the absence of positive male role models, and the lack of discipline at home as being key factors in determining whether youths will join gangs (Carlie, 2009, pp. 2-8). Other key findings highlight the fact that youths most often join gangs out of a need for positive emotional reinforcement, structure, discipline, a sense of belonging, acceptance, and recognition, among other needs (Lees, Dean, & Parker, 1994, p. 1). Congruent with these, the primary risk factors determining youth susceptibility to gang recruitment are racism, poverty, the lack of a support network, and media influences (Lees, Dean, & Parker, 1994, p. 1). The conclusions of these studies, primarily the demographic analyses and the corresponding socioeconomic factors identified as being at the root of gang recruitment and initiation, are nearly identical with those associated with the segment of the ethnic Somali diaspora residing in the United States, which is radicalizing and being recruited by Al Shabaab, as will be discussed next in this chapter.

B. SOCIOECONOMIC FACTORS CONTRIBUTING TO SOMALI-AMERICAN AL SHABAAB RECRUITMENT

In working to understand precisely what is driving a small percentage of Somali-American youth to radicalize and seek the jihadist lifestyle, we must first conduct a cursory examination of the history of Somali immigration into the United States. Such an

examination offers a glimpse of the genesis of the socioeconomic drivers of Somali-American radicalization. This is key since there exist few publicly available details regarding the socioeconomic background of all Somali-American jihadists identified to date (Weine et al., 2009, p. 185). In the early 1990s, after the outbreak of civil war in Somalia and the United States' humanitarian intervention in that country, the first mass migration of Somalis into this country began. Minneapolis, Minnesota, offering a bevy of social services and blue-collar employment opportunities, quickly became the seat of the Somali diaspora in North America (A. Elliott, 2009). The diaspora quickly grew and expanded into other states, including California, Massachusetts, Washington, Ohio, and Maine (Hsu & Johnson, 2009). Today the Somali-American population is estimated to be in the range of 150,000 to 200,000; however, this number could be higher, due to such factors as identity and documentation fraud, illegal immigration, and reluctance on the part of Somali-Americans to share personal information with U.S. census workers (Mudd, 2009). Unlike their European counterparts, Muslim immigrants to the United States (including Somali-Americans) seem to truly embrace the American dream and believe they have found a place where they can thrive (Sageman, 2007, p. 3) despite the fact that Somalis in general receive less cultural and language training prior to immigration than do other Muslims immigrants to the United States (Liepman, 2009). Even when having to overcome language and cultural barriers, first-generation Somali-Americans quickly entered the workforce, occupying mostly service-sector jobs, and by all accounts were productive members of society, except for a proclivity to keep to themselves within their ethnic enclaves (A. Elliott, 2009), which, given the clan-based nature of Somali society, is not unexpected or unusual. Perhaps the single greatest driving factor behind the Somali-American community's robust participation in the U.S. economy is the critical role that the global Somali diaspora plays in passing remittances back to family members and friends in Somalia, a sum estimated to be approximately one billion dollars annually (Menkhaus, 2009). The push for Somali-Americans to push remittances back to Somalia is so great that failure to do so on the part of any Somalis, even Somali-American youth capable of gaining employment (teens and above), would

mean instant renouncement by family and clan (Menkhaus, 2009). However, despite their strong work ethic and hard work, 60 percent of Somali-Americans live in poverty (Weine et al., 2009, p. 182).

While adult Somali-Americans could largely isolate themselves socially from their non-Somali neighbors, Somali-American youth could not do so—they were immersed in American schools and American life and forced to deal with the pains of assimilation (A. Elliott, 2009). Linguistic isolation has been identified as one of the primary reasons that Somali-Americans suffer high poverty rates, the lowest college graduation rate, and the highest unemployment rate among East African diaspora communities in the United States (Liepman, 2009). This is reflected in the testimony of one Somali-American, Abdirahman Mukhtar, who was born in Somali but fled with his family to the United States in 1998 and settled in Minneapolis, Minnesota (Mukhtar, 2009, p. 1). There Mukhtar entered high school—the same high school as many of the thus-far identified Somali-American jihadists, including Shirwa Ahmed (referred to in Chapter I), the first Somali-American to die serving as a suicide bomber for Al Shabaab in Somalia. Mukhtar struggled in school, due to a variety of factors, including his inability to speak English, his need to overcome social and cultural biases of other students, and the requirement that he work in order to send remittances back to the family in Somalia (Mukhtar, 2009, p. 2). Mukhtar, like many Somali-American youth, was caught between two worlds—that of older, first-generation Somali-American immigrants who live as if they plan to return some day to Somalia, and younger, second-generation Somali-Americans who struggle to assimilate and immerse themselves in American culture (Mukhtar, 2009, p. 5; Weine et al., 2009, p. 189; Temple-Raston, 2009). Mukhtar summed up his experiences as a Somali-American teen, and very likely the experiences of most Somali-American youth, saying, “Parents expect you to keep your culture, while the American education system and way of life forces you to assimilate” (Mukhtar, 2009, p. 3).

Stories like that of Mukhtar are common within the Somali-American community. In their often strained attempts to fit in, Somali-American youth are frequently chided for attempting to be something they are not. This is especially the case with their African-

American counterparts who mock Somali-American youth for their mimicry of “ghetto” customs (A. Elliott, 2009). At the same time, these same Somali-American youth are chastised by family members for being too “ghetto,” thus further alienating the youth and instilling within them strong feelings of self-doubt and identity confusion (A. Elliott, 2009). These same family members often show more interest in the struggles of life back in Somalia than in the mental well-being and social adjustment of their children (Mukhtar, 2009, p. 3). As a result, Somali-American youth suffer from a “crisis of belonging”—a phrase coined by the uncle of one boy who left America for Somalia and tutor of Somali-American youth at the same Minneapolis high school attended by Mukhtar (A. Elliott, 2009).

Facing barriers of “race and class, religion and language” (A. Elliott, 2009), many Somali-American youth seek a sense of brotherhood or family, where they can share their thoughts and experiences with like-minded individuals. There are those who believe that the Internet and certain fundamentalist mosques are to blame for the radicalization of Somali-American youth who are seeking ways to cope with American life and culture (Butty, 2010; Ali, 2006). Omar Jamal, executive director of the Somali Justice Advocacy Center in Minnesota, echoed these sentiments, saying, “You have high rates of young guys unemployed. You have a high rate of dropouts. They’re difficult to integrate and work into the mainstream.” Jamal further blamed religious extremists for having conducted outreach to disaffected youth and “indoctrinated them into this violent, radical ideology” (Hsu & Johnson, 2009), sentiments echoed by concerned members of the Somali-American community (Ahmed, 2009, pp. 3–4).

An examination of those criminally charged to date for their acts in support of Al Shabaab, or those directly supporting the terrorist organization, reveals that the ages of those involved ranges from the late teen years to the early forties. However, the vast majority of those criminally charged for traveling to Somalia for the purposes of engaging in armed combat have been between the ages of 18 through 27 at the time of charging. The exact age of the men at the time of their radicalization and subsequent recruitment by Al Shabaab is not clear, but it appears from the profiles of those Somali-American youth thus far criminally charged for their affiliation with, and support of, Al-

Shabbaab that this time period can typically be measured in months, not years All of the Somali-Americans identified to date as being involved in activities supporting Al Shabaab immigrated as children to the United States from Somalia (Ahmed, 2009, p. 3) and were subjected to the pressures and strife spoken of by Abdirahman Muhktar and others. Six of these young men died as a result of their participation in jihadist fighting in Somalia, with one of the young men, Shirwa Ahmend, dying as a suicide bomber.

Table 3. Somali-Americans Supporting Al Shabaab

Somali- Americans supporting Al Shabaab			
Name	Age when charged	Education	Role
Ahmed, Salah Osman	26	began college	jihadist
Abdulle, Adarus	25		jihadist facilitator
Abdow, Abdow Munye	26		jihadist facilitator
Abshir, Khalid Mohamud		High School	recruiter / jihadist
Ahmed, Shirwa (deceased)	27	High School	jihadist
Bana, Jamal (deceased)	19	began college	jihadist
Faarax, Cabdulaahi Ahmed	32		recruiter / jihadist
Hassan, Mohamed Abdullahi	18	High school (incomplete)	jihadist
Hassan, Kamal Said	24	began college	jihadist
Hassan, Mohamoud (deceased)	23	began college	jihadist
Hassan, Burhan (deceased)	17	High school (incomplete)	jihadist
Isse, Abdiweli Yassin			provided funding / recruiter
Isse, Abdifatah Yusuf	25	began college	jihadist
Maruf, Zakaria (deceased)	30		jihadist
Mohamed, Omar Abdi	24	High school	recruiter
Omar, Ahmed Ali		High school	recruiter / jihadist
Omar, Mahamud Said	43		provided funding / recruiter
Salat, Mustafa Ali	18	High school (incomplete)	jihadist
Shumpert, Ruben (deceased)			jihadist

(Anti Defamation League, 2010; US Department of Justice press release, November 23, 2009)

An examination of the above chart might at first glance give no indication of the turmoil that the Somali-American youth highlighted endured, since many completed high school, and some even began taking college courses. However, closer examination of the facts reveals that several of the highlighted youth never completed high school but instead dropped out in order to begin their jihadist exploits (A. Elliott, 2009). The same is

the case for those few who had begun college courses. Nearly all of these Somali-American youth turned Al Shabaab jihadists once lived in an impoverished neighborhood infested with gangs, drugs, and violence in a community geographically isolated from the rest of Minneapolis (Weine et al., 2009, p. 189) in a group of tall, public-housing buildings known as “the Towers” (Temple-Raston, 2009). It seems that all these youths followed the same path: social isolation as a result of language and cultural barriers, followed by disenfranchisement and disillusionment, followed by radicalization, and ultimately culminating in their recruitment by Al Shabaab.

While the vast majority of those charged thus far in the United States for crimes related to support of the Al Shabaab terrorist organization have been Somali-Americans, there have been several non-Somali-Americans charged, including the previously mentioned Daniel Maldonado, who warrant a cursory review. The following table lists other non-Somali-Americans charged to date.

Table 4. Non-Somali-American Converts Supporting Al Shabaab

Non Somali-American converts supporting Al Shabaab

NAME	Age when charged*	Education	Role
Chesser, Zachary Adam	20		facilitator / jihadist
Hammammi, Omar	26	High school (incomplete)	recruiter / jihadist
Kastigar, Troy (deceased)	28		jihadist
Maldonado, Daniel J	28		recruiter / jihadist
Masri, Shaker	26		jihadist
Mehanna, Tarek	27		facilitator

(*US Department of Justice press release, October 20, 2010; US Department of Justice press release, August 5, 2010; Family Security Matters, 2010; US Department of Justice press release, July 20, 2007; Family Security Matters, 2010; US Department of Justice press release November 5, 2009)

Although not a Somali-American himself, Daniel Maldonado, the first American citizen criminally charged for his jihadist activities in Somalia (Anti Defamation League, 2010, p. 6), perhaps best summed up the feelings of many Somali-American youth when he said that his reason for traveling to Somalia to live and fight alongside Al Shabaab was so that he, “would be able to live, pray, act, dress and be a Muslim without anyone

yelling at me, calling me names, refusing me jobs or apartments” (Family Security Matters, 2010). An American convert to Islam, Maldonado’s words highlight his frustrations with being singled out and chastised for being a Muslim and his corresponding need to feel a sense of belonging. So what leads such non-Somali-Americans to take up the cause of Al Shabaab? The answer to this question remains unclear, but terrorism expert Marc Sageman believes that “terrorists are idealistic young people, who seek glory and thrills by trying to build a utopia. Contrary to popular belief, radicalization is not the product of poverty, various forms of brainwashing, youth, ignorance or lack of education, lack of job, lack of social responsibility, criminality or mental illness. Their mobilization into this violent Islamist born-again social movement is based on friendship and kinship” (Sageman, 2007, p. 1). As we have seen in this chapter, this need to feel a sense of kinship and belonging is a characteristic common to both Somali-Americans radicalizing and joining the ranks of Al Shabaab, as well as to thousands of other American youth who seek such belonging within criminal gangs.

The sources documenting radicalization in the United States are largely in lockstep agreement with the fact that militant Islamic extremism has not simply taken root in one isolated corner of the homeland—it has spread throughout the country. The promises of self-fulfillment and individual honor have attracted and continue to attract disaffected Muslims, primarily young Muslim men. From a review of the limited body of work related to radicalization of Somali-Americans, it appears that there are many barriers that law enforcement and social welfare organizations must overcome in order to effectively address the radicalization of the U.S. Somali diaspora. The United States finds itself in a difficult situation: how to address the very real problem of the spread of Islamic radicalization while not alienating the moderate Muslim communities in the United States and abroad and further fanning the flames of radicalization. John Miller, FBI Assistant Director of the Office of Public Affairs, in a 2007 statement before the Senate Committee on Homeland Security and Governmental Affairs, spoke to the need for the FBI and other elements of government to conduct outreach to the Muslim community in the United States in order to earn their respect and trust. Echoing these sentiments is Dr. Ken Menkhaus, professor of political science at Davidson College and noted expert on Somali

issues and Al Shabaab specifically, who identified six such barriers between law enforcement outreach efforts and Somali-Americans. These barriers include Somali-Americans' distrust of law enforcement due to harsh treatment endured in Somalia at the hands of security services; the illegal status of some Somalis residing in America; Somali customary laws that are often in conflict with U.S. laws; the Somali people's history of persecution; ignorance of U.S. laws; and the collective failure of Somali-Americans to take responsibility for ensuring that their youth do not engage in terrorism or activities supportive of terrorism (Menkhaus, 2009, pp.13–14). So why do these barriers exist, and can we get beyond them in order to address the problems of radicalization and recruitment? The answer to these questions comes with the introduction of the psychosocial perspective.

In trying to understand why a small percentage of Somali-American youth are radicalizing and seeking to wage jihad in Somalia, there is value in examining what these youth experience psychologically while trying to assimilate into American culture. Stevan Weine and his associates examined community and family approaches that could be utilized in combating the radicalization and recruitment of Somali-American youth utilizing the psychosocial perspective. This perspective is one that seeks to go beyond the perspectives of politics, criminal justice, history, or theology and instead takes into account community and family processes when assessing the mental well-being of an individual; it further seeks to address imbalances in this well-being through intervention at both the community and family levels (Weine et al., 2009, p. 184). The psychosocial perspective, methodologically speaking, focuses on allowing individuals to, in their own words, describe their strengths, weaknesses, and needs, as well as their perceptions of their families, peer groups, schools, and communities, and then uses those narratives in scripts utilized during intervention sessions (Weine, Ware, & Klebic, 2004, p. 924). Like “situationists” such as Zimbardo and Moghaddam who argue that the behavior of individuals and groups can be manipulated through a convergence of situational factors (Zimbardo, 2007, p. 25; Moghaddam, 2006, p. 22), the psychosocial perspective examines how certain environmental factors can help determine why some people commit violent or terrorist acts. However, unlike the “situationists,” the psychosocial

perspective focuses less on addressing certain specific negative behaviors (i.e., violent acts) as it is with addressing the underpinning social and psychological factors contributing to radicalization (Weine et al., 2009, p. 185). As summarized by Weine, “Identity confusion, social isolation, academic underachievement, or high-risk behaviors may not only reflect individual psychopathology but also be manifestations of trauma to families, to communities, and to cultures” (Weine, Ware & Klebic, 2004, p. 923). Weine makes it clear that he and his colleagues are concerned that current counterterrorism approaches advanced by terrorism experts and law enforcement “lack a fundamental appreciation of the significance of knowledge about community and family processes in refugee and immigrant groups,” processes that Weine and his colleagues believe could help significantly mitigate the risk of radicalization and Al Shabaab recruitment occurring among Somali-American youth (Weine et al., 2009, p. 193).

Looking at the Somali-American community through the psychosocial perspective, Weine notes, one quickly sees a variety of factors that have led to the current occurrences of radicalization and Al Shabaab recruitment within that community. Some of these factors include nationalist feelings of wanting to fight in defense of the Somali homeland (Weine et al., 2009, p. 188), trauma experienced in refugee camps overseas prior to migrating to the United States (Weine et al., 2009, p. 188), the prevalence of Somali mothers who were torture survivors and single parents (Weine et al., 2009, p. 188), high levels of poverty (Weine et al., 2009, p.189), clan/tribal divisions that continue despite migration to the United States and that “impede the delivery of community-level support as well as community collaboration with social services, health services, and law enforcement (Weine et al., 2009, p.189), language deficiencies that limit education and thus opportunities (Weine et al., 2009, p.189), being “Americanized” too quickly, which leads to feelings of being “trapped between different and at times dissonant identities” (Weine et al., 2009, p.189), and the lack of fathers and other positive male role models to steer young Somali-American males away from gang activity or Islamic extremists (Weine et al., 2009, p.189), among others. Weine’s argument is that all of these factors, as well as others not highlighted, diminish the positive psychosocial

processes that might have otherwise been able to prevent certain Somali-American youth from straying down the path of radicalization and Al Shabaab recruitment, or gang violence for that matter (Mukhtar, 2009, p. 4).

Weine's answer to how local, state, and federal government in the United States can leverage psychosocial approaches in dealing with this problem centers around government learning about, and taking into account, the psychosocial issues that are key to combating radicalization in diaspora communities (Weine et al., 2009, p. 192). These issues include diaspora-specific cultural beliefs and practices, the differences between refugees in the United States and immigrants, an understanding of those in the diaspora most at risk and what exactly that entails, the diversity of Islamic perspectives, the roles and function of families within immigrant communities, the structure and function of immigrant community leadership, and disparities between immigrant and non-immigrant educational opportunities (Weine et al., 2009, pp. 192–93). Wine's solution is made up of the following five-steps.

Step one is identifying community and family protective resources. Since a psychosocial approach assumes that susceptibility to radicalization and recruitment can be reduced by strengthening family and community protective processes, government and private-sector agencies should examine and strengthen the roles of parenting, including parental involvement in education, government outreach to families, mentoring, and faith communities (Weine et al., 2009, p. 194). Step two is building family interventions based on well-researched knowledge of the social circumstances of refugee and immigrant Somali-American youth, especially those between the ages of 15 and 25 and from single-mother households (Weine et al., 2009, p. 194). By speaking with Somali-American youth who do not radicalize or are not recruited by Al Shabaab or criminal gangs—the vast majority of this group—authorities can use this information in creating positive counter radicalization programs (Weine et al., 2009, p. 194). Step three is building multilevel community interventions that go beyond just family-level intervention and seek to engage Somali-American youth in a comprehensive fashion. This can be done through programs that leverage the assistance of positive, adult Somali-American male mentors who encourage Somali-American youth in such areas as education, careers, and

personal development, programs that promote the formation of local and state Somali-American leadership groups that encourage civic engagement and public service, programs that provide imams and other community leaders with the necessary tools and training for dealing with gang and extremist recruiters, and also programs that seek to counter the negative messages of extremists on the Internet (Weine et al., 2009, pp. 195–96). Step four is forming community collaborative partnerships that develop, refine, and test different intervention strategies through partnerships between local organizations, businesses, schools, and religious institutions using the knowledge gained by identifying the positive psychosocial processes found within the community that tend to prevent radicalization and recruitment (Weine et al., 2009, p. 196). And finally, step five involves forming multidisciplinary collaborations among counterterrorism, law enforcement, social and mental health services, education, and academia. Such collaboration would bring to bear psychosocial expertise in supporting the efforts of law enforcement and other counterterrorism experts, including research and analysis support in furtherance of efforts to tailor counterradicalization programs and messages, and could also offer to law enforcement education, training, technical assistance, and fellowships on psychosocial issues, while also offering to psychosocial workers similar programs on counterterrorism issues (Weine et al., 2009, pp. 196–97).

In the same vein as Weine and his colleagues, Dr. Walid Phares, senior fellow at the Foundation for the Defense of Democracies, in 2006 testimony before the House of Representatives Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, outlined a six-point plan for countering radicalization. In step one, according to Phares, government, the media, and subject matter experts must identify and accept the notion of the existence of an ideology of jihadism to pave the way for step two, in which the public and educational institutions mobilize against this ideology by teaching counterphilosophies (Phares, 2006, p. 27). Step three involves the government’s banning of this ideology, based upon its violent teachings and the threat the ideology poses to society, followed by step four, which involves a massive public education campaign conducted with the assistance of publicly funded media—i.e., National Public Radio, C-SPAN, the Public Broadcasting System (Phares, 2006, pp. 27–28). Step five involves

enlisting the public's assistance, along with that of domestically based nongovernmental organizations (NGOs) in countering radicalization, which builds into step six in which the assistance of international NGOs, and specifically democratic and humanist Muslims is enlisted (Phares, 2006, pp. 27–28).

Can plans like those of Weine and his colleagues, or like those of Dr. Phares, work? Will Somali-Americans buy into such plans and participate? The answer to these questions may be reflected in the responses of American Muslims to polls focusing on American Muslims perceptions of life in American. A 2007 Pew Research poll found that despite the fact that 53% of American Muslims believe it is more difficult since the 9/11 attacks to be a Muslim in America, 78% were either “happy” or “very happy” with their lives. Also, 76% of American Muslims were very or somewhat concerned about the rise of Islamic extremism around the world, and 61% were concerned about its rise specifically in the United States. These statistics are supported by the observations of scholars and experts such as Dr. Marc Sageman, who notes, “The American Dream is alive and well among Muslim Americans” (Sageman, 2007, p. 5). Dr. M. Saud Anwar, chairman of the American Muslim Peace Initiative, offers a similar perspective, pointing to a poll conducted of the Pakistani American community regarding Muslim integration in the post-9/11 era in the United States. Anwar notes that in that poll 2,000 individuals were polled, with 10% responding. While the poll suggests that American Muslims (84%) are more inclined to integrate into American society and maintain their heritage as opposed to assimilating, they at the same time overwhelmingly (99.5%) value interaction with non-Muslim Americans (Anwar, 2006, pp. 3–4). Additionally, the majority of the Muslim Americans polled said they were comfortable talking to a law enforcement officer (75%) (Anwar, 2006, pp. 3–4). Dr. Anwar, drawing upon these statistics, advocates increased communication and coordination between law enforcement and American Muslims in order to counter the effects of radicalization. (Anwar, 2006, pp. 3–4).

C. CONCLUSION

In examining the threat associated with Americans who radicalize and travel to the Horn of Africa region to train and fight alongside Al Shabaab, it is clear that not all who do so are ethnic Somalis or members of the Somali diaspora. However, the majority of the identified Americans to date who have traveled to Somalia for the purposes of jihad have been Somali-Americans. While no counterradicalization program can be expected to be 100% effective, just as no nation can ever prevent every threat (Brennan, 2010), it seems evident that a focused and tailor-made counterradicalization program structured so as to empower and equip Somali-American communities to police themselves is what is needed. Such a program would make allowances for the unique cultural customs and beliefs, and would avoid the accusations of excessive government focus on Muslims, as well as the government surveillance and spying experienced by the U.K. government. However, such a program is needed quickly and must have a high probability for success. Focusing on enforcement efforts alone, however, would likely prove to be counterproductive, as has been the case in efforts to counter gangs. As pointed out by Robert Scott, chairman of the U.S. House of Representatives Subcommittee on Crime, Terrorism, and Homeland Security, enforcement approaches disproportionately target minorities, especially blacks and Hispanics, who are frequently treated more harshly than their white counterparts (Scott, 2007, p. 2). Additionally, Scott identified the need for government and communities to address the underlying reasons that youths join gangs and engage in criminal activity: to ignore these reasons and focus simply on enforcement will serve only to perpetuate gangs and their expansion (Scott, 2007, p. 3).

While the problem of gangs and gang violence have not been eradicated in the United States, after decades of experience, much trial and many errors, there are effective countergang best practices that, modified properly, could be quickly applied to the problem of radicalization occurring among Somali-Americans. The focus of such best

practices, and the corresponding reason for their success, is the combination of community engagement and empowerment in addressing the problem of gangs and gang violence.

The authors of all the sources reviewed agree is that the solution to the problems of Islamic extremist radicalization and recruitment in the United States is not likely to be found in “quick-fix” remedies. The effort will require extensive community engagement and trust building and will take time measured in years, not months or days. Noted terrorism expert Bruce Hoffman, in his book “Inside Terrorism,” echoes the common sentiment of the majority of works on this topic: “Winning the war on terrorism will take decades, not years, to accomplish. If we are to succeed our efforts must be as tireless, innovative, and dynamic as those of our opponents” (Hoffman, 2006, p. 295). FBI Director Robert Mueller III, during one of many public addresses on the issue of radicalization, echoes these words:

We must continue to work with our law enforcement and intelligence partners around the world. But we must also work here in the United States with the citizens we serve, to identify and disrupt those who would do us harm. Too often, we run up against a wall between law enforcement and the community—a wall based on myth and misperception of the work we do. We know that the best way to tear down that wall is brick by brick, person by person. Yet we understand the reluctance of some communities to sit down at the table with us. They may come from countries where national police forces and security services engender fear and mistrust. Oftentimes, the communities from which we need the most help are those who trust us the least. But it is in these communities that we must redouble our efforts. (Mueller, 2009)

While there is a great deal of agreement among the various pundits and experts regarding the causative factors of radicalization, there is clearly no consensus on how best to counter it. Further, despite the significant attention given to the radicalization of American ethnic Somali youths and their travels to the HOA region to fight alongside Al Shabaab during the past two years, there has been little study of how this particular problem set could or should be addressed. However, the materials available suggest that the solution to the problem of the radicalization of ethnic Somali-Americans is not to be found in one place. Instead, the solution will come from a combination of increased

public awareness of the need to help American Muslims integrate into American society and from government conducting effective outreach to disaffected Muslims with the assistance of both government and nongovernmental organizations.

V. FINDINGS AND RECOMMENDATIONS

Trust is an integral part of the fabric of our society.... Without trust, society closes down and will ultimately self-destruct.

-Stephen R. Covey

Much of the defense against jihadist radicalization will be invisible—quiet discouragement, interventions by family members and friends, and when necessary, discreet assistance to the authorities.

-Brian M. Jenkins

It is reckless to leave the task of combating terrorism only to the professionals when the changing nature of the threat requires that ordinary Americans play a larger support role in detecting and preventing terrorist activities.

-Bergen & Hoffman

The goal of this research was to determine whether there were any best practices that could be culled from past and current countergang initiatives and then applied to a program to counter radicalization occurring within Somali-American communities in the United States. Such radicalization of Americans, especially those who subsequently receive jihadist training and experience outside the United States, jeopardizes the national security of this country. Toward the end of addressing radicalization within this segment of the U.S. populace, the research within this thesis addressed the following critical question: What, if any, best practices can be derived from law enforcement and public welfare agency efforts over the last four decades to stem youth gang recruitment and initiation and then be applied to efforts to counter radicalization and Al Shabaab recruitment within the ethnic Somali diaspora in the United States?

A. FINDINGS

Examination of countergang best practices for this thesis led to the identification of the U.S. Department of Justice-adopted comprehensive, community-wide gang program model as one that encompasses the most effective elements culled from successful countergang programs nationwide. The program includes five field-tested core

strategies: community mobilization, opportunities provision, social intervention, suppression, and organizational change and development (USDOJ, OJJDP, 2009, p. 2). It may seem that there is no better critique of this program than the fact that it has yet to completely solve the gang problem. However, this would assume that the comprehensive, community-wide gang program model has been properly and uniformly applied throughout the country, which is not the case. The data discussed in Chapter III make it clear that, when the program is properly initiated and applied, it has not only demonstrated success in curbing violent youth gang recruitment and the criminal acts committed by youth gang members but has more importantly demonstrated success in mobilizing communities in addressing this problem (Howell & Curry, 2009, p. 13). For this reason, the comprehensive, community-wide gang program model shows promise as an effective approach for countering radicalization among ethnic Somali-American communities. However, modification of this model will be required in order to account for the differences between the gang and the radicalization problem sets. This would include changes in such areas as the formation and composition of the steering committee, as well as the intervention team and its outreach staff—all key elements of the comprehensive gang model and all necessary components of a comprehensive counterradicalization model program. Once necessary modifications are made, however, the comprehensive, community-wide gang program model shows great promise as being an effective means of addressing radicalization among Somali-American communities through engagement with, and empowerment of, those communities.

Just as the creator of the comprehensive, community-wide gang program model noted that the failure of the model to reduce gang recruitment and violence in certain locations was due primarily to the failure on the behalf of the initiating local governments to include community-based intervention into their countergang model (Spergel, Wa, & Sosa, 2006, p. 222), the failure of current counterradicalization efforts is due to the greater failure of government at all levels to empower communities to address the problem themselves. This view is supported by experts in the field of sociology, who affirm the need for communities to be supported in their efforts to police themselves with regard to addressing violence and other maladaptive behavior. Such support can be

derived from community partnerships with “agencies of formal social control,” such as law enforcement and community policing programs, among others (Sampson, Raudenbush, & Earls, 1997, p. 923).

B. NATIONAL POLICY GUIDANCE

How do we address radicalization of Somali-Americans, given that they tend to reside in enclaves largely isolated from mainstream American society? The research findings of this thesis make it evident that the answer lies in the successful engagement of Somali-American communities in countering radicalization and its negative effects. Fortunately, recent U.S. national policy has identified the need for such increased community engagement. The 2010 U.S. National Security Strategy specifically addresses the threat posed by radicalization and speaks to the need for new policies and programs to address this threat. While no specific plan is proffered, the National Security Strategy nonetheless identifies the need for programs that “expand community engagement” and “empower local communities.” (National Security Strategy of the United States, 2010, p. 19).

Following the conclusions of the National Security Strategy, the first Quadrennial Homeland Security Review (QHSR) report, released in February 2010, further addresses the need for government to enlist the participation of individual citizens and communities in countering radicalization and further emphasizes the need for clearly defined and publicly available methods for reporting suspicious activity (United States Department of Homeland Security [USDHS], 2010, p. 39). The QHSR further identifies one of the primary goals of the homeland security enterprise as being the fostering of communities that have the resources and ability to ensure their own “well-being” (USDHS, 2010, p. 36) and that work together toward common goals (USDHS, 2010, p. A-8). The report makes it clear that building such communities starts with the individual, who, when vigilant and aware (USDHS, 2010, p. A-8), fosters a prevention environment, which in turn makes for safer communities. These tenets were reinforced in the September 22, 2010, testimony of Michael Leiter, director of the National Counterterrorism Center, before the Senate Homeland Security and Government Affairs Committee, in which Mr.

Leiter pointed to community institutions as having a key role in countering radicalization. Mr. Leiter emphasized the need for community-based solutions that are “sensitive to local dynamics and needs,” and advocated that government serve as a facilitator, not direct community-led initiatives (Leiter, 2010, p. 8). Two prominent terrorism experts, Peter Bergen and Bruce Hoffman, in a recent paper entitled “Assessing the Terrorist Threat,” also highlight the importance of all Americans, not just homeland security professionals, in participating in the detection and prevention of terrorist acts (Bergen & Hoffman, 2010, p. 32).

C. BUILDING TRUST

The problem of radicalization is one born from a society in which malign and antisocial behavior is allowed to go unnoticed and unchecked. In his article “Bowling Alone: America’s Declining Social Capital,” Robert D. Putnam examines the trend toward declining civic engagement and civic trust in American culture. Putnam examines the contemporary phenomena of individual and communal isolation, as evidenced by substantial declines in Americans’ participation in civic organizations (Putnam, 1995, p. 5), civic duties such as voting (Putnam, 1995, p. 3), as well as declines in communal leisure activities (Putnam, 1995, p. 5). Putnam points to several possible causes of such social disengagement (Putnam, 1995, p. 3), such as the rise in the prevalence of technology in leisure activities such as television (Putnam, 1995, p. 9), which allow individuals to self-entertain versus engage with others, and demographic changes (Putnam, 1995, p. 8), such as the rise of single-parent families and lower birth rates. In the end, Putnam is at a loss to fully explain the current social disengagement phenomena and calls for further study. Nonetheless, his article highlights a key point regarding modern American culture—that Americans are not as socially connected as they were in past decades. It is evident that the result of this lack of civic engagement and trust is the rise in recent years of societal ills such as radicalization.

As identified by Putnam, a declining awareness by Americans of their fellow man and their surroundings has fostered an environment in which societal problems such as radicalization emerge and are able to exploit the inattentiveness of the populace. While

the American Somali diaspora communities suffer less from this phenomenon of individual social isolation because they are generally more cohesive, due primarily to their strong family/clan-based structure, they are nonetheless susceptible to the effects of this phenomenon to some degree—especially on the community level. Somali-American communities tend to be closed off to mainstream American society, and for this reason they have not fully assimilated into American culture to the degree that other immigrant diasporas have historically done.

In order for individuals and communities to accept and adopt government programs aimed at addressing radicalization through community engagement, there must be an effort on the part of the government to regain the trust of the Somali-American community. This trust has waned in the last three years as a result of the ongoing federal investigation into the terrorist activity of a select few within that community, and it has only recently begun to show signs of improvement. To build trust the government must be completely transparent in its efforts (Covey, 2006, p. 317). There can be no hidden agenda within the government's plans and no hint of deception, especially when public trust of government is at an all-time low (Pew Research Center, 2010.) Additionally, there must be trust among communities because without such bonds of trust there is little incentive for individuals to take a stand on behalf of the public good (Sampson, Raudenbush, & Earls, 1997, p. 919).

Research has shown that grassroots organizations within communities help build trust among individuals and foster the creation of additional ties on a personal level. These personal-level ties give grassroots organizations their strength because they demonstrate the individual's willingness to take action on behalf of his neighborhood or community secure in the knowledge his fellow community members will do the same (Howell & Curry, 2009, p. 11). As previously mentioned, most Somali-American communities already possess internal mechanisms of community organization (i.e., community elders who serve as informal leaders within the community), so in those instances such existing internal mechanisms can serve as vehicles of community

engagement and change. The stipulation is, of course, that those internal mechanisms of control must be trusting of government and other actors seeking the community's alliance in combating radicalization.

D. DECENTRALIZING THE EFFORT

As has been the message with countergang practices, so it must be with counterradicalization practices with regard to Somali-American communities. Each city, county, and region addressing radicalization along with their Somali community leaders and community groups must address their problems locally. This decentralization of the effort (Brafman & Beckstrom, 2007, pp. 46–53) transfers the responsibility for the planning for and implementation of counterradicalization initiatives out of Washington, D.C., and places it in the hands of those who can best address the problem—communities working with the assistance of local government. The role of the federal government should be relegated to that of being a provider of general program guidance and, most importantly, financial resources. In this way the problem of radicalization can be handled at the lowest possible level, while the community and local government implementers of the policy can still enjoy the centralized support and overarching program guidance offered by the federal government. Such a hybrid approach (Brafman & Beckstrom, 2007, p. 164) ensures that counterradicalization efforts are tailored to meet the needs of the many different Somali-American communities in the United States. Attacking the ideology of the decentralized Al Shabaab recruiting networks provides the decentralized network of Somali-American communities with their best chance of effectively countering radicalization (Brafman & Beckstrom, 2007, p. 144). In other words, destroy the message and you can destroy the threat.

After gaining the trust of Somali-Americans, government agencies, being sensitive to the concerns and unique cultural practices and norms of this group (Davies & Murphy, 2004, p. 2), must work to clarify not only the government's role but also the role of the communities in countering radicalization. Only through such a partnership can a counterradicalization program be effective and successful. What elements define an effective community mobilization program? This has been made clear in the decades of

countergang efforts here in the United States. Noted gang researchers James C. Howell and G. David Curry suggest that there are three hallmarks of effective community-based programs. The first of these is the inclusion of community-based grassroots organizations whose legitimacy and viability are accepted by both parochial and public organizations. The second is that decisions are made collectively among citizens, businesses, and government, and the third is that grassroots organizations and law enforcement must recognize the other's role in the process (Howell & Curry, 2009, p. 12).

Law enforcement agencies especially must strive to overcome Somali-Americans' inherent distrust of the dual roles of law enforcement as both enforcers of the law, as well as stewards of the social welfare. However, as RAND researcher Brian Michael Jenkins pointed out when speaking before the U.S. House of Representatives, government at all levels must be careful not to elevate the societal position of Muslims so as to make them of separate or even privileged status (Jenkins, 2010, p. 6). Such has been the case with the U.K.'s PREVENT program, with the unfortunate consequences discussed in Chapter II.

E. PROPOSAL

In summation, it is entirely feasible that a counterradicalization program modeled after the comprehensive, community-wide gang program model could be applied, with modification, within Somali-American communities in the United States as long as state and local governments and communities are brought early into the planning and coordination of such a program. In fact, the call for just such a model has already come from the Somali-American community (Mukhtar, 2009, p. 7). There will be a need, of course, for collective discussions about how the counterradicalization program and message will be crafted, what it will be, and how it will be disseminated. Additionally, the media's assistance will need to be formally enlisted to help with what will be a massive information campaign. The focus of such a campaign would be the education of the public as to the objective of the program, which is to empower communities to reject violent extremism and in so doing help to protect Americans from future terrorist attacks. Adoption of the following goals by law enforcement and social welfare agencies would go a long way toward ensuring the success of such a program in the United States. Goal

number one: the United States should commit itself to assertively and comprehensively addressing the issue of radicalization among Somali-Americans and other Americans susceptible to radicalization, in an effort to reduce the threat that they pose to the national security of the United States. Goal number two: the president of the United States should commission a panel of experts to examine the U.K.'s PREVENT program in order to identify best practices from that program to be applied within the United States. This panel should be comprised of personnel from key federal, state, tribal, and local government, as well as those private-sector agencies dedicated to addressing social welfare issues and should include, but not be limited to, the following:

- The Muslim Public Affairs Council;
- The Department of Homeland Security ;
- The U.S. Department of Justice;
- The Federal Bureau of Investigation;
- The International Association of Chiefs of Police;
- The National Sheriff's Association;
- The National Governors Association;
- The American Civil Liberties Union;
- The U.S. Department of Health and Human Services/Administration for Children & Families;
- The Anti Defamation League.

This working group should be convened immediately upon identification of the group's members, who should thoroughly study the comprehensive, community-wide gang program model and should examine government and private-sector reporting, both positive and negative, concerning the program. The panel should also, at a minimum, answer the following questions:

- Who will craft the counterradicalization message, what will that message be, and how will it be kept consistent across all U.S. policy and across the span of federal, state, and local governments?

- Who will define the roles of communities, as well as local, state, and federal governments, and how will these roles be complementary to one another? How could they or would they be opposed?
- What steps will local, state, and federal government take in rehabilitating those citizens identified by Somali-American communities as being radicalized to the extent that they are prepared to engage in violence or are on the path to being prepared to engage in violence?

With regard to the first question, there currently is no single agency, whether federal, state, or local, tasked with crafting a message that is as sensitive as will be a government counterradicalization message. The Federal Bureau of Investigation (FBI), with exclusive federal jurisdiction for investigating acts of terrorism domestically, as well as abroad, could be considered. However, given the FBI's well-known law enforcement mission, there exists the potential for conflict should the FBI also be tasked with crafting the nation's counterradicalization message. Since in any counterradicalization program the public's assistance will be enlisted in identifying citizens requiring diversion into government programs designed to stave off radicalization, the government must be able to maintain the public's trust. For an agency to be enforcing the nation's laws, including terrorism laws, while at the same time crafting and delivering the nation's counterradicalization message, invites controversy and certainly could hinder the mission of building public trust of the government's counterradicalization efforts. This has been demonstrated, as highlighted in Chapter II, by the U.K.'s Communities and Local Government agency, whose efficacy has been degraded due to public mistrust of the agency because of its role in the U.K.'s PREVENT program.

The National Counterterrorism Center (NCTC) might on the surface appear to offer hope as the nation's counterradicalization messaging center. An aspect of the NCTC's composition that is of great benefit and that will be essential for the entity tasked with crafting the nation's counterradicalization message is that it is an interagency body. However, in its current composition the NCTC is staffed and structured to serve primarily as an intelligence fusion and analysis center. In order to assume the mission of crafting and delivering the nation's counterradicalization message, the NCTC would need a

fundamental change not only in its charter, but it would also require internal restructuring to include the hiring of additional personnel with the skills and experience in crafting complex public-outreach programs.

The Department of Homeland Security (DHS) seems a logical choice as it was designed to be the clearinghouse with regard to matters relating to the nation's security. However, each of DHS's component agencies (e.g., Immigration and Customs Enforcement, Coast Guard, Federal Air Marshals Service), as currently configured, is already heavily tasked and likely not resourced to handle such a unique and sensitive mission. In order for DHS to assume this mission, a new entity within DHS with the sole mission of crafting the nation's counterradicalization message would need to be formed. Perhaps that is the answer—the creation of a new entity, whether within an existing federal agency (which would likely save precious time and resources) or outside and independent of existing agencies, with the express purpose of crafting and disseminating the nation's counterradicalization message. Either way, whether tasked to an existing agency or to an agency yet to be created, it seems clear that the agency responsible for the mission must be properly resourced and situated within the bureaucracy so as to be the most effective it can be with regard to interagency and intergovernmental collaboration. The agency will need to guard against growing too large and unwieldy so as not to lose sight of its sole mission and purpose, and it must be a truly interagency effort representing the interests of government at all levels—from local to state to federal—since all will be involved in the counterradicalization mission. As to the role of communities, as well as each of the levels of government, and how they will complement and oppose one another, those items must be addressed at length by the aforementioned panel of national leaders and subject matter experts.

There is no quick or easy answer regarding the nation's counterradicalization message, its composition, and how it will be kept consistent across all U.S. policy and across the span of federal, state, and local governments. Suffice to say, the message will need to be broad enough to address varying forms of radicalization, not myopically focused on violent Islamic extremism but instead also address violent domestic militias, violent ecoterrorists, white supremacists, and the like; it must originate from, if not be

directly managed from, one central office so as to ensure the consistency of the message. As for the remaining question concerning the format and structure of any radicalization diversion and rehabilitation programs, this too will require a great deal of discussion. The discussion must be had among leaders at all levels of government, from local to state and federal and must include subject matter experts who can guide the discussion based upon known facts concerning indicators of extremist ideology and radicalization. Only through such collaboration and open discourse can there be any hope that a unified and cohesive approach can come to fruition.

Additionally, learning from the example of our U.K. partner, all levels of government in the United States involved in the counterradicalization mission must work collectively to ensure that the local, state, and federal agencies and/or departments chosen to coordinate and lead the U.S.'s counterradicalization efforts are not ones whose current missions conflict with, or would otherwise be counterproductive to, that of the U.S.'s counterradicalization program (as experienced in the U.K. by the CLG.) By empanelling leaders from across the local, state, and federal government spectrum, as well as community leaders and social welfare and watchdog organizations, true transparency and consensus can be achieved. Additionally, the United States will need to ensure that its message is clear: that violent interpretations of Islam and violent Islamist extremism are antithetical to the American principles of freedom and democracy and that such interpretations of Islam must not be allowed to flourish, but that any form of Islam that respects these principles and that can peacefully coexist with them will be embraced within the United States.

It will require the commitment of all levels of government to ensure that Somali-Americans do not feel under siege and the sole focus of government observation but instead feel empowered to help government root out and identify those who twist Islam to fit their own selfish political agenda. The process will likely proceed slowly at first, but with the participation of community organizers and leaders helping to work past apathy and community denial, there will come positive changes in community response to the problem of radicalization (Spergel, 1992).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- 2010 Canada. (2010). U.S. Gang Summit Program. Retrieved October 6, 2010, from, <http://www.gangcolors.com/wp-content/uploads/2005/11/CanadaSummit.pdf>
- Ahmed, Osman. (2009). Violent Islamist extremism: Al-Shabaab recruitment in America. Hearing before the Senate Homeland Security and Governmental Affairs Committee. Retrieved August 13, 2009, from <http://www.fbi.gov/congress/congress09/mudd031109.htm>
- Ali, Javed. (2006). The homeland security implications of radicalization. Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. Retrieved August 18, 2009, from http://www.fas.org/irp/congress/2006_hr/radical.pdf
- Anti Defamation League. (2010). Al Shabaab's American recruits. Retrieved February 24, 2010 from, http://www.adl.org/main_Terrorism/al_shabaab_american_recruits.htm
- Anwar, M. Saud. (2006). Immigrant American Muslims and European Muslims: Similarities and differences and homeland security implications. Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. Retrieved September 28, 2009, from http://www.fas.org/irp/congress/2006_hr/radical.pdf
- Apuzzo, Matt. (2010). Obama changes subject with Muslim nations. *Washington Times*, April 8, 2010. Retrieved April 9, 2010 from, <http://www.washingtontimes.com/news/2010/apr/08/obama-changes-subject-with-muslim-nations/>
- Associated Press. (2009). Saleh Ali Saleh Nabhan, major Al Qaeda militant, killed in Somalia: Group vows revenge against U.S. *NY Daily News*, September 15, 2009. Retrieved October 18, 2009 from http://www.nydailynews.com/news/world/2009/09/15/2009-09-15_major_al_qaeda_saleh_ali_saleh_nabhan_militant_killed_in_somalia.html#
- Association of Chief Police Officers. (2010). About Us. Retrieved April 25, 2010 from, <http://www.acpo.police.uk/about.html>

- Bergen, Peter, & Hoffman, Bruce. (2010). Addressing the terrorist threat: A report of the Bipartisan Policy Center's National Security Preparedness Group. Bipartisan Policy Center. Retrieved October 4, 2010 from <http://bipartisanpolicy.org/library/report/assessing-terrorist-threat>
- Blair, Dennis C. (2010). Annual threat assessment of the U.S. intelligence community. Testimony before the U.S. Senate Select Committee on Intelligence. Retrieved September 1, 2010, from http://www.dni.gov/testimonies/20100202_testimony.pdf
- Brafman, O., & Beckstrom, R. (2007). The starfish and the spider: The unstoppable power of leaderless organizations. London: Penguin Group.
- Brennan, John. (2010). Securing the homeland by renewing America's strengths, resilience, and values. Speech before the Center for Strategic and International Studies (CSIS). Retrieved July 30, 2010, from http://csis.org/files/attachments/100526_csis-brennan.pdf
- Butty, James. (2010). Analyst sees Internet and mosques radicalizing young Somalis. *Voice of America News*. Retrieved June 11, 2010, from <http://www.voanews.com/english/news/africa/Butty-US-Somalia-Terror-Arrests-React-Samatar-07june10-95751049.html>
- Cahill, M., Coggeshall, M., Hayeslip, D., Wolff, A., Lager-son, E., Scott, M., Davies, E., Roland, K., & Decker, S. (2008). Community collaboratives addressing youth gangs: Interim findings from the Gang Reduction Program. Washington, D.C.: Urban Institute Justice Policy Center. Retrieved October 6, 2010, from http://www.urban.org/UploadedPDF/411692_communitycollaboratives.pdf
- Carlie, Mike. (2009). Into the abyss: A personal journey into the world of street gangs. Retrieved October 30, 2009, from <http://faculty.missouristate.edu/M/MichaelCarlie/>
- Communities and Local Government. (2007). Preventing violent extremism—Winning hearts and minds. Retrieved April 12, 2010, from <http://www.communities.gov.uk/documents/communities/pdf/320752.pdf>
- Communities and Local Government. (2010). What we do. Retrieved April 21, 2010, from <http://www.communities.gov.uk/corporate/about/whatwedo/>
- Connecting Communities. (2010) Retrieved April 21, 2010, from <http://www.communities.gov.uk/communities/racecohesionfaith/connectingcommunities/>

- Covey, Stephen R. (2006). *The speed of trust*. New York: Free Press.
- Dagne, Ted. (2009). Somalia: Current conditions and prospects for a lasting peace. Congressional Research Service. Retrieved September 28, 2009, from <https://www.hsdl.org>
- Davies, Heather J., & Murphy, Gerard R. (2004). Protecting your community from terrorism: Strategies for local law enforcement. U.S. Department of Justice Community Oriented Policing Services (COPS), Police Executive Research Forum.
- Elliott, A. (2009). A call to jihad, answered in America. *New York Times*, July 12, 2009. Retrieved November 14, 2009, from <http://www.nytimes.com/2009/07/12/us/12somalis.html>
- Elliott, A. (2010). The jihadist next door. *The New York Times* (January 31, 2010). Retrieved January 31, 2010, from <http://www.nytimes.com/2010/01/31/magazine/31Jihadist-t.html>
- Elliott, Delbert S. (2007). Making communities safer: Youth violence and gang interventions that work. Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, One Hundred Tenth Congress, First Session. Serial 110-14. U.S. Government Printing Office. Retrieved February 25, 2010, from <http://judiciary.house.gov/hearings/printers/110th/33314.PDF>
- Emerson, Steven. (2002). *American jihad: The terrorists among us*. New York: Free Press.
- Ephron, Dan, & Hosenball, Mark. (2009). Recruited for jihad? *Newsweek* (January 24, 2009). Retrieved January 27, 2009, from <http://www.newsweek.com/id/181408/output/print>
- Esbensen, Finn-Aage. (2000). Preventing adolescent gang involvement. *Juvenile Justice Bulletin*. U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention. Retrieved October 30, 2009, from http://www.ncjrs.gov/html/ojjdp/2000_9_2/contents.html
- Family Security Matters. (2010). Al-Shabaab in Somalia: A magnet for American jihadists? Retrieved November 1, 2010, from http://www.familysecuritymatters.org/publications/id.6956/pub_detail.asp
- Federal Bureau of Investigation. (2010). Uniform Crime Reports. Retrieved April 25, 2010, from <http://www.fbi.gov/ucr/ucr.htm>

- Fernandez, Mai. (2007). Making communities safer: Youth violence and gang interventions that work. Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, One Hundred Tenth Congress, First Session. Serial 110-14. U.S. Government Printing Office. Retrieved February 25, 2010, from <http://judiciary.house.gov/hearings/printers/110th/33314.PDF>
- Flores, Ely. (2008). Addressing gangs: What's effective? What's not? Written testimony submitted to the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, One Hundred Tenth Congress, Second Session. Serial 110-151. U.S. Government Printing Office. Retrieved February 25, 2010 from <http://judiciary.house.gov/hearings/printers/110th/42827.PDF>
- Gerencser, M., Lee, R., Napolitano, F., & Kelly, C. (2008). *Megacommunities: How leaders of government, business and non-profits can tackle today's global challenges together*. New York: Martin's Press.
- Hill, Karl G., Lui, Christina, & Hawkins, David J. (2001). Early precursors of gang membership: A study of Seattle youth. U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention. Retrieved October 27, 2009, from <http://www.ncjrs.gov/pdffiles1/ojjdp/190106.pdf>
- Hoffman, Bruce. (2006). *Inside terrorism*. New York: Columbia University Press.
- Home Office.gov.UK. (2010). The UK counter-terrorism strategy (CONTEST). Retrieved November 28, 2010, from <http://www.homeoffice.gov.uk/counter-terrorism/uk-counter-terrorism-strat/>
- Homeland Security Institute. (2006). Radicalization: An overview and annotated bibliography of open-source literature. Retrieved August 13, 2009, from http://www.homelandsecurity.org/hsireports/Radicalization_Final_Report_15Dec06.pdf
- House of Commons, Communities and Local Government Committee. (2010). Preventing violent extremism. HC65. Retrieved April 12, 2010, from <http://www.publications.parliament.uk/pa/cm200910/cmselect/cmcomloc/65/65.pdf>
- Howell, James C. (1998). Youth gangs: An overview. Juvenile Justice Bulletin. U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention. Retrieved October 30, 2009, from <http://www.ojjdp.ncjrs.gov/jjbulletin/9808/contents.html>

- Howell, James C. (2000). Youth gang programs and strategies. U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention. Retrieved June 12, 2010, from <http://www.ncjrs.gov/pdffiles1/ojjdp/171154.pdf>
- Howell, James C., & Curry, David G. (2009). Mobilizing communities to address gang problems. U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, National Youth Gang Center (NYGC) Bulletin. Retrieved July 22, 2009, from <http://www.iir.com/nygc/publications/NYGC-bulletin-4.pdf>
- Hsu, Spencer S. (2009). Concern grows over recruitment of Somali Americans by Islamists. *Washington Post* (October 4, 2009), p. A7.
- Hsu, Spencer S., & Johnson, Carrie. (2009). Somali Americans recruited by extremists. *Washington Post* (March 11, 2009). Retrieved June 11, 2010, from <http://www.washingtonpost.com/wp-dyn/content/article/2009/03/10/AR2009031003901.html>
- Intelligence and Security Committee. (n.d.). Annual Report 2008–2009, Cm7807. Retrieved April 12, 2010, from <http://www.cabinetoffice.gov.uk/media/346792/isc-annualreport-0809.pdf>
- International Crisis Group. (2005). Counter-terrorism in Somalia: Losing hearts and minds? Africa Report N° 95.
- Jenkins, Brian Michael. (2010). No path to glory: Deterring homegrown terrorism. Testimony before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, U.S. House of Representatives. Retrieved August 11, 2010, from www.rand.org
- Kennedy, David M. (2007). Making communities safer: Youth violence and gang interventions that work. Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, One Hundred Tenth Congress, First Session. Serial 110-14. U.S. Government Printing Office. Retrieved February 25, 2010, from <http://judiciary.house.gov/hearings/printers/110th/33314.PDF>
- Kepel, Gilles. (2004). *The war for Muslim minds: Islam and the West*. Cambridge, MA: Belknap Press of Harvard University Press.
- Klein, M.W. (1995). *The American street gang*. New York: Oxford University Press. Retrieved August 11, 2010, from http://www.amazon.com/American-Street-Gang-Prevalence-Control/dp/0195115732#reader_0195115732
- Lake, Eli. (2010). Strategy focuses on terrorists at home. *Washington Times*, May 27, 2010, p. A-1.

- Lees, Mary H., Deen, Mary, & Parker, Louise. (1994). Research review: Gang violence and prevention. Washington State University. Retrieved November 4, 2009, from <http://web.archive.org/web/20021213231002/http://coopext.cahe.wsu.edu/~sherfey/issue4c.htm>
- Leiter, Michael. (2010). *Nine years after 9/11: Confronting the terrorist threat to the homeland*. Statement for the record before the Senate Homeland Security and Government Affairs Committee. Retrieved September 30, 2010, from <http://www.dni.gov/testimonies/2010-09-22%20D-NCTC%20Leiter%20Testimony%20for%20SHSGAC%20Hearing.pdf>
- Lewis, Bernard. (2003). *The crisis of Islam: Holy war and unholy terror*. New York: Modern Library.
- Lieberman, Joseph I. (2009). Violent Islamist extremism: Al Shabaab recruitment in America. Hearing before the Senate Homeland Security and Governmental Affairs Committee. Retrieved August 13, 2009, from <http://www.fbi.gov/congress/congress09/mudd031109.htm>
- Liepman, Andrew. (2009). Violent Islamist extremism: Al Shabaab recruitment in America. Hearing before the Senate Homeland Security and Governmental Affairs Committee. Retrieved August 13, 2009, from http://hsgac.senate.gov/public_files/031109Liepman.pdf
- Menkhaus, Ken. (2009). Violent Islamist extremism: Al Shabaab recruitment in America. Hearing before the Senate Homeland Security and Governmental Affairs Committee. Retrieved August 13, 2009, from http://hsgac.senate.gov/public_files/031109Menkhaus031109.pdf
- Moghaddam, Fathali M. (2006). *From the terrorists' point of view: What they experience and why they come to destroy*. Praeger Security International. Westport, CT.
- Mudd, Philip. (2009). Violent Islamist extremism: Al Shabaab recruitment in America. Hearing before the Senate Homeland Security and Governmental Affairs Committee. Retrieved August 13, 2009, from <http://www.fbi.gov/congress/congress09/mudd031109.htm>
- Mueller, Robert III. (2009). *The globalization and evolution of the terrorist threat*. Council on Foreign Relations. Washington, D.C. Retrieved October 20, 2009, from <http://www.fbi.gov/pressrel/speeches/mueller022309.htm>
- Mukhtar, Abdirahman. (2009). Violent Islamist extremism: Al Shabaab recruitment in America. Hearing before the Senate Homeland Security and Governmental Affairs Committee. Retrieved August 13, 2009, from <http://www.fbi.gov/congress/congress09/mudd031109.htm>

- Mullins, Sam. (2008). Homegrown terrorism: Issues and implications. *Perspectives on Terrorism: A Journal of the Terrorism Research Initiative*, p.3. Retrieved August 18, 2009, from http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=12
- National Gang Intelligence Center. (2009). National gang threat assessment 2009 (NGTA). Retrieved October 20, 2009, from <http://www.fbi.gov/publications/ngta2009.pdf>
- National Security Strategy of the United Kingdom. (2008). Security in an interdependent world. Cm 7291. Retrieved April 7, 2010, from http://www.cabinetoffice.gov.uk/reports/national_security.aspx
- National Security Strategy of the United Kingdom. (2009). Update 2009, Security for the next generation. Cm 7590. Retrieved April 7, 2010, from http://www.cabinetoffice.gov.uk/reports/national_security.aspx
- National Security Strategy of the United Kingdom. (2010). A strong Britain in an age of uncertainty. Cm 7953. Retrieved December 2, 2010, from http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf
- National Security Strategy of the United States. (2006). Retrieved April 25, 2010, from <http://www.strategicstudiesinstitute.army.mil/pdf/files/nss.pdf>
- National Security Strategy of the United States. (2010). Retrieved December 1, 2010, from http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
- Office for National Statistics. (2010). Retrieved April 25, 2010, from <http://www.statistics.gov.uk/statbase/product.asp?vlnk=601>
- Ogletree, Charles J., Jr. (2008). Addressing gangs: What's effective? What's not? Written testimony submitted to the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, One Hundred Tenth Congress, Second Session. Serial 110-151. U.S. Government Printing Office. Retrieved February 25, 2010, from <http://judiciary.house.gov/hearings/printers/110th/42827.PDF>
- Pantucci, Raffaello. (2009). Understanding the al-Shabaab network. Australian Strategic Policy Institute. Retrieved November 4, 2009, from http://www.humansecuritygateway.com/documents/ASPI_Somalia_UnderstandingAlShabaabNetworks.pdf

- Pew Research Center. (2007). Muslim Americans: Middle class and mostly mainstream. Retrieved August 18, 2009, from <http://pewresearch.org/assets/pdf/muslim-americans.pdf>
- Pew Research Center. (2010). Distrust, discontent, anger and partisan rancor: The people and their government. Retrieved July 16, 2010, from <http://people-press.org/report/606/trust-in-government>
- Phares, Walid. (2006). Intercepting radicalization at the inception phase. Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. Retrieved August 17, 2009, from http://www.walidphares.com/artman/publish/printer_1073.shtml
- Preventing Extremism Together Working Group Report. (2005). Retrieved April 16, 2010, from <http://www.communities.gov.uk/archived/publications/communities/preventingextremismtogether>
- Pursue Prevent Protect Prepare. (2009). The United Kingdom's strategy for countering international terrorism. Cm 7547. Retrieved April 7, 2010, from <http://security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy-2009.html>
- Putnam, Robert D. (1995). Bowling alone: America's declining social capital. An interview with Robert Putnam. *Journal of Democracy* 6.1, pp. 65–78. Retrieved June 18, 2010, from www.chds.us
- Roggio, Bill. (2009). Commando raid in Somalia is latest in covert operations across the globe. *Long War Journal*. Retrieved October 15, 2008, from http://www.longwarjournal.org/archives/2009/09/commando_raid_in_som.php
- Ruffer, G. (2008). What's in a name? Naming restrictions, social cohesion, and the integration of immigrants in the European Union. Paper presented at the annual meeting of the Law and Society Association, Montreal, Quebec, Canada. Retrieved November 5, 2010, from http://www.allacademic.com/meta/p236647_index.html
- Sageman, Marc. (2007). Radicalization of global Islamist terrorists. Hearing before the U.S. Senate Committee on Homeland Security and Governmental Affairs. Washington, D.C. Retrieved September 28, 2009, from <https://www.hsdl.org>
- Sampson, R.J., Raudenbush, S.W., & Earls, F. (1997). Neighborhoods and violent crime: A multilevel study of collective efficacy. *Science* 277, pp. 918–24.

- Scott, Robert C. (2007). Making communities safer: Youth violence and gang interventions that work. Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, U.S. House of Representatives, One Hundred Tenth Congress, First Session. Serial 110-14. U.S. Government Printing Office. Retrieved February 25, 2010, from <http://judiciary.house.gov/hearings/printers/110th/33314.PDF>
- Shinn, David H. (2009). Somalia's new government and the challenge of Al-Shabaab. Retrieved September 28, 2009, from <https://www.hsdl.org>
- Simmons, Rob. (2006). The homeland security implications of radicalization. Hearing before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. Retrieved August 18, 2009, from http://www.fas.org/irp/congress/2006_hr/radical.pdf
- Spergel, Irving A. (1992). Community mobilization technical assistance manual. School of Social Service Administration, University of Chicago. Retrieved June 7, 2010, from <http://www.ncjrs.gov/textfiles/d0015.txt>
- Spergel, Irving A., Wa, Kwai Ming, & Sosa, Rolando Villarreal. 2006. The comprehensive, community-wide gang program model: Success and failure. In James F. Short, Jr. & Lorine A. Hughes (Eds.), *Studying youth gangs* (pp. 203–24). Lanham, MD: AltaMira Press.
- Temple-Raston. (2009). Missing Somali teens may be terrorist recruits. NPR News Online (January 28, 2009). Retrieved November 5, 2010, from <http://www.npr.org/templates/story/story.php?storyId=99919934>
- Tyre, Peg. (2006). The trouble with boys. *Newsweek* (January 30, 2006). Retrieved December 1, 2009, from <http://www.msnbc.msn.com/id/1096522/site/newsweek/page4/print/1/displaymode/1098>
- United States Census. (2010). Retrieved April 25, 2010, from <http://www.census.gov/>
- United States Department of Homeland Security. (2010). Quadrennial homeland security review (QHSR) 2010. Retrieved December 1, 2010, from http://www.dhs.gov/xabout/gc_1208534155450.shtm
- United States Department of Justice. (2007) Press Release: U.S. citizen sentenced to prison for receiving military training from a terrorist organization. Retrieved November 30, 2010, from http://www.justice.gov/opa/pr/2007/July/07_nsd_531.html

- United States Department of Justice. (2009a). Press Release: Two men charged with material support to terrorists, conspiracy to kill in a foreign country and other offenses. Retrieved November 30, 2010, from <http://www.justice.gov/usao/ma/Press%20Office%20-%20Press%20Release%20Files/Nov2009/MehannaIndictmentPR.html>
- United States Department of Justice. (2009b). Press Release: Terror charges unsealed in Minneapolis against eight men, Justice Department announces. Retrieved November 24, 2009, from <http://www.justice.gov/opa/pr/2009/November/09-nsd-1267.html>
- United States Department of Justice. (2010a). Press Release: Fourteen charged with providing material support to Somalia-based terrorist organization Al-Shabaab. Retrieved November 24, 2009, from <http://www.justice.gov/opa/pr/2010/August/10-ag-898.html>
- United States Department of Justice. (2010b). Press Release: Virginia man pleads guilty to providing material support to a foreign terrorist organization and encouraging violent jihadists to kill U.S. citizens. Retrieved November 2, 2010, from <http://www.justice.gov/opa/pr/2010/October/10-nsd-1174.html>
- United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention. (2008). Best practices to address community gang problems: OJJDP's comprehensive gang model. Prepared by the National Youth Gang Center. <http://ojjdp.ncjrs.gov/Publications/PubAbstract.asp?pubi=244701>
- United States Department of State. (2008). Designation of al-Shabaab as a specially designated global terrorist. Public Notice 6137 by the Office of the Coordinator for Counterterrorism. Retrieved November 5, 2010, from <http://www.state.gov/s/ct/rls/other/des/102448.htm>
- Vigil, J.D. (2003). Urban violence and street gangs. *Annual Review of Anthropology* 32(1), pp. 225–42. Retrieved August 11, 2010, from <http://web.ebscohost.com.libproxy.nps.edu/ehost/pdfviewer/pdfviewer?vid=2&hid=11&sid=a1ffbad3-6a38-4927-9eef-0f40b4afcccf%40sessionmgr14>
- Waterman, Shaun. (2009). Somali militia pledges allegiance to bin Laden. *Washington Times* (September 23, 2009), pp. A1, A14.

- Weine, Stevan, Horgan, John, Robertson, Cheryl, Loue, Sana, Mohamed, Amin, & Noor, Sahra. (2009). Community and family approaches to combating the radicalization and recruitment of Somali-American youth and young adults: A psychosocial perspective, *Dynamics of Asymmetric Conflict* 2(3), pp.181–200. Retrieved July 29, 2010, from <http://www.informaworld.com/smpp/content~db=all?content=10.1080/17467581003586897>
- Weine, S.M., Ware, N., & Klebic, A. (2004). An ethnographic study of converting cultural capital in teen refugees and their families from Bosnia-Herzegovina. *Psychiatric Services* 55, pp. 923–27. Retrieved July 29, 2010, from <http://psychservices.psychiatryonline.org/cgi/reprint/55/8/923?submit.y=19&submit.x=63&gca=55%2F8%2F923&>
- White House. (2009). Remarks by the President on a new beginning. Retrieved April 25, 2010, from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-at-Cairo-University-6-04-09/
- Zimbardo, P. (2007). *The Lucifer effect*. New York: Random House.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California




74 PAGE(S) OF RECORDS

Referred to National Counterterrorism
Center

DHS's Countering Violent Extremism and Active Shooter (CVE-AS) Mission

THE DEPARTMENT OF HOMELAND SECURITY (DHS) VISION

The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. Three key concepts form the foundation of our national homeland security strategy designed to achieve this vision:

-  Security
-  Resilience
-  Customs and Exchange

DHS's VIOLENT EXTREMISM PREVENTION AND ACTIVE SHOOTER MISSION:

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. Additionally, the trends of Active Shooter individuals have grown more complex with numerous motivating factors. Groups and individuals inspired by a range of personal, religious, political, or other ideological beliefs have promoted and used violence. Accordingly, DHS has designed a Countering Violent Extremism and Active Shooter (CVE-AS) approach that applies to all forms of violent extremism, regardless of ideology; which focuses not on radical thought or speech, but instead on preventing violent attacks. Increasingly sophisticated use of the internet, mainstream and social media, and information technology by violent extremists and active shooters adds an additional layer of complexity.

To counter violent extremism and prevent active shooter incidents, the Department is working with a broad range of government and civilian partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to potential violent and/or terrorist activity; and the best ways to mitigate or prevent that activity. Supporting communities and local law enforcement through collaboration, information sharing, and outreach efforts (e.g. 'See Something, Say Something'TM and 'Run, Hide, Fight') is imperative to bringing awareness to the public and accurate, appropriate, and relevant information to our federal, state and local partners. This approach supports our stakeholders to prevent, protect against, mitigate, respond to, and recover from threats or incidents.

Our approach to CVE and AS emphasizes the strength of local communities. DHS aims to enhance incident preparedness through a "whole community" approach by providing training, products, and resources to a broad range of stakeholders on issues such as active shooter awareness and violent extremism. We begin with the premise that well-informed and –equipped families, communities, and local institutions represent the best defense against violent and terrorist ideologies. And while our primary purpose is to prevent an active shooter incident or a terrorist and violent extremist attack by an individual or group recruited by violent extremist organization or inspired by a violent extremist ideology, we also support strong and resilient communities as important ends themselves.

CVE-AS MISSION PRIORITIES:

The Department's efforts are categorized into three broad objectives, listed below:

- ✚ Understanding Violent Extremism - Support and coordinate efforts to better understand the phenomenon of individual and group violent extremism, including assessing the threat it poses to the nation as a whole within specific communities;
- ✚ Support Local Communities - Bolster efforts to catalyze, prepare, and support non-governmental, community-based programs, and strengthen relationships with communities that may experience an active shooter event or be targeted for recruitment by violent extremists; and
- ✚ Support Local Law Enforcement – Disrupt and deter recruitment or individual mobilization through support for local law enforcement programs, including information-driven, community-oriented policing efforts that for decades have proven effective in preventing violent crime.

HSIN CVE-AS Web Portal:

One of the venues utilized by DHS to promote information and intelligence sharing on a broad range of topics is the joint DHS and FBI Countering Violent Extremism and Active Shooter (CVE-AS) web portal on DHS's Homeland Security Information Network (HSIN). The new CVE-AS portal provides a more user-friendly environment to promote information sharing and collaboration between Federal, State, Local, Private, civilian, and International entities working to counter the threat of violent extremists and help prevent active shooter incidents.

The portal provides a well-organized listing of topics so users can quickly locate and access the information relevant to their interests. The Portal provides videos and training resources as well as a document library with intelligence, federal, academia, and other resources covering numerous CVE and AS topics. It provides a forum for the exchange of Unclassified For Official Use Only (FOUO), Sensitive But Unclassified (SBU) and Law Enforcement Sensitive (LES) information to sworn, full-time, Federal, State and Local law enforcement officers; federal employees affiliated with the criminal justice system or intelligence communities; military personnel and government agencies associated with infrastructure protection of the United States. The CVE-AS web portal also shares Unclassified FOUO and SBU information with private sector partners, civilian security personnel, corporate executives, educational institutions/academia, international federal and Law Enforcement partners, community leaders and other State and Local partners, as appropriate. In addition, the portal includes information on outreach initiatives, subject matter experts and forums to provide feedback, share products and ask questions.

To implement this approach, we are working closely with our federal and international partners, as well as our many partners at the community, state, local, and tribal level across the country. We are an important partner in supporting the *National Strategy on Empowering Local Partners to Prevent Violent Extremism* and the *Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States* which President Obama released in 2011 and the *Implementing Recommendations of the 9/11 Commission Act of 2007*.

For more information on the CVE-AS mission and who can obtain access to the portal, visit www.dhs.gov/cveas-portal.

Suspicious Activity Indicators

DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY

Category	Description of Possible Indicator
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents (classified or unclassified), which are proprietary to the facility.
Sabotage/Tampering/Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.

POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION***

Category	Description of Possible Indicator
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., which would arouse suspicion in a reasonable person.
Testing or Probing of Security Recruiting	Deliberate interactions with, or challenges to installations, personnel, or systems that reveal physical, personnel or cyber security capabilities. Building of operations teams and contacts, personnel data or travel data.
Recruiting	Building operations teams and contacts, personnel data, banking data, or travel data.
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras) etc.
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.

Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.

*****Note:** These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

If you witness any of the above defined criminal activities or valid suspicious behaviors, please contact your local Police Station and/or local FBI Field Office.

18 PAGE(S) OF RECORDS

Referred to DHS S&T

40 PAGE(S) OF DOCUMENT(S)

Referred to Department of Justice

141 PAGE(S) OF RECORDS

Referred to DHS PRIVACY OFFICE

Middle East Broadcasting Networks, Inc.

Fast Facts

Audience	Weekly reach of more than 25 million
Headquarters	Springfield, Va.
Language	Arabic
Outlets	Alhurra TV, Alhurra-Iraq, Radio Sawa, Afia Darfur, RadioSawa.com and Alhurra.com

Overview

The Middle East Broadcasting Networks, Inc. (MBN) is a non-profit grantee of the Broadcasting Board of Governors that operates Alhurra Television and Radio Sawa. MBN is a multimedia organization that enables the U.S. to communicate to the Middle East via television, radio and the Internet.

Alhurra Television broadcasts objective and accurate Arabic-language news and information to 22 countries throughout the Middle East and North Africa. In addition to reporting on world

events, Alhurra provides context and analysis to give viewers a broader understanding of the actions impacting the region.

MBN also broadcasts a second channel specifically for Iraq. Alhurra-Iraq is broadcast via satellite, as well as via terrestrial transmitters in five Iraqi cities. Alhurra-Iraq's news and current affairs programs concentrate on issues facing the Iraqi viewers as they move into a new era, rebuilding their country.

Launched in 2002, Radio Sawa effectively reaches a significant portion of the influential under-35 population of the Middle East. Broadcasting 24/7, mostly on FM, Radio Sawa provides its audience with reliable and objective up-to-date news, interesting information and an upbeat blend of mainstream Western and Arabic popular music. Radio Sawa broadcasts more than six hours of news and information each day.

Alhurra and Radio Sawa's all news Websites provide the most up-to-date news and information in Arabic on the Web.

Mission

MBN's mission is to provide objective, accurate, and relevant news and information to the people of the Middle East about the region, the world, and the United States. MBN supports democratic values by expanding the spectrum of ideas, opinions, and perspectives available in the region's media.

Staff

MBN's Arabic-speaking editorial staff generates much of the news from a facility in Springfield, Va. Alhurra and Radio Sawa have bureaus and production centers in Baghdad, Dubai, Beirut, Cairo and Jerusalem, as well as correspondents and stringers throughout the Middle East and the United States.

Distribution

Alhurra and Alhurra-Iraq are distributed around-the-clock on Nilesat and Arabsat covering the entire Arab-speaking world from the Atlantic Ocean to the Gulf. Additionally, Alhurra-Iraq is also available terrestrially in Baghdad, Al Hilla, Basra, Tekreet, and Mosul. Alhurra HD is broadcast on Eutelsat Hotbird. Live streaming can be found at www.alhurra.com.

Radio Sawa broadcasts on FM in Jordan, Kuwait, United Arab Emirates, the Palestinian Territories, Qatar, Lebanon, Bahrain, Morocco, Sudan, Libya, Mauritania and Djibouti as well as in Iraq. It is broadcast on medium wave (AM) from transmitters in Cyprus (covering Egypt, Lebanon, Syria, Gaza and the Eastern Mediterranean), in UAE (covering parts of Saudi Arabia), in Kuwait (covering Iraq) and in Djibouti (covering Sudan, Yemen and parts of Saudi Arabia). Radio Sawa is also available on Arabsat, Nilesat and Eutelsat Hotbird. Streaming audio is available on the Internet at www.radiosawa.com.

For more information about MBN contact:
Deirdre Kline, MBN Director of Communications
703-852-9250 dkline@alhurra.com

Raise Your Voice

The Middle East Broadcasting Networks (MBN) *Raise Your Voice* campaign is designed as a platform that encourages Iraqi citizens to speak out and be a part of the discussion about the fight against extremism and the underlying causes of terrorism. MBN's brands have established their credibility in the highly biased media environment by presenting accurate and objective news and information. MBN brands reach nearly 41% of the adult Iraqi population weekly, and 85% of the audience say that Alhurra-Iraq and Radio Sawa's content is credible.

How *Raise Your Voice* (RYV) campaign is different:

- Instead of responding to daily news events, the RYV campaign focuses on the underlying conditions that have allowed Daesh to grow. RYV explores topics such as women's rights, free speech, sectarian tension, unemployment, lack of youth opportunities, religious intolerance, and the building of a fair and equitable civil society.
- RYV leverages the reach and credibility of MBN brands. When consuming Alhurra-Iraq and Radio Sawa, Iraqis know they are watching, listening and reading opinions and discussions without political and sectarian bias.
- RYV provides an opportunity for the Iraqi population to voice their opinions and discuss issues relevant to their daily lives. The campaign will crossover digital, television and radio making it accessible to all Iraqis.
- The goal is to encourage Iraqis to seek constructive solutions to the problems that afflict this troubled country.

The main components of the RYV campaign are:

DIGITAL

- ***www.irfaasawtak.com***-- This interactive website creates a community where the underlying causes for extremism are discussed openly and respectfully. The website concentrates on a different theme every week and will be a platform where essayists, reporters and the broader community can share their thoughts and opinions.

TELEVISION

- ***What is Your Opinion***—A weekly call-in program that would provide Iraqi citizens an outlet to share their thoughts and feelings towards the situation in Iraq. The show will host Iraqi government officials, religious figures and community leaders who can answer questions and share their perspectives with Iraqi callers.
- ***Your Question***—This monthly program serves as a platform where activists, young people and students can ask questions to people they do not normally have access to. Each episode will focus on a different topic such as freedom of expression, sectarian relationships and the importance of interfaith harmony.
- ***From Irbil***—Kurdistan is not well represented in the major Arabic-language satellite television networks. *From Irbil* will be a weekly program in Arabic that reports from the streets of Kurdistan and will focus on the plurality of Iraq, discussing issues that are important to Kurds, Shias and Sunnis.
- ***Light Among Us***—A weekly program coming from the streets of Iraq, it will be dedicated to stories of Iraqis who have overcome challenges and obstacles to better their lives and their country despite the current crisis.
- ***Delusional Paradise***—A weekly program from across the MENA region that features stories of families and communities who have suffered at the hands of Daesh. Whether it is a family member that has joined Daesh or a community that has lost loved ones at the hands of the extremist group, the program examines how people throughout the region are struggling to cope and tell the true story of the savagery of Daesh.

RADIO

- ***What is Your Opinion***—A daily call-in program on Radio Sawa's Iraq stream during evening drive time. The program's two Iraqi hosts will field calls and social media interaction throughout the program. Like its counterpart on TV, this program will discuss topics that serve as the root causes of Daesh.

For more information about MBN or Raise Your Voice contact:

Deirdre Kline, MBN Director of Communications

703-852-9250

dkline@alhurra.com

7600 BOSTON BOULEVARD, SPRINGFIELD, VIRGINIA 22153





STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

DECEMBER 2011





Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States

As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it. At the same time, countering al-Qa'ida's violent ideology is one part of our comprehensive strategy to defeat al-Qa'ida. Over the past 2½ years, more key al-Qa'ida leaders—including Usama bin Laden—have been eliminated in rapid succession than at any time since the September 11 attacks. We have strengthened homeland security and improved information sharing. Thanks to coordinated intelligence and law enforcement, numerous terrorist plots have been thwarted, saving many American lives.

—President Barack Obama, August 2011

Law enforcement and government officials for decades have understood the critical importance of building relationships, based on trust, with the communities they serve. Partnerships are vital to address a range of challenges and must have as their foundation a genuine commitment on the part of law enforcement and government to address community needs and concerns, including protecting rights and public safety. In our efforts to counter violent extremism, we will rely on existing partnerships that communities have forged with Federal, State, and local government agencies. This reliance, however, must not change the nature or purpose of existing relationships. In many instances, our partnerships and related activities were not created for national security purposes but nonetheless have an indirect impact on countering violent extremism (CVE).

At the same time, this Strategic Implementation Plan (SIP) also includes activities, some of them relatively new, that are designed specifically to counter violent extremism. Where this is the case, we have made it clear. It is important that both types of activities be supported and coordinated appropriately at the local level.

Background

The President in August 2011 signed the *National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States* (National Strategy for Empowering Local Partners), which outlines our community-based approach and the Federal Government's role in empowering local stakeholders to build resilience against violent extremism.¹ It recognizes that, as the National Security Strategy from May 2010 highlights, "our best defenses against this threat are well informed and equipped families, local communities, and institutions." To support our overarching goal of preventing violent extremists and their supporters from inspiring, radicalizing, financing, or recruiting individuals or groups in the

1. The National Strategy for Empowering Local Partners defines violent extremists as "individuals who support or commit ideologically motivated violence to further political goals."

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

United States to commit acts of violence, the Federal Government is focused on three core areas of activity: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals.

The SIP details how we are implementing the National Strategy for Empowering Local Partners. It explains our core objectives and sub-objectives; describes how activities by departments and agencies are aligned with these; lists planned activities that address gaps and expand efforts; and assigns Federal Government leads and partners for various actions. The SIP provides a blueprint for how we will build community resilience against violent extremism.² It does not address our overseas CVE efforts, other than ensuring we coordinate domestic and international activities.

Although the SIP will be applied to prevent all forms of violent extremism, we will prioritize preventing violent extremism and terrorism that is inspired by al-Qa'ida and its affiliates and adherents, which the 2010 National Security Strategy, the 2011 National Strategy for Counterterrorism, and the National Strategy for Empowering Local Partners identify as the preeminent security threats to our country. This is, however, a matter of emphasis and prioritization, and does not entail ignoring other forms of violent extremism. As the July 2011 terrorist attack in Norway underscored, free societies face threats from a range of violent extremists.

As the activities described in the SIP are executed, there will be major and long-lasting impacts:

- There will be platforms throughout the country for including communities that may be targeted by violent extremists for recruitment and radicalization into ongoing Federal, State, and local engagement efforts;
- The Federal Government will support that engagement through a task force of senior officials from across the government;
- Community-led efforts to build resilience to violent extremism will be supported;
- Analysis will increase in depth and relevance, and will be shared with those assessed to need it, including Governor-appointed Homeland Security Advisors, Major Cities Chiefs, Mayors' Offices, and local partners;
- Training for Federal, State, tribal, and local government and law enforcement officials on community resilience, CVE, and cultural competence will improve, and that training will meet rigorous professional standards; and
- Local partners, including government officials and community leaders, will better understand the threat of violent extremism and how they can work together to prevent it.

2. The concept of "resilience" has applied to a range of areas such as emergency preparedness and critical infrastructure protection (e.g., the ability of financial markets, power suppliers, and telecommunications companies to withstand an attack or disaster and resume operations rapidly.) The National Security Strategy emphasized the importance of including individuals and communities in our approach to enhancing resilience. Both the National Strategy for Empowering Local Partners and the 2011 National Strategy for Counterterrorism expanded this concept to CVE, the latter explicitly stating, "We are working to bring to bear many of these capabilities to build resilience within our communities here at home against al-Qa'ida inspired radicalization, recruitment, and mobilization to violence."

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

The SIP outlines ongoing, as well as planned, activities to counter violent extremism, which will be accomplished through existing funding and by prioritizing within the resources available to relevant departments and agencies. Some of these activities are specific to CVE, while others address broader non-security policy objectives but may have an indirect effect on countering radicalization to violence. Because our efforts are threaded across a range of different missions, such as training, outreach, and international exchanges, the execution of the SIP will be impacted by funding for both security and non-security related activities.

Process for Developing the SIP

The Obama Administration continues to prioritize and stress the critical importance of CVE in the Homeland. Given the complexities of addressing this threat and the uniqueness of the operating environment in the United States, the Administration recognizes the potential to do more harm than good if our Nation's approach and actions are not dutifully considered and deliberated. Throughout this process, careful consideration was given to the rule of law and constitutional principles, particularly those that address civil rights and civil liberties. With those principles in mind, we noted that departments and agencies with domestically focused mandates have an array of tools and capabilities that can be leveraged to prevent violent extremism, though some have limited experience in the national security arena. This necessitated a deliberative and carefully calibrated approach with an extensive evaluative period to fully address their potential roles and participation, which for some entailed thinking outside their traditional mandates and areas of work.

After assessing how individuals are radicalized and recruited to violence in the United States, the Administration established an accelerated process, led by the National Security Staff (NSS), to develop the National Strategy for Empowering Local Partners and the SIP. An Interagency Policy Committee (IPC) on countering and preventing violent extremism in the United States was established—with Assistant and Deputy Assistant Secretary-level representatives from across government—to consider roles and responsibilities, potential activities, guiding principles, and how best to coordinate and synchronize our efforts. The IPC, with support from specialist sub-IPCs, drafted our first national strategy on preventing violent extremism in the United States, which was approved by Deputies from the various departments and agencies and signed by the President.

- The following departments and agencies were involved in the deliberations and approval process: the Departments of State (State), the Treasury, Defense (DOD), Justice (DOJ), Commerce, Labor, Health and Human Services (HHS), Education (EDU), Veterans Affairs, and Homeland Security (DHS), as well as the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC).

To develop the SIP, the NSS tasked NCTC with coordinating the first comprehensive baseline of activities across the United States Government related to countering and preventing violent extremism in the United States, which constitutes the ongoing activities outlined in the SIP. This included CVE-specific initiatives, as well as activities that were not developed for CVE purposes, but nonetheless may indirectly contribute to the overall goals of the National Strategy for Empowering Local Partners. These activities were aligned with objectives and sub-objectives—based on the strategy and approved by the IPC—to

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

assess our overall effort and identify gaps. The IPC then considered ongoing and potential actions to address these gaps, which form the basis of planned activities outlined in the SIP. The SIP was approved by Deputies from the various departments and agencies in November 2011.

Compliance with the Rule of Law

A fundamental precept of the SIP is that the Federal Government's actions must be consistent with the Constitution and in compliance with U.S. laws and regulations. Departments and agencies are responsible for identifying and complying with legal restrictions governing their activities and respective authorities. Compliance with the rule of law, particularly ensuring protection of First Amendment rights, is central to our National Strategy for Empowering Local Partners and the execution of the SIP.

Crosscutting and Supportive Activities

There are fundamental activities that are critical to our success and cut across the objectives of the SIP. These include: (1) whole-of-government coordination; (2) leveraging existing public safety, violence prevention, and community resilience programming; (3) coordination of domestic and international CVE efforts, consistent with legal limits; and (4) addressing technology and virtual space. In many instances, these crosscutting and supportive activities describe the ongoing activities of departments and agencies in fulfilling their broader missions. As they implement new initiatives and programs in support of the SIP, departments and agencies will ensure these enabling activities appropriately guide their efforts.

1. Whole-of-Government Coordination

Leveraging the wide range of tools, capabilities, and resources of the United States Government in a coordinated manner is essential for success. Traditional national security or law enforcement agencies such as DHS, DOJ, and the FBI will execute many of the programs and activities outlined in the SIP. However, as the National Strategy for Empowering Local Partners states, we must also use a broader set of good governance programs, "including those that promote immigrant integration and civic engagement, protect civil rights, and provide social services, which may also help prevent radicalization that leads to violence." To this end, agencies such as EDU and HHS, which have substantial expertise in engaging communities and delivering services, also play a role.

This does not mean the missions and priorities of these partners will change or that their efforts will become narrowly focused on national security. Their inclusion stems from our recognition that radicalization to violence depends on a variety of factors, which in some instances may be most effectively addressed by departments and agencies that historically have not been responsible for national security or law enforcement. These non-security partners, including specific components within DOJ and DHS, have an array of tools that can contribute to this effort by providing indirect but meaningful impact on CVE, including after school programs, networks of community-based organizations that provide assistance to new immigrants, and violence prevention programs. We will coordinate activities, where appropriate, to support the CVE effort while ensuring we do not change the core missions and functions of these departments and agencies.

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

2. Leveraging Existing Public Safety, Violence Prevention, and Resilience Programming

While preventing violent extremism is an issue of national importance, it is one of many safety and security challenges facing our Nation. As we enter an era of increased fiscal constraints, we must ensure our approach is tailored to take advantage of current programs and leverages existing resources. Our efforts therefore will be supported, where appropriate, by emphasizing opportunities to address CVE within available resources related to public safety, violence prevention, and building resilience.

3. Coordination of Domestic and International Efforts

While always ensuring compliance with applicable laws and regulations, we must ensure a high level of coordination between our domestic and international efforts to address violent extremism. Although both the National Strategy for Empowering Local Partners and the SIP specifically address preventing violent extremism in the United States, the delineation between domestic and international is becoming increasingly less rigid. Violent extremists operating abroad have direct access to Americans via the Internet, and overseas events have fueled violent extremist radicalization and recruitment in the United States. The converse is also true: events occurring in the United States have empowered the propaganda of violent extremists operating overseas. While making certain that they stay within their respective authorities, departments and agencies must ensure coordination between our domestic and international CVE efforts. Given its mandate to support both domestic and international planning, NCTC will help facilitate this part of the CVE effort so that our Homeland and overseas activities are appropriately synchronized, consistent with all applicable laws and regulations. While individual departments and agencies will regularly engage foreign partners, all international engagement will continue to be coordinated through State.

4. Addressing Technology and Virtual Space

The Internet, social networking, and other technology tools and innovations present both challenges and opportunities. The Internet has facilitated violent extremist recruitment and radicalization and, in some instances, attack planning, requiring that we consider programs and initiatives that are mindful of the online nature of the threat. At the same time, the Federal Government can leverage and support the use of new technologies to engage communities, build and mobilize networks against violent extremism, and undercut terrorist narratives. All of our activities should consider how technology impacts radicalization to violence and the ways we can use it to expand and improve our whole-of-government effort. As noted in sub-objective 3.3, we will develop a separate strategy focused on CVE online.

Roles and Responsibilities

The SIP assigns Leads and Partners in each of the Future Activities and Efforts listed under respective sub-objectives. Leads and Partners have primary responsibility for coordinating, integrating, and synchronizing activities to achieve SIP sub-objectives and the overall goal of the National Strategy for Empowering Local Partners.

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

Expectation of Leads and Partners are as follows:

Lead: A department or agency responsible for convening pertinent partners to identify, address, and report on steps that are being taken, or should be taken, to ensure activities are effectively executed. The Lead is accountable for, among other things:

- Fostering communication among Partners to ensure all parties understand how to complete the activity;
- Identifying, in collaboration with assigned Partners, the actions and resources needed to effectively execute the activity;
- Identifying issues that impede progress; and
- Informing all departments and agencies about the status of progress by the Lead and other sub-objective Partners, including impediments, modifications, or alterations to the plan for implementation.

Partner: A department or agency responsible for collaborating with a Lead and other Partners to accomplish an activity. Partner(s) are accountable for:

- Accomplishing actions under their department or agency's purview in a manner that contributes to the effective execution of an activity;
- Providing status reports and assessments of progress on actions pertinent to the activity; and
- Identifying resource needs that impede progress on their department or agency's activities.

Assessing Progress

It is important to recognize that the National Strategy for Empowering Local Partners represents the first time the United States Government has outlined an approach to address ideologically inspired violent extremism in the Homeland. While the objectives and sub-objectives listed in the SIP represent the collective wisdom and insight of the United States Government about what areas of action have the greatest potential to prevent violent extremism, we will learn more about our effectiveness as we assess our efforts over time, and we will adjust our activities accordingly.

Given the short history of our coordinated, whole-of-government approach to CVE, we will first develop key benchmarks to guide our initial assessment. Where possible, we will also work to develop indicators of impact to supplement these performance measures, which will tell us whether our activities are having the intended effects with respect to an objective or sub-objective. As we implement our activities, future evaluations will shift away from benchmark performance measures towards impact assessments. Departments and agencies will be responsible for assessing their specific activities in pursuit of SIP objectives, in coordination with an Assessment Working Group. We will develop a process for identifying gaps, areas of limited progress, resource needs, and any additional factors resulting from new information on the dynamics of radicalization to violence. Our progress will be evaluated and reported annually to the President.

Objectives, Sub-Objectives, and Activities

The SIP's objectives mirror the National Strategy for Empowering Local Partners' areas of priority action: (1) enhancing Federal engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting our ideals. Each of these is supported by sub-objectives, which constitute measurable lines of effort with which our specific programs and initiatives are aligned. A key purpose of the SIP is to describe the range of actions we are taking to improve or expand these efforts.

1. Enhancing Federal Engagement with and Support to Local Communities that May be Targeted by Violent Extremists

Communication and meaningful engagement with the American public is an essential part of the Federal Government's work, and it is critical for developing local partnerships to counter violent extremism. Just as we engage and raise awareness to prevent gang violence, sexual offenses, school shootings, and other acts of violence, so too must we ensure that our communities are empowered to recognize threats of violent extremism and understand the range of government and nongovernment resources that can help keep their families, friends, and neighbors safe. As noted in the National Strategy for Empowering Local Partners:

Engagement is essential for supporting community-based efforts to prevent violent extremism because it allows government and communities to share information, concerns, and potential solutions. Our aims in engaging with communities to discuss violent extremism are to: (1) share sound, meaningful, and timely information about the threat of violent extremism with a wide range of community groups and organizations, particularly those involved in public safety issues; (2) respond to community concerns about government policies and actions; and (3) better understand how we can effectively support community-based solutions.

At the same time, we must ensure that our efforts to prevent violent extremism do not narrow our relationships with communities to any single issue, including national security. This necessitates continuing to engage on the full range of community interests and concerns, but it also requires, where feasible, that we incorporate communities that are being targeted by violent extremists into broader forums with other communities when addressing non-CVE issues. While we will engage with some communities specifically on CVE issues because of particular needs, care should be taken to avoid giving the false impression that engagement on non-security issues is taking place exclusively because of CVE concerns. To ensure transparency, our engagement with communities that are being targeted by violent extremists will follow two tracks:

- We will specifically engage these communities on the threat of violent extremism to raise awareness, build partnerships, and promote empowerment. This requires specific conversations and activities related to security issues.
- Where we engage on other topics, we will work to include them in broader forums with other communities when appropriate.

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

1.1 Improve the depth, breadth, and frequency of Federal Government engagement with and among communities on the wide range of issues they care about, including concerns about civil rights, counterterrorism security measures, international events, and foreign policy issues.

Violent extremist narratives espouse a rigid division between “us” and “them” that argues for exclusion from the broader society and a hostile relationship with government and other communities. Activities that reinforce our shared sense of belonging and productive interactions between government and the people undercut this narrative and emphasize through our actions that we are all part of the social fabric of America. As President Obama emphasized, when discussing Muslim Americans in the context of al-Qa’ida’s attempts to divide us, “we don’t differentiate between them and us. It’s just us.”

Current Activities and Efforts

Departments and agencies have been conducting engagement activities based on their unique mandates. To better synchronize this work, U.S. Attorneys, who historically have engaged with communities in their districts, have begun leading Federal engagement efforts. This includes our efforts to engage with communities to (1) discuss issues such as civil rights, counterterrorism security measures, international events, foreign policy, and other community concerns; (2) raise awareness about the threat of violent extremism; and (3) facilitate partnerships to prevent radicalization to violence. The types of communities involved in engagement differ depending on the locations. United States Attorneys, in consultation with local and Federal partners, are best positioned to make local determinations about which communities they should engage. Appointed by the President and confirmed by the Senate, U.S. Attorneys are the senior law enforcement and executive branch officials in their districts, and are therefore well-placed to help shape and drive community engagement in the field.

In December 2010, 32 U.S. Attorneys’ Offices began expanding their engagement with communities to raise awareness about how the United States Government can protect all Americans from discrimination, hate crimes, and other threats; to listen to concerns; and to seek input about government policies and programs. In some instances, these efforts also included initiatives to educate the public about the threat of violent extremist recruitment, which is one of many components of a broader community outreach program.

- During this initial pilot, these U.S. Attorneys significantly expanded outreach and engagement on a range of issues of interest to communities; built new relationships where needed; and communicated the United States Government’s approach to CVE.
- Departments and agencies, including State, the Treasury, EDU, HHS, and DHS provided information, speakers, and other resources for U.S. Attorneys’ community engagement activities, frequently partnering with DOJ on specific programs and events.

A National Task Force, led by DOJ and DHS, was established in November 2010 to help coordinate community engagement at the national level. It includes all departments and agencies involved in relevant community engagement efforts and focuses on compiling local, national, and international best practices and disseminating these out to the field, especially to U.S. Attorneys’ Offices. The Task Force is also responsible for connecting field-based Federal components to the full range of United States Government officials involved in community engagement to maximize partnerships,

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

coordination, and resource-sharing. The following are some examples of engagement efforts that are, or will be, coordinated with the Task Force:

- The DHS Office for Civil Rights and Civil Liberties (CRCL) this year doubled its outreach to communities and expanded its quarterly engagement roundtables to 14 cities throughout the country. During Fiscal Year 2011, CRCL also conducted 72 community engagement events, some of which included CVE-related topics.
- State engaged on U.S. foreign policy with a range of interested domestic communities. The Bureau of Near Eastern Affairs alone conducted 80 outreach events over the past year.
- DOJ has produced a number of brochures and other materials on civil rights protections and steps individuals can take to prevent or respond to discrimination, and has disseminated these to various communities, including those being targeted by violent extremists. DOJ has translated these materials into a number of languages, including Arabic, Somali, Urdu, Farsi, and Hindi.
- DOJ, in coordination with DHS, expanded the Building Communities of Trust (BCOT) Initiative, which focuses on developing relationships among local law enforcement departments, fusion centers, and the communities they serve to educate communities on: (1) the Nationwide Suspicious Activity Reporting Initiative (NSI); (2) how civil rights and liberties are protected; and (3) how to report incidents in order to help keep our communities safe. DOJ continues to support the BCOT Initiative.

Future Activities and Efforts

The primary focus for the next year will be: (1) expanding the scope of engagement; (2) building new partnerships between communities and local law enforcement, local government officials, and civil society; (3) incorporating communities that are being targeted by violent extremist radicalization into broader forums with other communities to engage on a range of non-security issues; and (4) increasing our engagement specifically on CVE. Additional activities going forward include the following:

- DOJ will incorporate more U.S. Attorneys' Offices as engagement leads in the field, building on the initial U.S. Attorney-led effort. (Lead: DOJ; Partners: All)
- The National Task Force will: (1) disseminate regular reports on best practices in community engagement to local government officials, law enforcement, U.S. Attorneys' Offices, and fusion centers; (2) work with departments and agencies to increase their support to U.S. Attorney-led engagement efforts in the field; and (3) closely coordinate Federal engagement efforts with communities targeted by violent extremist radicalization. (Leads: DOJ and DHS; Partners: All)
- In consultation with Federal and local partners, the National Task Force and the U.S. Attorneys' Offices will facilitate, where appropriate, the inclusion of communities that may be targeted by violent extremist radicalization into broader engagement forums and programs that involve other communities. (Leads: DOJ and DHS; Partners: All)
- U.S. Attorneys will coordinate closely with local government officials, law enforcement, communities, and civil society to enhance outreach events and initiatives. (Lead: DOJ; Partners: All)

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

- In Fiscal Year (FY) 2012, CRCL plans on expanding its quarterly community engagement roundtables to a total of 16. CRCL is also in the process of implementing a campus youth community engagement plan, through which it will engage with young adults on the topic of violent extremism. (Lead: DHS)
- Depending on local circumstances, and in consultation with the FBI and other agencies as appropriate, U.S. Attorneys will coordinate any expanded engagement specific to CVE with communities that may be targeted by violent extremist radicalization. (Lead: DOJ; Partners: DHS, NCTC, and FBI)
- An FBI CVE Coordination Office will be established and, as part of its activities, will coordinate with the National Task Force on CVE-specific education and awareness modules. These modules will be developed and implemented, in part, by leveraging some of the FBI's existing programs and initiatives. (Lead: FBI; Partners: DOJ and DHS)
- DHS will oversee an online portal to support engagement by government officials and law enforcement with communities targeted by violent extremist radicalization, which will be used to share relevant information and build a community of interest. The portal will be accessible to government officials and law enforcement involved in overseas and domestic CVE and community engagement efforts to share best practices. (Lead: DHS; Partners: State, and NCTC)
- DOJ will expand the efforts of the BCOT initiative to help facilitate trust between law enforcement and community leaders. This dialogue could include local issues, as well as CVE. (Lead: DOJ; Partner: DHS)
- The United States Government will build a digital engagement capacity in order to expand, deepen, and intensify our engagement efforts. Where possible, virtual engagement will build on real world engagement activities and programs. (Lead: DHS; Partners: All)

1.2 Foster community-led partnerships and preventative programming to build resilience against violent extremist radicalization by expanding community-based solutions; leveraging existing models of community problem-solving and public safety; enhancing Federal Government collaboration with local governments and law enforcement to improve community engagement and build stronger partnerships; and providing communities with information and training, access to resources and grants, and connections with the philanthropic and private sectors.

The Federal Government can foster nuanced and locally rooted counter-radicalization programs and initiatives by serving as a facilitator, convener, and source of information to support local networks and partnerships at the grassroots level. Importantly, because the dynamics of radicalization to violence frequently vary from location to location, we recognize that a one-size-fits-all approach will be ineffective.

Current Activities and Efforts

The Federal Government has held a series of consultative meetings with communities, local government and law enforcement, civil society organizations, foundations, and the private sector to better understand how it can facilitate partnerships and collaboration. This leverages a key strength identified

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

in the National Strategy for Empowering Local Partners: “The Federal Government, with its connections to diverse networks across the country, has a unique ability to draw together the constellation of previously unconnected efforts and programs to form a more cohesive enterprise against violent extremism.” Examples of this include the following:

- DHS Secretary Napolitano tasked her Homeland Security Advisory Council (HSAC) to develop recommendations on how the Department can best support law enforcement and communities in their efforts to counter violent extremism. An HSAC CVE Working Group convened multiple meetings with local law enforcement, local elected officials, community leaders (including faith-based leaders), and academics. The working group released its recommendations in August 2010, highlighting the importance of: (1) research and analysis of violent extremism; (2) engagement with communities and leveraging existing partnerships to develop information-driven, community-based solutions to violent extremism and violent crime; and (3) community oriented policing practices that focus on building partnerships between law enforcement and communities.
- DHS and NCTC began raising awareness about violent extremism among private sector actors and foundations and connected them with community civic activists interested in developing programs to counter violent extremism. DHS is now working with a foundation to pilot resiliency workshops across the country that address all hazards, including violent extremism.

We also began exploring how to incorporate CVE as an element of programs that address broader public safety, violence prevention, and resilience issues. This has the advantage of leveraging preexisting initiatives and incorporates CVE in frameworks (such as safeguarding children) used by potential local partners who may otherwise not know how they fit into such efforts. For example, although many teachers, healthcare workers, and social service providers may not view themselves as potentially contributing to CVE efforts, they do recognize their responsibilities in preventing violence in general. CVE can be understood as a small component of this broader violence prevention effort. Departments and agencies will review existing public safety, violence prevention, and resilience programs to identify ones that can be expanded to include CVE as one among a number of potential lines of effort.

- As an example, the Federal Government helped support a community-led initiative to incorporate CVE into a broader program about Internet safety. The program addressed protecting children from online exploitation, building community resilience, and protecting youth from Internet radicalization to violence.

Future Activities and Efforts

Planned activities to expand support to local partners include the following:

- The Federal Government will help broker agreements on partnerships to counter violent extremism between communities and local government and law enforcement to help institutionalize this locally focused approach. (Lead: DHS)
- DHS and DOJ will work to increase support for local, community-led programs and initiatives to counter violent extremism, predominantly by identifying opportunities within existing appropriations for incorporating CVE as an eligible area of work for public safety, violence prevention, and community resilience grants. (Leads: DHS and DOJ)

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

- DHS is working to increase funding available to integrate CVE into existing community-oriented policing efforts through FY12 grants. (Lead: DHS)
- DHS is establishing an HSAC Faith-Based Community Information Sharing Working Group to determine how the Department can: (1) better share information with faith communities; and (2) support the development of faith-based community information sharing networks. (Lead: DHS)
- DHS is developing its Hometown Security webpage to include resources such as training guidance, workshop reports, and information on CVE for both the general public and law enforcement. (Lead: DHS)
- The Treasury will expand its community outreach regarding terrorism financing issues. (Lead: Treasury; Partners: State, DOJ, DHS, FBI, and the U.S. Agency for International Development)³
- Depending on local circumstances and in consultation with the FBI, U.S. Attorneys will coordinate, as appropriate, any efforts to expand connections and partnerships at the local level for CVE, supported by the National Task Force where needed. (Lead: DOJ; Partners: All)
- Departments and agencies will expand engagement with the business community by educating companies about the threat of violent extremism and by connecting them to community civic activists focused on developing CVE programs and initiatives. (Lead: DHS; Partner: NCTC)

2. Building Government and Law Enforcement Expertise for Preventing Violent Extremism

It is critical that the Federal Government and its local government and law enforcement partners understand what the threat of violent extremism is, and what it is not. This helps ensure that we focus our resources where they are most effective and that we understand how we can best empower and partner with communities. Building expertise necessitates continued research about the dynamics of radicalization to violence and what has worked to prevent violent extremism; sharing this information as widely as possible; and then leveraging it to train government officials and law enforcement.

2.1 Improve our understanding of violent extremism through increased research, analysis, and partnerships with foreign governments, academia, and nongovernmental organizations.

The Federal Government has built a robust analytic program to understand violent extremism that includes analysis; research conducted by academia, think tanks, and industry; and exchanges with international allies to identify best practices. While we have increased our understanding of how individuals are radicalized to violence, we must continue to identify gaps, monitor changes in the dynamics of violent extremism, and remain vigilant by challenging our assumptions and continuing our research and analysis.

Current Activities and Efforts

The United States Government's research capacity on this issue has greatly expanded. DHS and NCTC both have analytic groups exclusively focused on violent extremist radicalization; the Interagency Intelligence Subcommittee on Radicalization helps coordinate and improve CVE intelligence analysis; and we work with foreign governments, academia, and nongovernmental organizations to inform and

3. The U.S. Agency for International Development's role will be limited to sharing relevant information.

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

supplement our analysis and understanding. In addition to a large volume of intelligence products on CVE, examples of activities include:

- DHS Science & Technology (S&T) sponsored research on violent extremism in the United States, which it has shared with DHS components and other departments and agencies. Over 20 reports have been produced since 2009 and 5 more will be produced by the end of 2011. DHS is also developing an integrated open source database to help inform CVE programs.
- DHS's Office of Intelligence and Analysis (I&A) collaborated with the FBI, the Bureau of Prisons (BOP), and NCTC to assess the capacity of state correctional institutions to detect and share information regarding individuals who demonstrate behaviors associated with violent extremism while in the correctional system.
- The National Intelligence Council, DHS, FBI, and NCTC briefed fusion centers and law enforcement around the country on violent extremism.
- DHS, in partnership with the FBI and NCTC, developed case studies on preoperational indicators and known threats for State and local law enforcement and affected communities.
- The United States Government held regular exchanges of best practices with Australia, Canada, Denmark, Germany, the European Union, the Netherlands, the United Kingdom, and other partners to gain comparative insights about what might be effective in the Homeland.
- DHS expanded cooperation between the United States and Canada on CVE research and lessons learned.
- The United States Government participates in the Global Counterterrorism Forum's CVE Working Group.
- As directed in the Fort Hood Follow-on Review, DOD established the Force Protection Senior Steering Group. Among the Steering Group's duties is the coordination of non-traditional partners' activities within DOD (e.g., counterintelligence and behavioral health) to better understand how to identify and prevent all forms of violent extremism—not limited to al-Qa'ida-inspired extremism—within the military, including the potential use of DOD's extensive network of programs designed to support individuals who are potentially at risk of committing acts of violence against themselves, their families, or co-workers.

Future Activities and Efforts

Although we have a better understanding of the threat, there are gaps that need to be addressed through additional research and analysis. In this regard, we will:

- Expand analysis in five priority areas (Leads: DHS, FBI, NCTC, and State):
 1. The role of the Internet in radicalization to violence and how virtual space can be leveraged to counter violent extremism.
 2. Single-actor terrorism (so called "lone wolves"), including lessons learned from similar phenomena such as a school shooters.
 3. Disengagement from terrorism and violent extremism.

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

4. Non-al-Qa'ida related radicalization to violence and anticipated future violent extremist threats.
 5. Preoperational indicators and analysis of known case studies of extremist violence in the United States.
- Continue DHS S&T's support for research on countering the threat of extremist violence. (Lead: DHS)
 - Continue DHS collaboration with the FBI, the BOP, and NCTC to: (1) improve awareness of the risk of violent extremism in correctional systems; (2) enhance screening of new inmates to detect individuals associated with violent extremist organizations; (3) improve detection of recruitment efforts within the correctional environment; and (4) increase information sharing, as appropriate, with Federal, State, and local law enforcement about inmates who may have adopted violent extremist beliefs and are being released. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
 - Complete the creation of the FBI CVE Coordination Office to help assess and leverage existing Bureau efforts to better understand and counter violent extremism. (Lead: FBI)
 - Build lines of research specifically to support non-security Federal partners. (Leads: DHS and NCTC; Partners: EDU and HHS)

2.2 Increase Federal Government information sharing with State, local, and tribal governments and law enforcement on terrorist recruitment and radicalization.

As we enhance our partnerships with State, local, and tribal governments and law enforcement to counter violent extremism, it is essential that we share our expertise and insights about the dynamics of radicalization to violence and what has worked to prevent it. This, in turn, will help our partners identify potential areas of collaboration with communities and other local actors.

Current Activities and Efforts

Examples include:

- Based on direction from the Office of the Director of National Intelligence (DNI), DHS led an effort to improve the analysis of homegrown violent extremism, including analytic tools to share with State, local, and tribal partners. DHS briefed representatives of 47 states on the project.
- DHS generated case studies of known and suspected terrorists and assessments of radicalization to violence, based on recent arrests, to share with local partners.
- FBI disseminated information to public safety partners, including information about radicalization to violence.
- DHS, NCTC, and FBI briefed and disseminated information on how individuals are radicalized to violence to law enforcement, fusion centers, and local government officials, including the Major Cities Chiefs, representatives from 47 states, Mayors' Offices, and State Homeland Security Advisors.

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

- In partnership with NCTC, DOJ, DNI, and FBI, DHS led the first National CVE Workshop in August 2011, which brought together intelligence commanders from major metropolitan areas and fusion center directors to increase their understanding of CVE.

Future Activities and Efforts

More work needs to be done to ensure our State, local, and tribal partners have the information they need to counter violent extremism. Classification remains an obstacle to broader sharing with these partners, but we can better ensure that analytic production is tailored to the needs of practitioners in the field. Major work over the next year will focus on creating more analytic products on CVE that directly support local law enforcement and government. Planned actions include:

- Development of an analytic team focused on supporting local government and law enforcement CVE practitioners and increased production of analysis at appropriate classification levels. (Lead: DHS; Partners: FBI and NCTC)
- Development of practitioner-friendly summaries of current research and literature reviews about the motivations and behaviors associated with single-actor terrorism and disengagement from violent extremism. (Lead: DHS)
- Review of information-sharing protocols to identify ways of increasing dissemination of products to State, local, and tribal authorities. (Leads: DHS, DOJ, FBI, and NCTC)
- Expansion of briefings and information sharing about violent extremism with State and local law enforcement and government. (Lead: DHS, FBI, and NCTC)

2.3 Improve the development and use of standardized training with rigorous curricula based on the latest research, which conveys information about violent extremism; improves cultural competency; and imparts best practices and lessons learned for effective community engagement and partnerships.

The Federal Government has expanded and improved training related to CVE over the past year, but challenges remain. In particular, there is a need for a review process and standards for training specific to CVE, which was underscored by a small number of instances of Federally sponsored or funded CVE-related and counterterrorism training that used offensive and inaccurate information, which was inconsistent with our values and core principles. As our National Strategy to Empower Local Partners highlights, “Misinformation about the threat and dynamics of radicalization to violence can harm our security by sending local stakeholders in the wrong direction and unnecessarily creating tensions with potential community partners.” Therefore, improving Federal Government-approved training practices and processes related to CVE is a top priority of this plan.

Current Activities and Efforts

In November 2010, the IPC tasked DHS to form an Interagency Working Group on Training to catalogue and recommend improvements for CVE-related training across government. The Working Group brought together individuals responsible for CVE training and substantive specialists from civil rights and civil liberties offices, Federal law enforcement, and the analytic community. This is part of our overall

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

emphasis on improving the quality and quantity of CVE-related training. Notable accomplishments in our efforts to improve training include:

- Between October 2010 and October 2011, DHS CRCL trained nearly 2,700 law enforcement officials on CVE and cultural awareness at 46 separate events. The training served as the basis for best practices recommended by the Interagency Working Group on Training.
- Based on input from participating agencies, DHS issued CVE training guidance and best practices in October 2011 for Federal, State, local, and tribal government officials charged with organizing training related to CVE, cultural awareness, and counterterrorism.
- The Federal Emergency Management Agency (FEMA) in October 2011 issued an Information Bulletin on CVE Training, which includes DHS's training guidance and best practices, as well as guidance for State, local, and tribal entities that regularly leverage FEMA grants to fund CVE-related trainings. DHS sent the best practices paper and the FEMA guidance to all DHS grantees, State and local governments, State and local law enforcement, relevant community stakeholders, and interagency partners.
- DHS provided a full-day of training, which included training on cultural competency, civil rights, and civil liberties to Federal, State, local, and tribal partners at 12 fusion centers in the past year and over 30 fusion centers since 2008. These trainings were coupled with 3- to 4-hour CVE training sessions for State and local law enforcement operating in the same state. Additionally, DHS provided "train the trainer" sessions for staff from nearly all fusion centers nationwide.
- DHS, working closely with other departments and agencies, local law enforcement, academics, and curriculum development experts, developed guidelines for a CVE curriculum that focuses on information-driven community-oriented policing practices and how to leverage existing community partnerships to counter violent extremism and violent crime. These guidelines were reviewed and validated in February 2011 at a "proof-of-concept" session at the Federal Law Enforcement Training Center (FLETC), which was attended by State, local, and tribal law enforcement executives and frontline officers from rural and major city jurisdictions.
- State, working closely with NCTC and DHS, piloted specialized CVE training for United States Government officials working on CVE in the United States and abroad through its Foreign Service Institute in May 2011. Participation by domestic and international practitioners provided opportunities for exchanging best practices, enhanced the coordination of our Homeland and overseas efforts, and encouraged interagency partnerships.

Future Activities and Efforts

A review process by the Interagency Working Group on Training, as well as internal assessments by departments and agencies, identified two key challenges, which we will address over the next year:

- Many departments and agencies lack a review process for training materials and outside speakers on CVE, which led to a small number of cases of training that violated internal principles as well as core tenets of the National Strategy to Empower Local Partners.

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

- There has been a lack of guidance and standards for training related to CVE, which left field offices, in particular, vulnerable to bad training. Without guidance or standards, it has been difficult to enforce accountability.

We have prioritized addressing these two shortcomings by doing the following:

- Departments and agencies are taking steps to identify training materials that may not meet internal standards and to improve processes for creating and reviewing such materials. Some departments are consulting with outside experts with established reputations to evaluate the content and training review process. Guidance on CVE-related training is being developed and will be issued, both across the organizations and to field components. Some departments may issue this as part of broader training guidance. (Lead: All)
- DHS, via FLETC, is in the process of developing a CVE curriculum to be integrated into existing training programs for Federal law enforcement. The curriculum will give Federal law enforcement a better understanding of CVE and how to more effectively leverage existing local partnerships. (Lead: DHS)
- DHS is in the process of establishing an internal committee to review all directly funded and issued DHS training on cultural competency, engagement, CVE, and counterterrorism. The committee will be responsible for reviewing any new content, evaluating experts, and establishing quality control. FEMA will incorporate the recently released Informational Bulletin and training guidance into FY12 grant guidance and will also leverage existing mechanisms to hold grantees and sub-grantees accountable. (Lead: DHS)

In addition to addressing the quality issue, we will work to expand the quantity of training.

- DHS, in partnership with the Los Angeles Police Department and the National Consortium for Advanced Policing, is developing a CVE curriculum that includes a 16-hour continuing education module for executive and frontline officers, as well as a 30-minute module that will be introduced at police academies. Both will be certified by the Police Officers Standards and Training Council. In October 2011 the Major Cities Chiefs Association passed a motion to adopt and implement the DHS CVE curriculum, which will be piloted with State and local law enforcement in San Diego by the end of 2011. By 2013, DHS seeks to: (1) implement the curriculum across the country on a regional basis; (2) develop a national network of trainers and subject matter experts who can administer the training and keep it current; and (3) build an online component for the curriculum. (Lead: DHS; Partners: DOJ and NCTC)
- DHS, via FLETC, will update current Federal training programs to integrate the CVE curriculum for Federal law enforcement in the coming year. (Lead: DHS)
- DHS is working with European law enforcement partners to share best practices and case studies to improve training, community policing, and operational information sharing. (Lead: DHS)
- DHS CRCL is expanding and institutionalizing its CVE and cultural competence training curricula to further enhance the material and its effectiveness. (Lead: DHS)

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

- The Interagency Working Group on Training will facilitate a “train the trainer program” to increase the reach of CVE training. (Leads: DHS and NCTC; Partners: DOJ, EDU, HHS, and FBI)
- The Interagency Working Group on Training will facilitate the development of an online training program that provides professional development credit for a broad range of professions, particularly those involved with public safety, violence prevention, and resilience. This will help build a basic understanding of CVE among a broad cross-section of stakeholders who have related mandates. (Leads: DHS and NCTC; Partners: DOJ, FBI, EDU, and HHS)
- The Interagency Working Group on Training will collaborate with non-security partners, such as EDU, to build CVE training modules that can be incorporated, as appropriate, into existing programs related to public safety, violence prevention, and resilience. These modules will be crafted in a way that is relevant to the specific audiences and their missions. Only trainers who have undergone CVE-specific training will deliver training programs that include CVE modules. (Lead: DHS; Partners: DOJ, EDU, HHS, FBI, and NCTC)
- DOD’s training programs and curricula will be informed by the work of the Interagency Working Group on Training, as appropriate. Additionally, DOD is conducting a review of CVE-related curricula and will make revisions and adjustments as necessary. (Lead: DOD; Partner DHS)

3. Countering violent extremist propaganda while promoting our ideals

As the National Counterterrorism Strategy emphasizes, “[t]he United States was founded upon a belief in a core set of values that is written into our founding documents and woven into the very fabric of our society. Where terrorists offer injustice, disorder, and destruction the United States must stand for freedom, fairness, equality, dignity, hope, and opportunity. The power and appeal of our values enables the United States to build a broad coalition to act collectively against the common threat posed by terrorists, further delegitimizing, isolating, and weakening our adversaries.”

Countering the ideologies and narratives that legitimize violence is central to our effort, but it also is the most challenging area of work, requiring careful consideration of a number of legal issues, especially those related to the First Amendment. In many instances, it will be more effective to empower communities to develop credible alternatives that challenge violent extremist narratives rather than having the Federal Government attempt to do so.

Our efforts include not only challenging justifications for violence, but affirming American ideals of inclusiveness and opportunity as well. Violent extremist narratives feed on disenchantment and the sense of exclusion. Our efforts therefore must include positive affirmation of our unity as a country. To some extent, this is addressed through our engagement activities, particularly where they address challenges facing all communities and not just those targeted by violent extremist radicalization. But there are also situations where we will need to more directly challenge violent extremist narratives.

3.1 Increase the capacity of communities to directly challenge violent extremist ideologies and narratives.

While the government cannot always directly contest violent extremist ideas, it can support capacity building within communities to take on this role. Whereas sub-objective 1.2 emphasizes preventative

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

measures and a defensive posture to build capacity for enhancing community resilience, sub-objective 3.1 focuses on increasing the ability of communities to push back against violent extremist propaganda.

Current Activities and Efforts

Most of our work in this area to date has focused on connecting community activists to potential civil society and private sector partners to focus specifically on undermining violent extremist narratives. Over the past year, we have taken the following steps:

- NCTC in 2010 developed a Community Awareness Briefing (CAB) to inform members of the public about efforts by al-Qa'ida and its adherents and affiliates to recruit Americans. The CAB highlights recruiting videos and examples of violent extremist propaganda, while underscoring the fact that these materials are often easily available on the Internet. Most importantly, the CAB aims to facilitate a discussion about what government and communities can do, together and independently, to counter the threat of violent extremist narratives. NCTC continues to deliver the presentation at forums composed of community leaders, educators, and parents in cities across the United States. In March 2011, NCTC held a workshop for local, State, and field-based Federal officials on how the CAB could be used in engagement efforts, when it makes sense and is appropriate.
- NCTC connected civic activists with technology experts, resulting in a training seminar on how to maximize the use of technology to counter violent extremism online.
- State sponsored speaker series and exchanges between international CVE practitioners and American communities targeted by violent extremist recruiters to better understand effective models for countering violent extremist narratives.

Future Activities and Efforts

This is a nascent area of effort and therefore will necessitate greater focus over the next year. Our planned actions include:

- Expanding efforts to raise community awareness about the threat of radicalization to violence, building from the experience of the CAB, and adapting those materials for different audiences where appropriate. (Leads: DOJ, DHS, FBI, and NCTC)
- Learning from former violent extremists, specifically those who can speak credibly to counter violent narratives, provide insights to government, and potentially catalyze activities to directly challenge violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Providing grants to counter violent extremist narratives and ideologies, within authorities and relevant legal parameters, by reprioritizing or increasing the flexibility of existing funding. (Lead: DHS)
- Brokering connections between private sector actors, civil society, and communities interested in countering violent extremist narratives. (Lead: DHS; Partner: NCTC)
- Promoting international exchange programs to build expertise for countering violent extremist narratives. (Lead: State; Partners: DOJ, DHS, FBI, and NCTC)

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

- Increasing technical training to empower communities to counter violent extremists online, including the development of training for bloggers. (Lead: DHS; Partners: State, NCTC, and FBI)

3.2 Improve and increase our communication to the American public about the threat posed by violent extremist groups, myths and misperceptions about violent extremist radicalization, and what we are doing to counter the threat.

It is important that we communicate to the American public the realities of what the threat is, and what it is not. Misconceptions about the threat and statements and actions that cast suspicion on entire communities based on the actions of a few distract attention from the real threat and can undermine our ability to build partnerships. An informed citizenry enhances our national security.

Current Activities and Efforts

In 2011, the Federal Government focused on developing its approach to domestic CVE and communicating this to the American public. This involved briefings to Congress, public addresses, and media interviews. We will continue these activities.

Future Activities and Efforts

In 2012, we will work to expand our efforts to raise awareness in the general public about radicalization to violence in the United States and the tools to prevent it by:

- Providing regular briefings to Congress, think tanks, and members of the media. (Lead: DHS; Partners: DOJ, FBI, and NCTC)
- Creating programs to directly engage the public on the issue. (Lead: All)
- Building a public website on community resilience and CVE. (Lead: DHS)

3.3 Build a strategy to leverage new technologies and address online violent extremist radicalization

The Internet has become an increasingly potent element in radicalization to violence, enabling violent extremists abroad to directly communicate to target audiences in the United States. This direct communication allows violent extremists to bypass parents and community leaders. The SIP specifically addresses the online arena in several sub-objectives, but because of the importance of the digital environment, we will develop a separate, more comprehensive strategy for countering and preventing violent extremist online radicalization and leveraging technology to empower community resilience that considers: (1) the latest assessment of the role of the Internet; (2) the absence of clear national boundaries in online space and the relationship between international and domestic radicalization to violence; (3) relevant legal issues; and (4) the differing authorities and capabilities of departments and agencies.

Conclusion

Protecting our Nation's communities from violent extremist recruitment and radicalization is a top national security priority. It is an effort that requires creativity, diligence, and commitment to our fundamental rights and principles. In his cover letter to the National Strategy for Empowering Local Partners, President Obama wrote:

STRATEGIC IMPLEMENTATION PLAN FOR EMPOWERING LOCAL PARTNERS TO PREVENT VIOLENT EXTREMISM IN THE UNITED STATES

Sadly, the threat of violent extremism in America is nothing new. Throughout our history, misguided groups—including international and domestic terrorist organizations, neo-Nazis and anti-Semitic hate groups—have engaged in horrific violence to kill our citizens and threaten our way of life. Most recently, al-Qa’ida and its affiliates have attempted to recruit and radicalize people to terrorism here in the United States, as we have seen in several plots and attacks, including the deadly attack 2 years ago on our service members at Fort Hood. As a government, we are working to prevent all types of extremism that leads to violence, regardless of who inspires it.

—President Barack Obama, August 3, 2011

A complex issue like violent extremist radicalization and recruitment requires a nuanced path to guide a whole-of-government approach. The SIP outlines this path and facilitates a division of labor by assigning responsibilities between Federal Government departments, agencies, and components focused on law enforcement and national security and those whose efforts support, but do not directly lie within, these areas.

From: [DHS.IGA](#)
To: [DHS.IGA](#)
Subject: STATEMENT BY SECRETARY JEH C. JOHNSON ON DHS'S NEW OFFICE FOR COMMUNITY PARTNERSHIPS
Date: Monday, September 28, 2015 12:35:31 PM

Press Office
U.S. Department of Homeland Security

Press Release

Sept. 28, 2015
Contact: DHS Press Office, (202) 282-8010

STATEMENT BY SECRETARY JEH C. JOHNSON ON DHS'S NEW OFFICE FOR COMMUNITY PARTNERSHIPS

Violent extremism - that which is inspired by foreign terrorist groups and that which is rooted in a range of domestic-based radical ideologies - pose a persistent and unpredictable threat to our homeland. Countering violent extremism has become a key focus of DHS's work to secure the homeland. Last year I appointed a Department-wide coordinator for our efforts to counter violent extremism. As Secretary of Homeland Security, I am also personally committed to this mission, having traveled to Boston, Chicago, Columbus, Houston, Los Angeles, Minneapolis, New York City, northern Virginia and suburban Maryland to meet with community leaders as part of this effort. We heard many strongly-held views, generated conversations, and built some bridges.

It is now time to take our efforts to the next level.

Today I announce the creation of the DHS Office for Community Partnerships. This Office will be dedicated to the mission of countering violent extremism, but its ultimate mission is as its name suggests - community partnerships. My charge to this Office, to be set forth in a more detailed plan, is to continue to build relationships and promote trust, and, in addition, find innovative ways to support communities that seek to discourage violent extremism and undercut terrorist narratives.

In this new Office, we will consolidate and reassign key personnel who are dedicated to countering violent extremism, but who are presently working in various different components of this Department. Longer term, we intend to call upon DHS personnel in field offices across the country to take part in our efforts at building community partnerships, under the coordination of this Office. The Office will coordinate its efforts with other departments and agencies in the federal government, and with similar efforts at the state and local government level.

For the Director of the Office for Community Partnerships, I am appointing Mr. George Selim. Since January 2012, George has been the Director for Community Partnerships for the National Security Council. George was a senior policy advisor in DHS's Office for Civil Rights and Civil Liberties, and has also served at the Department of Justice at the Community Relations Service.

For Deputy Director of the Office, I am appointing Mr. David Gersten, the current Coordinator of the Department's efforts to counter violent extremism. Prior to that, David, like George, had extensive experience in DHS's Office of Civil Rights and Civil Liberties.

Both George and David are well known within the CVE community.

Finally, DHS's Office for Civil Rights and Civil Liberties (CRCL) has been integral in our efforts at engaging communities, and they will continue to be. Civil rights and civil liberties are invariably part of the discussion when this Department engages communities. CRCL will therefore participate with the Office for Community Partnerships when we engage communities. More specifically, as we enter this new phase of our efforts, CRCL will, in consultation with the Office for Community Partnerships, continue to lead, improve and expand this Department's community engagements, including Community Engagement Roundtables, Town Hall Meetings, and Youth Forums across the country.

Given the evolution of threats to the homeland, I am convinced that efforts to counter violent extremism here at home are vital. I am determined that we make real progress in this area.

###



The Domestic Terrorist Threat: Background and Issues for Congress

Jerome P. Bjelopera

Specialist in Organized Crime and Terrorism

January 17, 2013

Congressional Research Service

7-5700

www.crs.gov

R42536

Summary

The emphasis of counterterrorism policy in the United States since Al Qaeda's attacks of September 11, 2001 (9/11) has been on jihadist terrorism. However, in the last decade, domestic terrorists—*people who commit crimes within the homeland and draw inspiration from U.S.-based extremist ideologies and movements*—have killed American citizens and damaged property across the country. Not all of these criminals have been prosecuted under terrorism statutes. This latter point is not meant to imply that domestic terrorists should be taken any less seriously than other terrorists.

The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) do not officially list domestic terrorist organizations, but they have openly delineated domestic terrorist “threats.” These include individuals who commit crimes in the name of ideologies supporting animal rights, environmental rights, anarchism, white supremacy, anti-government ideals, black separatism, and anti-abortion beliefs.

The boundary between constitutionally protected legitimate protest and domestic terrorist activity has received public attention. This boundary is especially highlighted by a number of criminal cases involving supporters of animal rights—one area in which specific legislation related to domestic terrorism has been crafted. The Animal Enterprise Terrorism Act (P.L. 109-374) expands the federal government's legal authority to combat animal rights extremists who engage in criminal activity. Signed into law in November 2006, it amended the 1992 Animal Enterprise Protection Act (P.L. 102-346).

Five discussion topics in this report may help explain domestic terrorism's significance for policymakers:

- **Level of Activity.** Domestic terrorists have been responsible for orchestrating more than two-dozen incidents since 9/11, and there appears to be growth in anti-government extremist activity as measured by watchdog groups in the last several years.
- **Use of Nontraditional Tactics.** A large number of domestic terrorists do not necessarily use tactics such as suicide bombings or airplane hijackings. They have been known to engage in activities such as vandalism, trespassing, and tax fraud, for example.
- **Exploitation of the Internet.** Domestic terrorists—much like their jihadist analogues—are often Internet savvy and use the medium as a resource for their operations.
- **Decentralized Nature of the Threat.** Many domestic terrorists rely on the concept of *leaderless resistance*. This involves two levels of activity. On an operational level, militant, underground, ideologically motivated cells or individuals engage in illegal activity without any participation in or direction from an organization that maintains traditional leadership positions and membership rosters. On another level, the above-ground public face (the “political wing”) of a domestic terrorist movement may focus on propaganda and the dissemination of ideology—engaging in protected speech.

- **Prison Radicalization.** Prison has been highlighted as an arena in which terrorist radicalization can occur. Some prison gangs delve into radical or extremist ideologies that motivate domestic terrorists, and in a number of instances, these ideologies are integral to fashioning cohesive group identities within prison walls. It must be reiterated, however, that even for gangs that exhibit these ideological dimensions, criminal enterprises such as drug trafficking—not radical beliefs—largely drive their activities.

Congress may choose to consider issues in three areas regarding the federal role in combating domestic terrorism. First is the issue of definitions. It is difficult to assess the scope of domestic terrorism because federal agencies use varying terms to describe it. Even more basically, there is no clear sense of how many domestic terrorist attacks have occurred or how many plots the government has foiled in recent years. Second, Congress may review the adequacy of domestic terrorism intelligence collection efforts. For intelligence gathering and program prioritization purposes, there is no standard set of intelligence collection priorities across federal agencies that can be applied to domestic terrorism cases. Also, there likely is no established standard for the collection of intelligence from state and local investigators—aside from suspicious activity reporting. Finally, it may be of value to explore how domestic terrorism fits into the Obama Administration's community outreach-driven strategy to quell terrorism-related radicalization in the United States. Congress may query the Administration on which brand of domestic terrorists it plans to focus on under the strategy and which local community groups it intends to engage regarding domestic terrorism issues.

Contents

Introduction.....	1
Domestic Terrorism Defined.....	2
What Is Domestic Terrorism?	3
Toward a Narrower Definition	4
Ambiguity Regarding “U.S.-Based Extremist Ideologies”	5
Factors Complicating the Descriptions of the Domestic Terrorism Threat	5
Counting Terrorism Cases	5
Sifting Domestic Terrorism from Other Illegal Activity	6
Extremism vs. Terrorism	7
The Lack of an Official Public List.....	9
Toward a Practical Definition: Threats Not Groups	10
Animal Rights Extremists and Environmental Extremists.....	11
Anarchist Extremists	13
White Supremacist Extremists	16
Anti-Government Extremists	22
Black Separatist Extremists.....	31
Anti-Abortion Extremists.....	32
Protected Activities vs. Terrorism—Divergent Perceptions of the ALF.....	34
A Serious Domestic Concern or “Green Scare?”	34
Assessing Domestic Terrorism’s Significance.....	38
Counting Incidents.....	39
Growth in Hate Groups and Anti-Government Extremism.....	40
“Non-Violent” Strategies.....	42
Direct Action	42
The ALF: “Live Liberations” and “Economic Sabotage”	43
The ELF: “Monkeywrenching”	43
“Paper Terrorism”: Liens, Frivolous Lawsuits, and Tax Schemes	47
The Internet and Domestic Terrorists	49
A Decentralized Threat	51
Leaderless Resistance.....	52
Lone Wolves.....	54
Prison Radicalization.....	58
Policy Considerations for Congress.....	60
Scoping the Threat.....	60
Terminology	61
Designating Domestic Terrorist Groups.....	61
A Public Accounting of Plots and Incidents.....	62
Intelligence	63
How Does Domestic Terrorism Fit into the U.S. Countering Violent Extremism Strategy?	64

Figures

Figure 1. Hate Groups and Militia Groups, 2000-2010	41
---	----

Figure 2. ALF and ELF Guidelines	46
--	----

Contacts

Author Contact Information.....	64
---------------------------------	----

Introduction

Since the terrorist attacks of September 11, 2001 (9/11), domestic terrorists—*people who commit crimes within the homeland and draw inspiration from U.S.-based extremist ideologies and movements*¹—have not received as much attention from federal law enforcement as their foreign counterparts inspired by Al Qaeda. This was not necessarily always the case. The FBI reported in 1999 that “[d]uring the past 30 years, the vast majority—but not all—of the deadly terrorist attacks occurring in the United States have been perpetrated by domestic extremists.”²

The U.S. government reacted to 9/11 by greatly enhancing its counterterrorism efforts. This report discusses how *domestic* terrorists broadly fit into this new counterterrorism landscape, a terrain that in the last 10 years has been largely shaped in response to terrorists inspired by *foreign* ideologies. This report focuses especially on how domestic terrorism is conceptualized by the federal government and issues involved in assessing this threat’s significance. Today (perhaps in part because of the government’s focus on international terrorist ideologies) it is difficult to evaluate the scope of domestic terrorist activity. For example, federal agencies employ varying terminology and definitions to describe it. Also, domestic terrorism-related intelligence collection efforts have not necessarily received the same attention as similar efforts to counter foreign threats. Beyond these issues, the Obama Administration’s community outreach-driven strategy to quell terrorism-related radicalization in the United States focuses on individuals inspired by Al Qaeda. How domestic terrorism fits into this strategy is unclear. Congress may opt to examine these and other issues related to domestic terrorism.

Domestic terrorists may not be the top federal counterterrorism priority, but they feature prominently among the concerns of some law enforcement officers. For example, in 2011, Los Angeles Deputy Police Chief Michael P. Downing included “black separatists, white supremacist/sovereign citizen extremists, and animal rights terrorists” among his chief counterterrorism concerns.³ Also possibly contributing to domestic terrorism’s secondary status as a threat, a large number of those labeled as domestic terrorists do not necessarily use traditional terrorist tactics such as bombings or airplane hijackings. Additionally, many domestic terrorists do not intend to physically harm people but rather rely on alternative tactics such as theft, trespassing, destruction of property, and burdening U.S. courts with retaliatory legal filings.

¹ This conceptualization of the term “domestic terrorism” is derived from a number of U.S. government sources detailed in this report. They are further discussed below. This paper *will not* focus on homegrown violent jihadists. However, when referring to such actors, for this report, “homegrown” describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, permanent legal residents, or visitors radicalized largely within the United States. “Jihadist” describes radicalized Muslims using Islam as an ideological and/or religious justification for belief in the establishment of a global caliphate—a jurisdiction governed by a Muslim civil and religious leader known as a caliph—via violent means. Jihadists largely adhere to a variant of Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and follow the model of the immediate followers and companions of the Prophet Muhammad.

² Federal Bureau of Investigation, *Terrorism in the United States: 30 Years of Terrorism—A Special Retrospective Edition*, (2000) p. 16.

³ Bill Gertz, “L.A. Police Use Intel Networks against Terror,” *Washington Times*, April 11, 2011, <http://www.washingtontimes.com/news/2011/apr/11/la-police-use-intel-networks-against-terror/?page=all#pagebreak>. See also Joshua D. Freilich, Steven M. Chermak & Joseph Simone Jr. “Surveying American State Police Agencies About Terrorism Threats, Terrorism Sources, and Terrorism Definitions,” *Terrorism and Political Violence*, vol. 21, no. 3 (2009) pp. 450-475. Freilich, Chermak, and Simone found that domestic terrorist groups featured prominently among the concerns of U.S. state police officials.

While plots and attacks by foreign-inspired homegrown violent jihadists have certainly earned more media attention, domestic terrorists have been busy as well. It is worth noting that in terms of casualties on U.S. soil, an act of domestic terrorism is second only to the events of 9/11. Timothy McVeigh's bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, claimed 168 lives and injured more than 500 others. Some estimates suggest that domestic terrorists are responsible for carrying out dozens of incidents since 9/11, and there appears to be growth in anti-government extremist activity as measured by watchdog groups in the last several years. Much like their jihadist counterparts, domestic terrorists are often Internet savvy and use the medium as a resource for their operations. Prison has been highlighted as an arena that can foster terrorist radicalization, and white supremacy—a set of beliefs held by white supremacist extremists—has long played a role in the activities of several U.S. prison gangs. Sovereign citizen anti-government ideas (that have inspired some domestic terrorists) have also circulated in U.S. prisons.

Terrorists are typically driven by particular ideologies. In this respect, domestic terrorists are a widely divergent lot, drawing from a broad array of philosophies and worldviews. These individuals can be motivated to commit crimes in the name of ideas such as animal rights, white supremacy, and opposition to abortion, for example. The expression of these worldviews—as opposed to violence in support of them—involves constitutionally protected activities.

Aware of the lines between constitutionally protected speech and criminality, domestic terrorists often rope themselves off from ideological (above-ground) elements that openly and often legally espouse similar beliefs. In essence, the practitioners who commit violent acts are distinct from the propagandists who theorize and craft worldviews that could be interpreted to support these acts. Thus, terrorist lone actors (lone wolves) or isolated small groups (cells) generally operate autonomously and in secret, all the while drawing ideological sustenance—not *direction*—from propagandists operating in the free market of ideas.

This report provides background regarding domestic terrorists—detailing what constitutes the domestic terrorism threat as suggested by publicly available U.S. government sources.⁴ It illustrates some of the key factors involved in assessing this threat and concludes by examining potential issues for Congress. This report does not discuss in detail either violent jihadist-inspired terrorism or the federal government's role in counterterrorism investigations. It is meant to be read in conjunction with CRS Report R41780, The Federal Bureau of Investigation and Terrorism Investigations; CRS Report R42553, Countering Violent Extremism in the United States; and CRS Report R41416, American Jihadist Terrorism: Combating a Complex Threat, which provide greater context in these areas.

Domestic Terrorism Defined

Two basic questions are key to understanding domestic terrorism. First, what exactly constitutes “domestic terrorism?” Answering this question is more complicated than it may appear. Some consider all terrorist plots occurring within the homeland as acts of domestic terrorism. According to this perspective, a bombing plot involving U.S. citizens motivated by a foreign terrorist group such as Al Qaeda constitutes domestic terrorism. While this conceptualization may be true at some level, a practical definition of domestic terrorism distilled from federal sources is much

⁴ This report does not presume the guilt of indicted individuals in pending criminal cases.

narrower. It suggests that domestic terrorists are Americans who commit ideologically driven crimes in the United States but lack foreign direction or influence—whether tactical or philosophical. This conceptualization excludes homegrown individuals directed or motivated by groups such as Al Qaeda. Second, what particular *groups* are considered domestic terrorist organizations? The U.S. government does not provide a precise, comprehensive, and public answer to this question. Rather, in broad terms, the Department of Justice (DOJ) has identified a number of general *threats* that embody this issue.

What Is Domestic Terrorism?

In the most general statutory terms, a domestic terrorist engages in terrorist activity that occurs in the homeland. The Federal Bureau of Investigation (FBI, the Bureau) has lead responsibility for terrorism investigations at the federal level.⁵

The FBI generally relies on two fundamental sources to define domestic terrorism. First, the Code of Federal Regulations characterizes “terrorism” as including “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”⁶ Second, 18 U.S.C. Section 2331(5) more narrowly defines “domestic terrorism” and differentiates it from international terrorism and other criminal activity.⁷ This definition comes from Section 802 of the USA PATRIOT Act (P.L. 107-52). According to 18 U.S.C. Section 2331(5), domestic terrorism occurs primarily within U.S. territorial jurisdiction, and domestic terrorism involves

(A) ... acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

(B) appear to be intended—

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping....⁸

⁵ 28 C.F.R. §0.85.

⁶ Ibid.

⁷ U.S. Congress, Senate Committee on Environment and Public Works, “Responses of John E. Lewis [then Deputy Assistant Director, Federal Bureau of Investigation] to Additional Questions from Senator Obama,” *Eco-Terrorism Specifically Examining the Earth Liberation Front and the Animal Liberation Front*, 109th Cong., 1st sess., May 18, 2005, S. Hrg. 109-947 (Washington: GPO, 2007), p. 41. Hereinafter: Responses of John E. Lewis.

⁸ 18 U.S.C. §2331(5).

Enforcement—Joint Terrorism Task Forces

Aside from the FBI, other federal agencies such as the Bureau of Alcohol Tobacco Firearms and Explosives (ATF) and the Internal Revenue Service (IRS) play a role in enforcement efforts to counter domestic terrorism. These agencies—as well as state and local law enforcement representatives—typically cooperate within the framework of Joint Terrorism Task Forces (JTTFs), multi-agency investigative units led by DOJ and the FBI across the country.⁹

JTTFs are teams of police officers, federal agents, analysts, linguists, SWAT experts, and other specialists who investigate terrorism and terrorism-related crimes. Seventy-one of the more than 100 JTTFs operated by DOJ and the FBI were created since 9/11. Over 4,400 federal, state, and local law enforcement officers and agents—more than four times the pre-9/11 total—work in them. These officers and agents come from more than 600 state and local agencies and 50 federal agencies.¹⁰

The FBI considers JTTFs “the nation’s front line on terrorism.”¹¹ They “investigate acts of terrorism that affect the U.S., its interests, property and citizens, including those employed by the U.S. and military personnel overseas.”¹² As this suggests, their operations are highly tactical and can involve developing human sources (informants) as well as gathering intelligence to thwart terrorist plots. JTTFs also offer an important conduit for the sharing of intelligence developed from FBI-led counterterrorism investigations with outside agencies and state and local law enforcement.¹³

Additionally, there is a National JTTF, which was established in July 2002 to serve as a coordinating mechanism with the FBI’s partners. Some 40 agencies are now represented in the National JTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners.¹⁴

Toward a Narrower Definition

The definitions cited above are too broad to capture what the FBI specifically investigates as “domestic terrorism.” Besides the statutory definitions regarding the crime of domestic terrorism, the FBI has historically emphasized particular qualities inherent to the *actors* who engage in domestic terrorism. According to the Bureau, domestic *terrorists* do not simply operate in the homeland, but they also *lack foreign direction*.¹⁵ In fact, the Bureau’s practical, shorthand definition of domestic terrorism is “Americans attacking Americans based on U.S.-based extremist ideologies.”¹⁶ The Department of Homeland Security (DHS) follows this construction.¹⁷

⁹ Federal Bureau of Investigation, “Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces,” http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jtfts, (n.d.).

¹⁰ Ibid.

¹¹ Federal Bureau of Investigation, “Protecting America against Terrorist Attack: A Closer Look at Our Joint Terrorism Task Forces,” May 2009, http://www.fbi.gov/page2/may09/jtfts_052809.html.

¹² Brig Barker and Steve Fowler, “The FBI Joint Terrorism Task Force Officer,” *The FBI Law Enforcement Bulletin*, vol. 77, no. 11 (November 2008), p. 13.

¹³ Kevin Johnson, “FBI Issues More Top Secret Clearance for Terrorism Cases,” USA Today, August 12, 2010, http://www.usatoday.com/news/nation/2010-08-12-secret-clearances_N.htm; STRATFOR, A Decade of Evolution in U.S. Counterterrorism Operations, Special Report, December 2009, http://www.stratfor.com/memberships/150745/analysis/20091216_us_decade_evolution_counterterrorism_operations?ip_auth_redirect=1; CRS Report RL33033, *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*.

¹⁴ DOJ, “Joint Terrorism Task Force,” <http://www.justice.gov/jtff/>.

¹⁵ James F. Jarboe, [then Domestic Terrorism Section Chief, Counterterrorism Division] Federal Bureau of Investigation, Testimony Before the House Resources Committee, Subcommittee on Forests and Forest Health, February 12, 2002, <http://www.fbi.gov/news/testimony/the-threat-of-eco-terrorism>. Hereinafter: Jarboe, Testimony.

¹⁶ Federal Bureau of Investigation, “Domestic Terrorism in the Post-9/11 Era,” September 7, 2009, http://www.fbi.gov/news/stories/2009/september/domterror_090709. Hereinafter: Federal Bureau of Investigation, “Domestic Terrorism.”

¹⁷ See Department of Homeland Security, “Domestic Terrorism and Homegrown Violent Extremism Lexicon,” November 10, 2011. Hereinafter: Department of Homeland Security, “Domestic Terrorism and Homegrown.”

Ambiguity Regarding “U.S.-Based Extremist Ideologies”

On the surface, the FBI’s shorthand definition for domestic terrorism appears straightforward. However, there is inherent ambiguity to it. Namely, some of the “U.S.-based extremist ideologies” driving what the Bureau views as domestic terrorism have international roots and active followings abroad. The ideologies supporting eco-extremism and animal rights extremism (discussed below) readily come to mind, and people have long committed crimes in their names outside the United States.¹⁸ At least in part, their origins lay in the United Kingdom. Nazism—with its German origins and foreign believers—is an element within domestic white supremacist extremism. Anarchism, the philosophy followed by anarchist extremists, also has longstanding European roots. The racist skinhead movement traces its origins abroad—to the United Kingdom—as well. It is unclear exactly what the FBI means when it emphasizes U.S.-based ideologies in its framing of domestic terrorism.

Factors Complicating the Descriptions of the Domestic Terrorism Threat

A few more issues make it hard to grasp the breadth of domestic terrorist activity in the United States. First, counting the number of terrorist prosecutions in general has been difficult in the post-9/11 period. Second, there may be some ambiguity in the investigative process regarding exactly when criminal activity becomes domestic terrorism. Third, the federal government appears to use the terms “terrorist” and “extremist” interchangeably when referring to domestic terrorism. It is unclear why this is the case. Finally, and most importantly, which specific *groups* are and should be considered domestic terrorist organizations? The U.S. government does not provide a public answer to this question. Rather, the federal government defines the issue in terms of “threats,” not groups.

Counting Terrorism Cases

While statutory and practical federal definitions exist for “domestic terrorism,” there is little clear sense of the scope of the domestic terrorist threat based on publicly available U.S. government information. Most broadly, it has been said that in much of the post-9/11 period, the federal courts and DOJ may have applied different parameters when sorting, counting, and categorizing *all types* of terrorist prosecutions—let alone domestic terrorism cases.¹⁹ A 2009 study (critiqued by DOJ) found that the U.S. Federal District Courts, DOJ’s National Security Division, and federal prosecutors rely on different criteria to determine whether or not specific cases involve terrorism at all.²⁰

¹⁸ See Gary A. Ackerman, “Beyond Arson? A Threat Assessment of the Earth Liberation Front,” *Terrorism and Political Violence*, vol. 15, no. 4 (2003), pp. 155-156. Hereinafter: Ackerman, “Beyond Arson?”

¹⁹ Transactional Records Access Clearinghouse (TRAC), *Who Is a Terrorist? Government Failure to Define Terrorism Undermines Enforcement, Puts Civil Liberties at Risk*, September 8, 2009, <http://trac.syr.edu/tracreports/terrorism/215/>. DOJ issued a press release that broadly challenged these findings and suggested that TRAC may have omitted certain statistics in its study. TRAC refuted these claims. For the interchange between DOJ and TRAC, see <http://trac.syr.edu/tracreports/terrorism/219/>.

²⁰ Ibid.

A bit more narrowly, in many instances, individuals considered to be domestic terrorists by federal law enforcement may be charged under non-terrorism statutes, making it difficult to grasp from the public record exactly how extensive this threat is. Regarding the prosecution of domestic terrorism cases, DOJ has noted that, “[a]lthough we do have at least one specialized [federal] statute aimed at animal enterprise terrorism,²¹ domestic terrorism cases often involve firearms, arson or explosive offenses; crimes relating to fraud; and threats and hoaxes.”²² In some instances, the crimes committed by people the FBI describes as domestic terrorism suspects do not violate federal law. When this occurs, the Bureau, “support[s] [its local] partners any way [it] can—sharing intelligence, offering forensic assistance, conducting behavioral analysis, etc.”²³ Thus, individuals considered domestic terrorists by federal law enforcement may not necessarily be federally charged as terrorists.

Sifting Domestic Terrorism from Other Illegal Activity

It may not be possible for investigators to describe the criminal activity involved early in an investigation as domestic terrorism. In these instances, investigators can work toward clarifying the motives of the suspects involved.²⁴ Domestic terrorism cases differ from ordinary criminal activity in key ways. Most importantly, unlike ordinary criminals—who are often driven by self-centered motives such as profit and tend to opportunistically seek easy prey—domestic terrorists are driven by a cause or ideology.²⁵ If the motives involved eventually align with the definition laid out in 18 U.S.C. Section 2331(5), presumably the case becomes a domestic terrorist investigation. In some instances, ideologically motivated actors can also collaborate with profit-driven individuals to commit crimes.

To further cloud matters, another category of criminal activity, hate crime, may appear to involve ideological issues.²⁶ However, as described by one federal official, a “hate crime” “generally involve[s] acts of personal malice directed at individuals” and is missing the broader motivations driving acts of domestic terrorism.²⁷ For investigators, distinguishing between “personal malice” and ideologically motivated actions may be difficult in specific cases. This suggests that sorting domestic terrorism from hate crimes depends on the degree of a suspect’s intent. Did the suspect articulate an ideology, belong to a domestic terrorist group, or follow an extremist movement? The grey area between domestic terrorism and hate crime hints that in some instances, suspects with links to domestic terrorist movements or ideologies supporting domestic terrorism may be

²¹ This likely refers to the Animal Enterprise Protection Act from 1992. In late 2006 shortly after the white paper’s publication, this act was amended by the Animal Enterprise Terrorism Act.

²² Department of Justice, *Counterterrorism White Paper*, June 22, 2006, p. 59. Hereinafter: Department of Justice, *White Paper*.

²³ Federal Bureau of Investigation, “Domestic Terrorism.”

²⁴ Responses of John E. Lewis, pp. 41, 42.

²⁵ In some instances such as those involving white-supremacist prison gangs who espouse extremist beliefs, the profit motive may be paramount in their criminal activity. See Joshua D. Freilich, Steven M. Chermak, and David Caspi, “Critical Events in the Life Trajectories of Domestic Extremist White Supremacist Groups,” *Criminology and Public Policy*, vol. 8, no. 3 (August 2009), p. 508. Hereinafter: Freilich, Chermak, and Caspi, “Critical Events. See also David Holthouse, “Smashing the Shamrock,” *Intelligence Report*, Southern Poverty Law Center, Issue 119, (Fall 2005), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2005/fall/smashing-the-shamrock?page=0,1>; Camille Jackson, “Nazi Low Riders,” *Intelligence Report*, Southern Poverty Law Center, Issue 114, (Summer 2004), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2004/summer/nazi-low-riders>.

²⁶ For more on hate crimes legislation, see CRS Report RL33403, *Hate Crime Legislation*, by William J. Krouse.

²⁷ Responses of John E. Lewis, p. 41.

charged with hate crimes.²⁸ It is unclear to what extent this influences how the government understands the threat posed by extremist movements that hold racist beliefs. If some individuals of this ilk commit crimes against police or judges, for example, is the government more apt to label this activity as terrorism while individuals sharing these same racist motivations but targeting ordinary citizens based on race, religion, disability, ethnic origin, or sexual orientation are charged with hate crimes?

The FBI's public description of the case of confessed would-be bomber Kevin Harpham exemplifies how difficult it may be to characterize acts as domestic terrorism. Initially the FBI viewed the case as domestic terrorism. In 2011, Harpham, allegedly motivated by white supremacist ideology, left a bomb—which never detonated—along the route of a parade in Spokane, WA, honoring Dr. Martin Luther King, Jr. The FBI's Northwest Joint Terrorism Task Force led the investigation.²⁹ In prepared public remarks framing the “current state of the terrorism threat” from April 2011, the FBI's Assistant Director for the Counterterrorism Division noted that Harpham's case was one of “several recent domestic terrorism incidents [that] demonstrate the scope of the threat.”³⁰ Harpham eventually pled guilty to committing a federal hate crime and attempting to use a weapon of mass destruction.³¹ Thereafter, the Bureau described the case as the successful prevention of a “horrific hate crime.”³²

Extremism vs. Terrorism

Another concept that muddies discussion of domestic terrorism is “extremism.” The latter term is commonly applied to homegrown actors, whether they be domestic terrorists or adherents of ideologies forwarded by foreign groups such as Al Qaeda. National security expert Jonathan Masters has suggested that many law enforcement officials likely view “extremism” as largely synonymous with “terrorism.”³³ Masters has also found that there is a “lack of uniformity in the way *domestic terrorist* activities are prosecuted” in the United States.³⁴ Presumably, using the term “extremist” allows prosecutors, policymakers, and investigators the flexibility to discuss terrorist-like activity without actually labeling it as “terrorism” and then having to prosecute it as

²⁸ While this discussion focuses on intent, domestic terrorists can exhibit additional traits that distinguish them from other offenders. For example, as part of their involvement in ideological movements, domestic terrorists often are exposed to more tactical training—in weapons, explosives, arson, reconnaissance, paramilitary discipline—than many more ordinary criminals. See Anti-Defamation League, *Guidebook on Extremism for Law Enforcement*, (2007), p. 9. Hereinafter: Anti-Defamation League, *Guidebook*.

²⁹ Department of Justice, press release, “Attempted Bomber Arrested,” March 9, 2011, <http://seattle.fbi.gov/dojpressrel/pressrel11/se030911.htm>.

³⁰ Mark F. Giuliano, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, prepared remarks delivered at the Washington Institute for Near East Policy, Stein Program on Counterterrorism and Intelligence, Washington, DC, April 14, 2011, <http://www.fbi.gov/news/speeches/the-post-9-11-fbi-the-bureaus-response-to-evolving-threats>.

³¹ Department of Justice, press release, “Attempted Bomber Pleads Guilty to Federal Hate Crime and Weapons Charge,” September 7, 2011, http://www.justice.gov/usao/wae/news/2011/2011_09_07_Harpham_Plea.html.

³² Federal Bureau of Investigation, “MLK Parade Bomber,” January 13, 2012, http://www.fbi.gov/news/stories/2012/january/hatecrime_011312/hatecrime_011312?utm_campaign=email-Immediate&utm_medium=email&utm_source=seattle-top-stories&utm_content=62754; Department of Justice, press release, “Colville, Wash., Man Indicted for Federal Hate Crime in Attempted Bombing of the MLK Unity March,” April 21, 2011, <http://www.justice.gov/opa/pr/2011/April/11-crt-509.html>.

³³ Jonathan Masters, *Militant Extremists in the United States*, Council on Foreign Relations, Washington, DC, February 7, 2011, <http://www.cfr.org/terrorist-organizations/militant-extremists-united-states/p9236>.

³⁴ Ibid.

such. This flexibility is certainly an asset to prosecutors. They can charge subjects of FBI domestic terrorism investigations under a wider array of statutes and, as a result, not describe the subjects publicly as terrorists. However, for policymakers this flexibility makes it hard to determine the scope of the domestic terrorist threat. One cannot get a clear sense of scope if some individuals are charged and publicly described as terrorists, others are discussed as extremists, and still others enter the public record only as criminals implicated in crimes not necessarily associated with terrorism, such as trespassing, arson, and tax fraud.

What Is Extremism?

The FBI's public formulation of "extremism" suggests two components. First, extremism involves hewing to particular ideologies. Second, it also includes criminal activity to advance these ideologies.³⁵ Thus, according to this construction, an anarchist believes in a particular ideology—anarchism. An "anarchist extremist" is an anarchist who adopts criminal tactics.³⁶

One scholar has indicated a similar bifurcation: First, extremism refers to an ideology outside a society's key values, and for liberal democracies, such ideologies "support racial or religious supremacy and/or oppose the core principles of democracy and human rights." Second, extremism can refer to the use of tactics that ignore the rights of others to achieve an ideological goal.³⁷

"Homegrown Violent Extremists" Are Not Domestic Terrorists

The FBI and DHS have recently popularized the phrase "homegrown violent extremist" (HVE). It separates domestic terrorists from U.S.-based terrorists *motivated by the ideologies of foreign terrorist organizations*. (HVEs include some of the actors this report considers as "homegrown violent jihadists.") According to DHS and the FBI, a HVE is "a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization."³⁸

³⁵ Federal Bureau of Investigation, "Domestic Terrorism: Anarchist Extremism, A Primer," December 16, 2010, http://www.fbi.gov/news/stories/2010/november/anarchist_111610/anarchist_111610. The focus of this piece, as the title suggests, is anarchist extremism, not necessarily defining the term "extremism." Hereinafter: Federal Bureau of Investigation, "Anarchist Extremism." This type of formulation—extremism consists of adherence to ideologies *and* criminal activity committed in the name of these ideologies—is replicated in the definitions provided within Department of Homeland Security, "Domestic Terrorism and Homegrown."

³⁶ Making things more complex, the broader concept of "violent extremism" has been used by the Obama Administration. According to the administration, "violent extremists" are "individuals who support or commit ideologically-motivated violence to further political goals." See *Empowering Local Partners to Prevent Violent Extremism in the United States*, August 2011, p. 1, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

³⁷ Peter R. Neumann, *Prisons and Terrorism: Radicalisation and De-Radicalisation in 15 Countries*, International Centre for the Study of Radicalisation and Political Violence, London, 2010, p. 12, <http://www.icsr.info/publications/papers/1277699166PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf>. In its *Guidebook on Extremism for Law Enforcement*, Hereinafter: Neumann, *Prisons and Terrorism*. The Anti-Defamation League has defined extremists as: "people who subscribe to extreme ideologies." The group goes on to say, "extreme ideologies are those that promote world views so radical that most other people will not agree with them." See Anti-Defamation League, *Guidebook*, p. 3.

³⁸ This definition appears to differ from the conceptualization of "homegrown jihadists" used in this report by (1) only (continued...)

According to the FBI and DHS, an HVE is not a domestic terrorist—they are two distinct categories of terrorist actors.³⁹

The Lack of an Official Public List

The federal government does not generate an official *and* public list of domestic terrorist organizations or individuals.⁴⁰ The development of such a list may be precluded by civil liberties concerns (i.e. inclusion in a publicly available list may impinge on a group's exercise of free speech or its other constitutionally protected activities). However, a lack of official lists or processes to designate groups or individuals as domestic terrorists makes it difficult to assess domestic terrorism trends and evaluate federal efforts to counter such threats. An unnamed DHS official cited in a news report stated that “unlike international terrorism, there are no designated domestic terrorist groups. Subsequently, all the legal actions of an identified extremist group leading up to an act of violence are constitutionally protected and not reported on by DHS.”⁴¹ Constitutionality aside, the lack of a list may also contribute to a certain vagueness in the public realm about which groups the federal government considers domestic terrorist organizations. While the government does not provide an official and public list of domestic terrorist organizations, it does include domestic terrorists (along with international terrorists) in its Terrorist Screening Database, commonly known as the “Terrorist Watchlist.”⁴²

The government is much less vague regarding foreign terrorist organizations. They are officially designated as such according to a well-established legally and procedurally proscribed regimen. According to the Department of State's Bureau of Counterterrorism, as of September 2012 the Secretary of State had designated 51 foreign terrorist organizations according to Section 219 of the Immigration and Nationality Act, as amended.⁴³

(...continued)

including individuals *not* directed by a foreign organization and by (2) including all sorts of terrorists motivated by foreign ideologies, not just violent jihadists. See Department of Homeland Security and Federal Bureau of Investigation, Joint Intelligence Bulletin, “Use of Small Arms: Examining Lone Shooters and Small-Unit Tactics,” August 16, 2011, p. 3.

³⁹ Ibid.

⁴⁰ See Christopher Bellavita, “Does the U.S. Have Any Domestic Terrorist Groups?” *Homeland Security Watch*, June 29, 2010, <http://www.hlswatch.com/2010/06/29/does-the-us-have-any-domestic-terrorist-groups/>. Hereinafter: Bellavita, “Domestic Terrorist Groups.” See also R. Jeffrey Smith, “Homeland Security Department Curtails Home-Grown Terror Analysis,” *Washington Post*, June 7, 2011, http://www.washingtonpost.com/politics/homeland-security-department-curtailed-home-grown-terror-analysis/2011/06/02/AGQEaDLH_story_1.html. Hereinafter: Smith, “Homeland Security.” David E. Heller, “Designating Domestic Terrorist Individuals or Groups,” (Master's Thesis, Naval Postgraduate School, 2010). Hereinafter: Heller, “Designating Domestic.”

⁴¹ Smith, “Homeland Security.”

⁴² Federal Bureau of Investigation, Terrorist Screening Center, “Frequently Asked Questions,” http://www.fbi.gov/about-us/nsb/tsc/tsc_faqs. See also Timothy J. Healy, Director, Terrorist Screening Center, Federal Bureau of Investigation, Statement before the House Judiciary Committee, Washington, DC, March 24, 2010, <http://www.fbi.gov/news/testimony/sharing-and-analyzing-information-to-prevent-terrorism?searchterm=Timothy+J.+Healy>; Bellavita, “Domestic Terrorist Groups.”

⁴³ For the legal criteria used to designate a foreign terrorist organization, the legal ramifications of designation, and ancillary effects of designation see Department of State, “Foreign Terrorist Organizations,” September 28, 2012, <http://www.state.gov/j/ct/rls/other/des/123085.htm>. Hereinafter: Department of State, “Foreign Terrorist Organizations.”

Toward a Practical Definition: Threats Not Groups

As discussed above, DOJ and the FBI do not list domestic terrorist organizations publicly and officially. This may complicate the understanding that federal policymakers have of what exactly the government considers “domestic terrorism.” While not naming specific *groups*, DOJ and the FBI have openly delineated domestic terrorist *threats*. DOJ has identified domestic terrorism threats to include criminal activity by “animal rights extremists, eco-terrorists, anarchists, anti-government extremists such as ‘sovereign citizens’ and unauthorized militias, [b]lack separatists, [w]hite supremacists, and anti-abortion extremists.”⁴⁴

The actors who constitute each of the domestic terrorist “threats” outlined by DOJ draw upon ideologies whose expression largely involves constitutionally protected activity. The FBI safeguards against cases focused solely on constitutionally protected activities. All FBI investigations have to be conducted for an authorized national security, criminal, or foreign intelligence collection purpose.⁴⁵ The purpose of an investigation may not be to solely monitor First Amendment rights.⁴⁶

However, it is unclear how DOJ or the FBI arrive at their list of domestic terrorism threats. This poses at least two fundamental questions:

- How does a particular brand of dissent become ripe for description by DOJ and the FBI as driving a “domestic terrorism” threat?

What criteria are involved in such a process?

How many crimes or plots attributed to a specific ideology have to occur to stimulate the identification of a new extremist threat? Is the severity of the crimes linked to an ideology taken into consideration?

- At what point do ideologically driven domestic terrorism threats cease to exist?

Should there be a means for public petitioning of the government to eliminate various threats as investigative priorities?

The below discussion of domestic terrorism threats will follow the order in which DOJ listed them. This does not necessarily presume the priority of one over the other. It is also important to note that instances of animal rights extremism and eco-terrorism within the last 10 years are

⁴⁴ Department of Justice, *White Paper*, p. 59. See also Federal Bureau of Investigation, “Domestic Terrorism.” The FBI’s domestic terrorism investigations likely cover these categories as well as lone wolves (lone offenders): extremists who commit crimes without the support of a formal organization or network. Some lone wolves are motivated by the ideologies behind the threats outlined by DOJ, but they can fashion their own ideologies as well. In the past, in the area of domestic terrorism, the FBI has distinguished between “special interest terrorism” and “traditional right-wing and left-wing terrorism: “Special interest terrorism differs from traditional right-wing and left-wing terrorism in that extremist special interest groups seek to resolve specific issues, rather than effect widespread political change. Special interest extremists continue to conduct acts of politically motivated violence to force segments of society, including the general public, to change attitudes about issues considered important to their causes. These groups occupy the extreme fringes of animal rights, pro-life, environmental, anti-nuclear, and other movements.” It is unclear whether the FBI still uses the categories of “special interest,” “left-wing,” and “right-wing” terrorism. See Jarboe, Testimony.

⁴⁵ Federal Bureau of Investigation, *Domestic Investigations and Operations Guide*, redacted, October 15, 2011, p. 4-1 through p. 4-2.

⁴⁶ Ibid.

more readily available in the public record than cases involving other types of domestic terrorism. The extensive use of such examples in this report does not imply the prominence of animal rights extremism or eco-terrorism over other domestic terrorist threats.

Animal Rights Extremists and Environmental Extremists

The term “animal rights extremism” covers criminal acts committed in the name of animal rights.⁴⁷ Environmental extremism—most often referred to as “Eco-terrorism”—includes criminal acts committed in the name of the environment.⁴⁸ These terms are not applied to groups or individuals involved with environmental movements or animal welfare protection/rights activism within the “confines of civil society and the rule of law.”⁴⁹

Many of the crimes committed by both animal rights extremists and eco-terrorists are perpetrated by independent small cells or individuals who harass and intimidate their victims.⁵⁰ These cells or lone actors engage in crimes such as vandalism, theft, the destruction of property, and arson. Most animal rights and eco-extremists also eschew physical violence directly targeting people or animals. Regardless, crimes committed by eco-terrorists and animal rights extremists have caused millions of dollars in property damage, and some have involved the intimidation and harassment of victims.⁵¹ These two types of extremism are often discussed together, because the two broader radical *movements* from which they draw their philosophical underpinnings have similar beliefs and overlapping membership.

The two *movements*—the Animal Liberation Front (ALF) and the Earth Liberation Front (ELF)—have the greatest reach among animal rights extremists and eco-terrorists. The ALF and the ELF are too diffuse to be called groups. Neither the ALF nor the ELF maintains formal rosters or leadership structures, for example.⁵² However, each communicates a sense of shared identity and attracts people who commit crimes in its name. They achieve this via “above-ground” wings. Largely using websites, ALF and ELF supporters publish literature highlighting movement philosophies, tactics, and accounts (press releases) of recent movement-related criminal activity. Much of this involves protected speech and occurs in the public realm. Press releases allow “underground” extremists to publicly claim responsibility for criminal activity in the name of either movement while maintaining secrecy regarding the details of their operations. The ALF and the ELF do not work alone. Members of other entities such as Stop Huntingdon Animal Cruelty (SHAC) have committed crimes in the name of animal rights, for example.

⁴⁷ Department of Homeland Security, “Domestic Terrorism and Homegrown.”

⁴⁸ For the purposes of this paper, “eco-terrorists,” “eco-extremists,” and “environmental extremists” are synonymous. These terms and “animal rights extremism” describe individuals engaged in criminal activity in the name of radical environmental ideologies or animal rights. It is unclear why environmental extremists are frequently dubbed “eco-terrorists” while animal rights extremists do not have a similar commonplace usage applied to them.

⁴⁹ See Kevin R. Grubbs, “Saving Lives or Spreading Fear: The Terroristic Nature of Eco-Extremism,” *Animal Law*, vol. 16, no. 2 (2010), p. 353-57. Hereinafter: Grubbs, “Saving Lives.”

⁵⁰ See Federal Bureau of Investigation, “Putting Intel to Work against ELF and ALF Terrorists,” June 30, 2008, http://www.fbi.gov/news/stories/2008/june/ecoterror_063008. Hereinafter: FBI, “Putting Intel.”

⁵¹ Ibid.

⁵² Both the ALF and the ELF focus on criminal activity as central tenets of their philosophies or operational guidelines, and the FBI emphasizes that criminal activity is a key element in the identities of these movements. See FBI, “Putting Intel.”

Additional factors tangle our understanding of the ALF and the ELF. People can simultaneously participate in both. This may partly be true because the movements are so amorphous. The two movements also share similar agendas, and in 1993 they declared solidarity.⁵³ All of this can play out confusingly in the real world. For example, an individual can commit a crime and claim responsibility for it online in the name of *both* the ALF and the ELF. One case especially highlights intersections between the ALF and the ELF.

In late 2005 and early 2006, the FBI dismantled a network that, according to DOJ, committed violent acts in the name of both the ALF and the ELF. The group included about 20 individuals and called itself “the Family.” It was reportedly responsible for at least 25 criminal incidents totaling approximately \$48 million in damages in the late 1990s and early 2000s and disbanded at some point in 2001, due to law enforcement pressure on the group. The Family was responsible for an arson attack in 1998 at the Vail Ski Resort. Eight simultaneous fires damaged radio towers, ski lift towers, restaurants, and the ski patrol office at the Colorado site and totaled over \$24 million in losses.⁵⁴

Philosophical Underpinnings

Both the ALF and the ELF rely on and borrow from a number of philosophical underpinnings to rationalize their beliefs and actions. These help forge a common identity among individuals in each movement. These ideas are also key principles professed by more mainstream animal rights or environmental activists engaged in legal protest.

The ALF: Animal Rights and Speciesism. The ALF’s moral code includes the belief that animals possess basic inalienable rights such as life, liberty, and the pursuit of happiness, and this suggests that animals cannot be owned. According to the ALF, the U.S. legal system—which describes animals as property—is corrupt, and there exists a “higher law than that created by and for the corporate-state complex, a moral law that transcends the corrupt and biased statutes of the US political system.”⁵⁵ Simply put, the rights of one species do not trump the rights of others. To suggest otherwise is to be prejudiced, according to animal rights adherents.

For the ALF and other animal rights supporters, the favoring of one species, particularly humans, over others has a name: speciesism. For the ALF, speciesism is a “discriminatory belief system as ethically flawed and philosophically unfounded as sexism or racism, but far more murderous and consequential in its implications.”⁵⁶ Thus, the movement couches the theft or illegal release of

⁵³ U.S. Congress, Senate Committee on Environment and Public Works, “Statement of Carson Carroll, Deputy Assistant Director, Bureau of Alcohol, Tobacco, Firearms, and Explosives,” *Eco-Terrorism Specifically Examining the Earth Liberation Front and the Animal Liberation Front*, 109th Cong., 1st sess., May 18, 2005, S. Hrg. 109-947 (Washington: GPO, 2007), p. 43. Hereinafter: Statement of Carson Carroll.

⁵⁴ Federal Bureau of Investigation, “Operation Backfire: Help Find Four Eco-Terrorists,” November 19, 2008, http://www.fbi.gov/news/stories/2008/november/backfire_11908; Department of Justice, press release, “Eleven Defendants Indicted on Domestic Terrorism Charges,” January 20, 2006, http://www.justice.gov/opa/pr/2006/January/06_crm_030.html. Hereinafter: Department of Justice, “Eleven Defendants.” See also *United States v. Joseph Dibee et al.*, Sentencing Memorandum, CR 06-60069-AA, CR 06-60070-AA, CR 06-60071-AA, CR 06-60078-AA, CR 06-60079-AA, CR 06-60080-AA, CR 06-60120-AA, CR-06-60122-AA, CR-06-60123-AA, CR-06-60124-AA, CR-06-60125-AA, CR-60126-AA, U.S. District Court, District of Oregon, May 4, 2007, pp. 6, 8, 19, 20-21. Hereinafter: *U.S. v. Dibee et al.*

⁵⁵ North American Animal Liberation Press Office, “History of the Animal Liberation Movement,” <http://www.animalliberationpressoffice.org/Background.htm>. Hereinafter: NAALPO, “History.”

⁵⁶ Steven Best and Anthony J. Nocella, II, “Behind the Mask: Uncovering the Animal Liberation Front,” in *Terrorists* (continued...)

animals used in research or for economic gain as “liberation.” The ALF views the destruction of laboratory infrastructure or tools as the elimination of items used to enslave species who have the same rights as humans. Intimidation of scientists and employees of businesses tied to animal research or testing is rationalized as confrontation with “oppressors” or those who, in the eyes of movement adherents, abuse and murder animals.⁵⁷

The ELF: An Ideological Mélange. Eco-terrorists are motivated by a mélange of environmental philosophies. There is no single formula for what constitutes the ideological makeup of an ELF follower, but several concepts likely play key roles in the movement. These are biocentrism, deep ecology, social ecology, and green anarchism. Biocentrism argues for the equality of all organisms.⁵⁸ Deep ecology suggests that all species are part of “the larger super-organism that is nature.”⁵⁹ It criticizes industrialization and views modern human impact on the earth as negative and harkens back to small communities centered on subsistence agriculture.⁶⁰ Social ecology suggests that hierarchical human society leads to social inequalities and environmental harm. Green anarchism ascribes environmental harm to civilization and domestication and embraces the notion of “rewilding,” or rejecting civilization and returning to a hunter-gatherer state to preserve one’s natural surroundings.⁶¹

Anarchist Extremists

According to the FBI, anarchist extremists commit crimes in the name of anarchist ideals.⁶² These ideals include belief that

individual autonomy and collective equality are fundamental and necessary for a functional, civilized society. [Anarchism] resists the existing hierarchical structure of society that gives some people authority and control over others. [According to anarchists] authority imbues power, and power always is used in illegitimate and self-serving ways by those who have it.⁶³

Anarchist extremists as well as anarchists engaging in constitutionally protected activity can oppose government, business, or social interests that they view as dangerous. As this suggests, anarchists advocate some form of revolution that realigns authority and power in the societies

(...continued)

or *Freedom Fighters? Reflections on the Liberation of Animals*, ed. Steven Best and Anthony J. Nocella, II (New York: Lantern Books, 2004), p. 24. Hereinafter: Best and Nocella, “Behind the Mask.” Best reportedly advises NAALPO, see <http://naalpo.posterous.com/our-task-new-essay-by-press-office-advisor-st-p-michael-conn-and-james-v-parker-the-animal-research-war> (New York: Palgrave Macmillan, 2008), p. xix. Hereinafter: Conn and Parker, *The Animal*. See also NAALPO, “History” which excerpts Best and Nocella’s work.

⁵⁷ NAALPO, “History.”

⁵⁸ Stefan H. Leader and Peter Probst, “The Earth Liberation Front and Environmental Terrorism,” *Terrorism and Political Violence*, vol. 15, no. 4 (Spring/Summer 2005), pp. 39-40. Hereinafter: Leader and Probst, “The Earth Liberation Front.”

⁵⁹ Conn and Parker, *The Animal*, xx.

⁶⁰ Leader and Probst, “The Earth Liberation Front,” pp. 39-40.

⁶¹ Sean Parson, “Understanding the Ideology of the Earth Liberation Front,” *Green Theory and Praxis: The Journal of Ecopedagogy*, vol. 4, no. 2 (2008), pp. 54-58.

⁶² Ibid.

⁶³ Randy Borum and Chuck Tilby, “Anarchist Direct Actions: A Challenge for Law Enforcement,” *Studies in Conflict and Terrorism*, vol. 28, no. 3, (2005), p. 202. Hereinafter: Borum and Tilby, “Anarchist Direct Action.”

they desire to transform. However, adherents cannot agree to a single means for attaining revolutionary change.⁶⁴

As one may assume, anarchist activity is decentralized. In fact, a basic, temporary organizational structure—the affinity group—likely plays a larger role in shaping the work of U.S. anarchists than any formal long-lasting entities or networks.⁶⁵ Affinity groups are “autonomous militant unit[s] generally made up of between five-to-twenty individuals who share a sense of the causes worth defending and the types of actions they prefer to engage in. The decision-making process is anarchist, that is to say, egalitarian, participatory, deliberative, and consensual.”⁶⁶ An affinity group often consists of a circle of friends. The friends coalesce around a specific objective and break apart when they achieve their desired ends. Individual groups can band together in “clusters” and clusters can coordinate their efforts, if need be.⁶⁷ The ends can be legal or illegal, violent or non-violent, covert or open. These structures have a long history among anarchists, but other movements use them as well.⁶⁸ Also, anarchists can engage in what they call “black bloc” tactics. These involve secretive planning for public—often criminal—activity in which participants, typically dressed in black, act en-masse.⁶⁹ Adding to the sprawling nature of the anarchist movement, some adherents also participate in the ALF and the ELF. These three movements share general philosophical tenets such as opposition to globalization and capitalism.⁷⁰

The FBI has described anarchist extremists as typically being “event driven,” meaning

they show up at political conventions, economic and financial summits, environmental meetings, and the like. They usually target symbols of Western civilization that they perceive to be the root causes of all societal ills—i.e., financial corporations, government institutions, multinational companies, and law enforcement agencies. They damage and vandalize property, riot, set fires, and perpetrate small-scale bombings. Law enforcement is also concerned about anarchist extremists who may be willing to use improvised explosives devices or improvised incendiary devices.⁷¹

Anarchist extremists in the United States have been involved in illegal activity during mass protests surrounding events such as the 1999 World Trade Organization Ministerial Conference in Seattle, WA.

Anarchist extremists reportedly committed crimes during the 2008 Republican National Convention in St. Paul, MN.⁷² To coordinate their protests during the convention, some anarchists

⁶⁴ Ibid., p. 203.

⁶⁵ Ibid., p. 207.

⁶⁶ Francis Dupuis-Déri, “Anarchism and the Politics of Affinity Groups,” *Anarchist Studies*, vol. 18, no. 1 (2010), p. 41. Hereinafter: Dupuis-Déri, “Anarchism.”

⁶⁷ CrimethInc. Workers’ Collective, *Recipes for Disaster: An Anarchist Cookbook*, (Olympia, WA: CrimethInc. Workers’ Collective, 2004), pp. 28-34. Hereinafter: *Anarchist Cookbook*.

⁶⁸ Dupuis-Déri, “Anarchism,” p. 43.

⁶⁹ *Anarchist Cookbook*, pp. 127-130.

⁷⁰ Borum and Tilby, “Anarchist Direct Action,” p. 208.

⁷¹ Federal Bureau of Investigation, “Anarchist Extremism.”

⁷² Ibid. For information on reported anarchist criminal activity related to the 2008 Republican National Convention, see Department of Justice, press release, “Michigan Man Sentenced for Possessing Molotov Cocktails,” March 10, 2009, <http://www.fbi.gov/minneapolis/press-releases/2009/mp031009.htm>; Department of Justice, press release, “Texas Man (continued...)”

formed what they called the “RNC Welcoming Committee” (RNCWC).⁷³ In September 2007, the RNCWC developed a plan to broadly organize the activities of affinity groups intending to disrupt the convention. Law enforcement infiltrated and undermined these efforts, arresting 800 people, including eight involved with the RNCWC.⁷⁴ Initially, in Minnesota state court, the eight “had been charged with felonies: first-degree damage to property and second-degree conspiracy to riot. Prosecutors added a more serious charge of conspiracy to riot in furtherance of terrorism, which was later dismissed.”⁷⁵ Five of the eight pled guilty to gross misdemeanor charges in 2010. The others had all of the charges they faced dismissed.⁷⁶

On April 30, 2012, five men who reputedly had anarchist sympathies were arrested for purportedly scheming to blow up a bridge near Cleveland, OH.⁷⁷ The plot was apparently timed to coincide with peaceful protest activity arranged by Occupy Cleveland, an offshoot of the Occupy Wall Street movement. Occupy Cleveland representatives have stated that the alleged would-be bombers “were in no way representing or acting on behalf of Occupy Cleveland.”⁷⁸ An FBI sting operation led to the quintet’s arrest.⁷⁹ Purportedly, the group relied on an undercover FBI employee to supply them with two inert bombs that the conspirators believed were functional.⁸⁰

Criminal acts involving anarchist extremists do not have to be event-driven. For example, Joseph Konopka, the self-dubbed “Dr. Chaos,” allegedly led a group of boys he called “The Realm of Chaos” in a series of crimes involving vandalism to radio and cell phone towers in the late 1990s and early 2000s. In 2002, he was arrested in Chicago for storing more than a pound of deadly

(...continued)

Sentenced on Firearms Charges Connected to the Republican National Convention,” May 21, 2009, <http://www.fbi.gov/minneapolis/press-releases/2009/mp052109a.htm>; Department of Justice, press release, “Austin, Texas Man Sentenced for Possessing Molotov Cocktails During the Republican National Convention,” May 14, 2009, <http://www.fbi.gov/minneapolis/press-releases/2009/mp051409.htm>. For information on a matter possibly related to the anarchist criminal activity at the 2008 convention, see James C. McKinley, Jr., “Anarchist Ties Seen in ‘08 Bombing of Texas Governor’s Mansion,” *New York Times*, February 22, 2011, <http://www.nytimes.com/2011/02/23/us/23texas.html>.

⁷³ For an archived version of the group’s website see <http://web.archive.org/web/20080907081250/http://www.nornc.org/>.

⁷⁴ Pat Pheifer, “Guilty Pleas Close Book on ‘08 Convention Protests,” *Minneapolis-St. Paul Star Tribune*, October 19, 2010, http://www.startribune.com/templates/Print_This_Story?sid=105311223. Hereinafter: Pheifer, “Guilty Pleas.” See also Fred Burton and Scott Stewart, “The Lessons of St. Paul,” *STRATFOR*, September 10, 2008, http://www.stratfor.com/weekly/lessons_st_paul?ip_auth_redirect=1.

⁷⁵ Pheifer, “Guilty Pleas.”

⁷⁶ Ibid.

⁷⁷ Department of Justice, press release, “Five Men Arrested in Plot to Bomb Ohio Bridge,” May 1, 2012, <http://www.fbi.gov/cleveland/press-releases/2012/five-men-arrested-in-plot-to-bomb-ohio-bridge>. Hereinafter: Department of Justice, “Five Men.” David Ariosto, “5 Arrested in Alleged Plot to Blow Up Cleveland-Area Bridge,” *CNN*, May 1, 2012, <http://www.cnn.com/2012/05/01/justice/ohio-bridge-arrests/index.html>.

⁷⁸ Henry J. Gomez, “Bridge Bomb Plot: Suspects Were Active in Occupy Cleveland, Even As Movement Slowed to a Crawl,” *Cleveland Plain Dealer*, May 2, 2012, http://www.cleveland.com/metro/index.ssf/2012/05/bridge_bomb_plot_suspects_were.html.

⁷⁹ Department of Justice, “Five Men.”

⁸⁰ Ibid. Four of the conspirators pled guilty “to conspiracy to use weapons of mass destruction, attempted use of weapons of mass destruction, and malicious use of an explosive device to destroy property used in interstate commerce.” See Department of Justice, press release, “Three Men Sentenced to Prison for Roles in Plot to Bomb Ohio Bridge,” November 20, 2012, <http://www.fbi.gov/cleveland/press-releases/2012/three-men-sentenced-to-prison-for-roles-in-plot-to-bomb-ohio-bridge>.

cyanide powder in a passageway in a Chicago Transit Authority subway tunnel.⁸¹ He had obtained the material (potassium cyanide and sodium cyanide) from an abandoned warehouse.⁸² In 2002, Konopka pled guilty in federal court to possessing chemical weapons, and in 2005 he pled guilty to 11 felonies, including conspiracy, arson, creating counterfeit software, and interfering with computers in Wisconsin.⁸³

White Supremacist Extremists

The term “white supremacist extremism” (WSE) describes people or groups who commit criminal acts in the name of white supremacist ideology. At its core, white supremacist ideology purports that the white race ranks above all others. WSE draws on the constitutionally protected activities of a broad swath of racist hate-oriented groups active in the United States ranging from the Ku Klux Klan to racist skinheads. Some of these groups have elaborate organizational structures, dues-paying memberships, and media wings. Additionally, many individuals espouse extremist beliefs without having formal membership in any specific organization.

A large proportion of white supremacists dualistically divide the world between whites and all other peoples who are seen as enemies.⁸⁴ Particular animus is directed toward Jews and African Americans. In fact, a common racist and revisionist historical refrain is that the civil rights movement succeeded only because Jews orchestrated it behind the scenes.⁸⁵

Scholars indicate that white supremacists believe in racial separation and that society discriminates against them. To them, whites have lost “ground to other groups and ... extreme measures are required to reverse the trend.”⁸⁶ All of this has been encapsulated in a slogan known as the “Fourteen Words”: “We must secure the existence of our race and a future for white children.” This was coined by David Lane, a member of a violent terrorist group active in the 1980s. The Fourteen Words have been described as “the most popular white supremacist slogan in the world.”⁸⁷

Neo-Nazism and its obsession with Adolph Hitler and Nazi Germany is also a prominent component of white supremacist extremism in the United States.⁸⁸ The father of American neo-Nazism, George Lincoln Rockwell, became publicly active in the late 1950s. According to one

⁸¹ Juliet Williams, Federal appeals Court Overturns Dr. Chaos Conviction,” *Associated Press*, May 31, 2005; Mike Robinson, “Federal Prosecutors Want ‘Dr. Chaos’ to Remain Locked Up,” *Associated Press*, March 13, 2002; Meg Jones and Jesse Garza, “‘Anarchist’ Charged Over Cache of Cyanide,” *Milwaukee Journal Sentinel*, March 12, 2002.

⁸² “Man Pleads Guilty to Storing Cyanide,” *Associated Press*, November 21, 2002.

⁸³ “Judge Sentences ‘Dr. Chaos’ to Prison for Damage to Wisconsin Power Systems,” *Associated Press*, November 30, 2005.

⁸⁴ Chip Berlet and Stanislav Vysotsky, “Overview of U.S. White Supremacist Groups,” *Journal of Political and Military Sociology*, vol. 34, no. 1 (Summer 2006), p. 13. Hereinafter: Berlet and Vysotsky, “Overview.”

⁸⁵ Leonard Zeskind, *Blood and Politics: The History of the White Nationalist Movement from the Margins to the Mainstream* (New York: Farrar, Straus, and Giroux, 2009), p. 40. Hereinafter: Zeskind, *Blood and Politics*.

⁸⁶ Rory McVeigh, “Structured Ignorance and Organized Racism in the United States,” *Social Forces*, vol. 82, no. 3 (March 2004), pp. 898-899.

⁸⁷ Anti-Defamation League, *Guidebook*, p. 16. Lane died in 2007 while serving 190 years in prison for his involvement with a terrorist group named the Order. See “Founder of Terrorist Group Dies in Prison,” *Terre Haute Tribune-Star*, May 29, 2007, <http://tribstar.com/local/x1155692948/Founder-of-terrorist-group-dies-in-prison>. Among other writings, Lane also drafted an influential racist ideological tract titled *The 88 Precepts*.

⁸⁸ Anti-Defamation League, *Guidebook*, p. 15.

scholar, Rockwell laid down three concepts that have shaped neo-Nazism ever since. For his followers, he reconfigured the racial notion of “white,” broadening it beyond “Aryan” to include people of Southern and Eastern European descent. Additionally, Rockwell denied the Holocaust. He also encouraged tying neo-Nazism to religion, and some of his followers took up the obscure creed of Christian Identity.⁸⁹

Conflict and Conspiracy

Aside from racial superiority, a dualistic view of the world, and neo-Nazism, at least two other broad concepts shape white supremacy in the United States. They are the inevitability of violent conflict, and a belief that conspiracies hostile to white supremacy shape the existing world.⁹⁰ It can be said that WSE broadly shares these concepts with the militia movement (discussed below).

The FBI has stated that white supremacists “commonly anticipate” waging war against their opponents.⁹¹ For example, the inevitability of RAHOWA—an acronym for “racial holy war”—is a central tenet of the neo-Nazi Creativity Movement, which has its roots in the Church of the Creator, a racist group founded by Ben Klassen in 1973.⁹² Klassen, who committed suicide in 1993, argued that whites had no choice but to wage war against non-whites.⁹³ Likewise, some white supremacists use racism to interpret apocalyptic imagery from Norse mythology embodied in Odinism.⁹⁴ Most Odinists are not racists, however.⁹⁵

Conspiracism has been defined as “the idea that most major historic events have been shaped by vast, long-term, secret conspiracies that benefit elite groups and individuals.”⁹⁶ Conspiracy

⁸⁹ Fredrick J. Simonelli, “The Neo-Nazi Movement,” Southern Poverty Law Center, <http://www.splcenter.org/get-informed/intelligence-files/ideology/neo-nazi/the-neo-nazi-movement>. See also Charles S. Clark, “An American Nazi’s Rise and Fall,” *American History*, vol. 40, no. 6 (February 2006), pp. 60-66; Simonelli, “The American Nazi Party,” *Historian*, vol. 57, no. 3 (Spring 1995), pp. 553-566. A follower assassinated Rockwell in 1967. For information on Christian Identity, see Kevin Borgeson and Robin Valeri, *Terrorism in America* (Sudbury, MA: Jones and Bartlett, 2009), pp. 47-72; Martin Durham, “Christian Identity and the Politics of Religion,” *Totalitarian Movements and Political Religions*, vol. 9, no. 1 (March 2008), pp. 79-91; Tanya Telfair Sharpe, “The Identity Christian Movement: Ideology of Domestic Terrorism,” *Journal of Black Studies*, vol. 30, no. 4 (March 2000), pp. 604-623; Anti-Defamation League, “Christian Identity,” http://www.adl.org/learn/ext_us/Christian_Identity.asp?xpicked=4&item=Christian_ID.

⁹⁰ Berlet and Vysotsky, “Overview,” pp. 12-13 highlights dualism, conspiracism, and apocalypticism as key themes.

⁹¹ The Bureau has noted that “warfare” is reflected in beliefs drawn from Christian Identity, the Creativity Movement, neo-Nazism, and Odinism. See Federal Bureau of Investigation, *White Supremacist Recruitment of Military Personnel since 9/11*, July 7, 2008, p. 4. Hereinafter: Federal Bureau of Investigation, *White Supremacist*.

⁹² After Klassen’s 1993 death, the Church of the Creator was revived in an altered form by Matt Hale. For more information see Southern Poverty Law Center, “Church of the Creator,” <http://www.splcenter.org/get-informed/intelligence-files/groups/creativity-movement>. See also Dobratz, “The Role,” p. 290; and Federal Bureau of Investigation, *White Supremacist*, p. 4.

⁹³ Ben Klassen, “RAHOWA: The Fighting Slogan of the White Race,” *Racial Loyalty*, no. 32 (February 1986), <http://www.archive.org/details/RahowaThisPlanetIsAllOurs>.

⁹⁴ Federal Bureau of Investigation, *White Supremacist*, p. 4. Odinism has been defined as either a combination of old Norse religion and Christianity or a belief system that draws exclusively on Nordic mythology. See Jonathan White, “Political Eschatology: A Theology of Antigovernment Extremism,” *The American Behavioral Scientist*, vol. 44, no. 6, (February 2001), p. 939.

⁹⁵ Berlet and Vysotsky, “Overview,” p. 30.

⁹⁶ Berlet and Vysotsky, “Overview,” p. 12. For more on conspiracy theories and terrorism see Jamie Bartlett and Carl Miller, *The Power of Unreason: Conspiracy Theories, Extremism, and Counter-Terrorism*, Demos, London, August 29, 2010. Bartlett and Miller (p. 24.) suggest that conspiracy theories “are one of a number of factors that can lead to extremism, and can turn extremism to violence.”

theories are not the province of a particular movement or group. Regardless, conspiracy theories can particularly shape the outlooks and actions of white supremacist extremists. Media sources have stated that Richard Poplawski—convicted of shooting and killing three Pittsburgh police officers in April 2009—believed that a Zionist conspiracy controlled government and major corporations in the United States.⁹⁷

As in Poplawski's example, anti-Semitism plays a prominent role in the racist conspiracies of many white supremacists.⁹⁸ These people—as well as anti-government extremists—believe in something they call the Zionist Occupied Government (ZOG).⁹⁹ ZOG refers to the federal government, which adherents contend is “controlled or manipulated by international Jewish interests.”¹⁰⁰ On its website, one WSE group has sold versions of a video game titled “ZOG's Nightmare.” Gameplay involves shooting nonwhites while being chased by a police agency controlled by Jews.¹⁰¹ Racists explain all sorts of personal or social grievances by invoking ZOG.¹⁰² One scholar has described ZOG as

an omnipresent and omnipotent cabal involving at its heart varying constellations of Jews, Illuminati, Freemasons, plutocrats, and multinational corporations. It operates through many social ‘front’ institutions, from the United Nations to Parent-Teacher Associations.... ZOG can be used to explain not only the existence of affirmative action, environmental pollution, and pornography but also why a certain individual made poor grades in school, lost his job, or seems unable to find a partner.¹⁰³

According to adherents, ZOG is said to control the media, arts, religion, science, and education.¹⁰⁴

Loss of Prominent Leaders

In the 1980s and 1990s, a small number of figures dominated white supremacist circles. They were intimately linked to their own relatively cohesive organizations. By the early 2000s, these groups fragmented as they lost their leaders. This fragmented situation likely persists. In fact, one study from 2006 has described “a recent crisis of leadership in the hate movement.”¹⁰⁵

⁹⁷ Timothy McNulty, Paula Reed Ward and Sadie Gurman, “Jury Decides Poplawski Should Die for Killing 3 Officers,” *Pittsburgh Post-Gazette*, June 28, 2011. Hereinafter: McNulty et al., “Jury Decides.” See also Anti-Defamation League, “Richard Poplawski: The Making of a Lone Wolf,” April 8, 2009, http://www.adl.org/learn/extremism_in_the_news/White_Supremacy/poplawski%20report.htm. Hereinafter: Anti-Defamation League, “Richard Poplawski.” Sean D. Hamill, “Man Accused in Pittsburgh Killings Voiced Racist Views Online,” *New York Times*, April 7, 2009, <http://www.nytimes.com/2009/04/07/us/07pittsburgh.html>. Hereinafter: Hamill, “Man Accused.”

⁹⁸ Berlet and Vysotsky, “Overview,” p. 13.

⁹⁹ Also seen as “Zionist Occupation Government.”

¹⁰⁰ Institute for Intergovernmental Research, *Investigating Terrorism*, p. 93; Mattias Gardell, *Gods of the Blood: The Pagan Revival and White Separatism* (Durham, NC: Duke University Press, 2003), pp. 11, 54, 68-69. Hereinafter: Gardell, *Gods*.

¹⁰¹ Anti-Defamation League, *The National Socialist Movement*, http://www.adl.org/Learn/Ext_US/nsm/tactics.asp?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_America&xpicked=3&item=nsm.

¹⁰² Gardell, *Gods*, p. 68.

¹⁰³ Ibid.

¹⁰⁴ Ibid.

¹⁰⁵ Jack Levin, *Domestic Terrorism* (New York: Infobase Publishing, 2006), pp. 48-49.

Two particularly well-known white supremacist figures died in the last decade. William Pierce, head of the National Alliance died in 2002. Richard Butler, leader of Aryan Nations, died in 2004. Both Pierce and Butler articulated clear ideologies that attracted followers and drew upon resources such as rural headquarters/compounds to sustain their organizations.¹⁰⁶ By the early 2000s, the National Alliance even had a substantial revenue stream estimated at \$1 million annually generated from a publishing company and record labels it owned as well as dues.¹⁰⁷ The deaths of Butler and Pierce exacerbated the downfall of both organizations. The decline of these groups also resulted from a number of other forces, such as infighting among members and pressure from law enforcement and watchdog groups.¹⁰⁸

Two prominent white supremacist movements are discussed below.

National Socialist Movement (NSM)

One white supremacist organization active in the United States is the National Socialist Movement (NSM). It has benefitted from the decline of these other groups as well as new leadership in the form of Jeff Schoep.¹⁰⁹ The NSM also capitalized on the expansion of the Internet in the early 2000s. The group, which emerged in 1974, is a descendant of the American Nazi Party, and until the 1990s and early 2000s “it operated only on the fringes of the neo-Nazi movement.”¹¹⁰ As of 2008, the group had around 500 members and close associates throughout the United States.¹¹¹ The NSM is flexible about membership, allowing its members to also participate in other white supremacist organizations.¹¹²

Individuals allegedly tied to the NSM at some point in their lives have run afoul of the law.

- In Minnesota in April 2012, Joseph Benjamin Thomas was indicted on drug-related charges, and Samuel James Johnson was indicted on weapons-related charges. Purportedly the two were tied to NSM—at one point Johnson had served as its leader in Minnesota. The duo had reportedly formed their own white supremacist group, gathering weapons and ammunition and planning to attack the government and other targets.¹¹³ In June 2012, Johnson pled guilty to “one count of being a felon in possession of firearms.”¹¹⁴ In July 2012, Thomas pled

¹⁰⁶ Freilich, Chermak, and Caspi, “Critical Events,” 511.

¹⁰⁷ *Ibid.*, pp. 512, 513.

¹⁰⁸ *Ibid.*, p. 516.

¹⁰⁹ Anti-Defamation League, *American Stormtroopers: Inside the National Socialist Movement*, (2008), p. 3. Hereinafter: Anti-Defamation League, *American Stormtroopers*.

¹¹⁰ *Ibid.*

¹¹¹ *Ibid.*

¹¹² Southern Poverty Law Center, “National Socialist Movement,” <http://www.splcenter.org/get-informed/intelligence-files/groups/national-socialist-movement>.

¹¹³ Department of Justice, press release, “Mendota Heights Man Indicted for Distributing Methamphetamine,” April 27, 2012, <http://www.fbi.gov/minneapolis/press-releases/2012/mendota-heights-man-indicted-for-distributing-methamphetamine>; Department of Justice, press release, “Austin Felon Indicted for Possessing Firearms,” April 27, 2012, <http://www.fbi.gov/minneapolis/press-releases/2012/austin-felon-indicted-for-possessing-firearms>; Amy Forliti, “Affidavit: 2 Men With Supremacist Ties Had Weapons,” *Associated Press*, April 27, 2012, <http://abcnews.go.com/US/wireStory/affidavit-men-supremacist-ties-weapons-16229960?singlePage=true#.T6LAcVVLts>.

¹¹⁴ Department of Justice, press release, “Austin Felon Pleads Guilty to Possessing an Assault Rifle,” June 6, 2012, <http://www.fbi.gov/minneapolis/press-releases/2012/austin-felon-pleads-guilty-to-possessing-an-assault-rifle>.

guilty to “possession with intent to distribute more than 50 grams of high-purity methamphetamine.”¹¹⁵

- In January 2011, William White, a onetime member of the NSM and founder of his own white supremacist organization, was convicted¹¹⁶ of soliciting violence online against the jury foreman in *U.S. v. Matthew Hale*.¹¹⁷ In April 2011, a federal judge reversed White’s conviction. The judge ruled that prosecutors had failed to prove that White actually intended to harm the foreman and that White’s web posting regarding the foreman was protected by the First Amendment.¹¹⁸ In an unrelated case, in December 2009, White was convicted of four counts of communicating threats in interstate commerce and one count of witness intimidation. One of the convictions for communicating threats in interstate commerce was later reversed.¹¹⁹ The witness intimidation charges involved White reportedly attempting to “delay or prevent the testimony” of African Americans in a discrimination case.¹²⁰ According to publicly available information, in 2005 and 2006 White was involved with NSM, for a time serving as its national spokesman.¹²¹ His activity with NSM ceased after he had a falling out with Schoep.¹²²

¹¹⁵ Department of Justice, press release, “Mendota Heights Man Pleads Guilty to Possessing Methamphetamine,” July 11, 2012, <http://www.fbi.gov/minneapolis/press-releases/2012/mendota-heights-man-pleads-guilty-to-possessing-methamphetamine>.

¹¹⁶ Department of Justice, press release, “Self-Proclaimed White Supremacist William White Convicted of Soliciting Violence Against Hale Jury Foreman,” January 5, 2011, <http://www.fbi.gov/chicago/press-releases/2011/cg010511a.htm>.

¹¹⁷ Matthew Hale was convicted of soliciting the murder of U.S. District Judge Joan Humphrey Lefkow. In the mid 1990s, Hale revived the Church of the Creator fortunes. He changed the organization’s name to the World Church of the Creator, and according to a watchdog group, by 2002 it had more chapters in the United States than any other neo-Nazi organization. Judge Lefkow had originally ruled in favor of Hale in a trademark infringement case involving the name “World Church of the Creator.” Her ruling was reversed on appeal, and as a result, she had to enforce the higher court’s reversal. Via email and during a conversation, Hale discussed with his security chief the idea of killing Lefkow. Hale did not know that his security chief was an FBI informant. In 2003, Hale was arrested for soliciting the murder of Judge Lefkow, and this, as well as his subsequent conviction on charges related to the case, hastened a downturn in fortune for his World Church of the Creator. Hale is serving a 40-year prison term. After another name change, the group—currently known simply as the Creativity Movement—shows signs of revival under new leadership. See Michael, *Theology of Hate*, pp. 120-133, 173-188; Southern Poverty Law Center, “Creativity”; Chris Dettro, “Follow-Up File: White Supremacist Finds Quiet Life in Prison,” *The State Journal-Register*, Springfield, IL, October 25, 2010; Larry Keller, “From the Ashes,” *Intelligence Report*, Southern Poverty Law Center, no. 140 (winter 2010), pp. 12-14; Federal Bureau of Investigation, “A Different Breed of Terrorist,” June 6, 2004, <http://www.fbi.gov/news/stories/2004/june/hale060904>.

¹¹⁸ Laurence Hammack, “Judge Tosses William A. White Verdict,” *The Roanoke Times*, April 20, 2011, <http://www.roanoke.com/news/roanoke/wb/283883>.

¹¹⁹ Department of Justice, press release, “Roanoke, Virginia Neo-Nazi Sentenced for Threats, Witness Intimidation,” April 14, 2010, <http://www.justice.gov/opa/pr/2010/April/10-crt-410.html>.

¹²⁰ Ibid. See also Laurence Hammack, “Former Neo-Nazi Leader Gets 3 More Months in Prison,” October 23, 2012, <http://hamptonroads.com/2012/10/former-neonazi-leader-gets-3-more-months-prison>.

¹²¹ Laurence Hammack, “White’s Life on Fringe Puts Him at Center of Storm,” *The Roanoke Times*, July 26, 2009, <http://www.roanoke.com/news/roanoke/wb/213109>.

¹²² Ibid; Southern Poverty Law Center, “Bill White,” 2011, <http://www.splcenter.org/get-informed/intelligence-files/profiles/bill-white>. For other cases involving individuals allegedly tied to NSM, see Department of Justice, press release, “Valley Man Enters Guilty Plea for Possession and Transport of an Improvised Explosive Device,” September 27, 2011, http://www.fbi.gov/phoenix/press-releases/2011/valley-man-enters-guilty-plea-for-possession-and-transport-of-an-improvised-explosive-device?utm_campaign=email-Immediate&utm_medium=email&utm_source=phoenix-press-releases&utm_content=34188; Department of Justice, press release, “Valley Man Indicted for Possessing and (continued...) ”

Racist Skinheads

In the United States, racist skinheads have a legacy stretching back to the early 1980s.¹²³ However, skinhead culture originated in the United Kingdom in the late 1960s and today has a global reach.¹²⁴ Since the early 2000s, the movement in the United States has been characterized by a proliferation of regional groups or crews rather than a united core organization.¹²⁵ In law enforcement circles, racist skinheads have a reputation for violence. This is “reinforced by hate-filled white power music and literature.” “[T]hey foster [their reputed toughness] through their appearance (shaved heads or close-cropped hair, white power tattoos) and dress (bomber jackets, ‘braces’ (suspenders), steel-toed boots).”¹²⁶

Skinheads emerged as a non-racist movement among British working-class youth in the late 1960s. These early skinheads rejected the hippie lifestyle and embraced elements of Jamaican culture, particularly reggae and ska music. As immigration from South Asia to the U.K. grew, some white British skinheads embraced racism and neo-Nazism. This racist skinhead variant of the subculture materialized in the U.S. Midwest and in Texas in the early 1980s.¹²⁷

In the mid-1990s, many U.S.-based racist skinhead groups allied with one another to form the Hammerskin Nation (HSN). HSN eventually developed chapters throughout the United States and in Europe. It had its own annual meeting/concert called Hammerfest, ran a record label, and had a publishing company. In the early 2000s, other groups such as the Outlaw Hammerskins, Hoosier State Hammerskins, and Ohio State Skinheads challenged HSN for preeminence. These groups saw HSN as “elitist.”¹²⁸ In 2011, by one measure, 133 skinhead groups were active in the United States.¹²⁹

In January 2010, the FBI released a bulletin that, among other things, emphasized that some racist skinheads formed the most violent segment of WSE adherents.¹³⁰ This supported the findings in a 2008 FBI assessment.¹³¹ Between 2007 and 2009, skinheads were involved in 36 of the 53 violent

(...continued)

Transporting Improvised Explosive Devices,” January 26, 2011, <http://phoenix.fbi.gov/dojpressrel/pressrel11/px012611.htm>; Rudabeh Shahbazi, “Documents Show Apache Junction Man Planned To Take IEDs to the Border,” *ABC 15*, http://www.abc15.com/dpp/news/region_southeast_valley/apache_junction/documents-show-apache-junction-man-planned-to-take-ieds-to-the-border; Federal Bureau of Investigation, “Domestic Terrorism: Tip Leads to Sting, Prison for Plotter,” November 29, 2006, http://www.fbi.gov/news/stories/2006/november/terror_112906.

¹²³ Southern Poverty Law Center, *Skinheads in America: Racists on the Rampage*, p. 3, http://www.splcenter.org/sites/default/files/downloads/publication/Skinhead_Report.pdf. Hereinafter: Southern Poverty Law Center, *Skinheads*.

¹²⁴ Ibid.

¹²⁵ Ibid., p. 13; Federal Bureau of Investigation, *Rage and Racism*, p. 8.

¹²⁶ Federal Bureau of Investigation, *Rage and Racism*, pp. 5-6.

¹²⁷ Michael R. Ronczkowski, *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*, 2nd ed. (Boca Raton, FL: CRC Press, Taylor and Francis Group, 2007), pp. 40-41. Hereinafter: Ronczkowski, *Terrorism*. Southern Poverty Law Center, *Skinheads*, pp. 3-4.

¹²⁸ Southern Poverty Law Center, *Skinheads*, p. 5.

¹²⁹ See Mark Potok, “The Year in Hate and Extremism,” *Intelligence Report*, Southern Poverty Law Center, no. 145 (Spring 2012), p. 46. Hereinafter: Potok, “The Year.” Potok notes that this count of skinhead groups “understates their numbers” because “skinheads are migratory and often not affiliated with groups.”

¹³⁰ Federal Bureau of Investigation, *White Supremacist Extremist Violence Possibly Decreases But Racist Skinheads Remain the Most Violent*, January 28, 2010. Hereinafter: Federal Bureau of Investigation, *White Supremacist Extremist Violence*.

¹³¹ Federal Bureau of Investigation, *Rage and Racism: Skinhead Violence on the Far Right*, December 10, 2008. (continued...)

incidents the FBI identified in the United States as being tied to WSE proponents.¹³² The Bureau has stated that “violence is an integral part of the racist skinhead subculture.”¹³³ Elements within the fractious movement even target one another.¹³⁴ These criminal acts are typically unrehearsed and opportunistic, targeting nonwhites and “other religious and social minorities.”¹³⁵

An apparent recent exception involved greater levels of planning. One man was convicted and two others pled guilty in a Connecticut case that involved the illegal sale of firearms and homemade grenades. The scheme included multiple meetings between late 2008 and early 2010 to negotiate the transactions, prepare the firearms, and assemble the grenades. The trio was tied to a skinhead group known as Battalion 14 (originally called the Connecticut White Wolves). They sold the weapons to a convicted felon working as an FBI cooperating witness. The informant posed as a member of the Imperial Klans of America, a Ku Klux Klan organization. Two others in the case, including the leader of Battalion 14 and a man not tied to the group, were acquitted of charges.¹³⁶

Anti-Government Extremists

As mentioned above, DOJ considers both unauthorized militias and sovereign citizens as anti-government extremists. *Neither militia membership nor advocacy of sovereign citizen tenets makes one a terrorist or a criminal.* However, in some instances both militia members and sovereign citizens have committed crimes driven in part by their ideologies.

Militia Extremists

The militia movement emerged in the 1990s as a collection of armed, paramilitary groups formed to stave off what they perceived as intrusions of an invasive government.¹³⁷ Central to this is a fear of firearm confiscation by a federal government thought to be out of control. Some adherents

(...continued)

Hereinafter: Federal Bureau of Investigation, *Rage and Racism*.

¹³² Federal Bureau of Investigation, *White Supremacist Extremist Violence*, p. 4.

¹³³ Federal Bureau of Investigation, *Rage and Racism*, p. 5.

¹³⁴ Southern Poverty Law Center, *Skinheads*, pp. 5, 16.

¹³⁵ Federal Bureau of Investigation, *Rage and Racism*, p. 5.

¹³⁶ Department of Justice, press release, “Milford Man Sentenced to 10 Years in Prison for Making Grenades and Selling Guns Intended for White Supremacist Group,” May 5, 2011, <http://newhaven.fbi.gov/dojpressrel/pressrel11/nh050511.htm>; Michael P. Mayko, “Two Acquitted in White Wolves Conspiracy Case,” *Connecticut Post*, December 2, 2010, <http://www.ctpost.com/local/article/Two-acquitted-in-White-Wolves-conspiracy-case-850538.php>; Michael P. Mayko, “White Wolves Called ‘Home Grown Terrorists,’” *Connecticut Post*, November 16, 2010, <http://www.ctpost.com/news/article/White-Wolves-called-home-grown-terrorists-812091.php>; Anti-Defamation League, “Connecticut White Supremacists Indicted on Firearms and Explosives Charges,” March 24, 2010; http://www.adl.org/learn/extremism_in_the_news/White_Supremacy/ct_arrets_batallian_14.htm?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_the_News. For another case allegedly involving racist skinheads, see Amy Pavuk and Henry Pierson Curtis, “Details Emerge in Osceola Skinhead Race-War Case,” *Orlando Sentinel*, May 8, 2012, http://articles.orlandosentinel.com/2012-05-08/news/os-white-supremacist-american-front-20120508_1_skinhead-american-front-cloud-police.

¹³⁷ Institute for Intergovernmental Research, *Investigating Terrorism and Criminal Extremism: Terms and Concepts*, Version 1.0, (Tallahassee, Florida: Institute for Intergovernmental Research, 2005), p. 49; Hereinafter: Institute for Intergovernmental Research, *Investigating Terrorism*.

also believe in anti-Semitic and racist ideologies.¹³⁸ Regardless, most militia members engage in constitutionally protected activity.

Militia groups typically coalesce around a specific leader. Groups can run training compounds where they rehearse paramilitary tactics, practice their survival skills, and receive weapons instruction and lessons in movement ideology. Some militia groups also maintain websites for recruitment and fundraising.¹³⁹ Extremists within the movement who run afoul of law enforcement “tend to stockpile illegal weapons and ammunition, trying illegally to get their hands on fully automatic firearms or attempting to convert weapons to fully automatic. They also try to buy or manufacture improvised explosive devices.”¹⁴⁰

Segments of the militia movement believe that the U.S. government is either run by some hidden conspiracy or is an overreaching sham. Some see a “New World Order” controlling U.S. institutions such as the media and the federal government. They contend that this is partly fostered by international organizations such as the United Nations. From this perspective, these organizations sap American sovereignty. Some militia supporters believe that agents of an un-authentic “Shadow Government” are interested in seizing lawfully owned firearms as part of a plan to undermine democracy.¹⁴¹ Importantly, others in the militia movement hold that the federal government has overstepped its constitutional bounds.¹⁴² One scholar has noted that some militia members assert that they have “the right to organize, purchase and use firearms, and enforce the law against agents of the government who behave unconstitutionally.”¹⁴³

A small minority of Americans who held anti-government fears formed militias largely in response to two incidents in the early 1990s. These were confrontations between federal law enforcement and private citizens at Ruby Ridge, ID, and at a site near Waco, TX.¹⁴⁴ Both involved warrants related to firearms violations.

- In August 1992, Randy Weaver and his family were engaged in an 11-day standoff with federal law enforcement agents. Randy Weaver had failed to appear in court on firearms-related charges in 1991. Subsequently, an unsuccessful operation to arrest Weaver led to the death of his 14-year-old son and a U.S. Marshal. It also precipitated the standoff. During the standoff, Weaver and a friend were shot and wounded. An FBI sniper also shot and killed Weaver’s wife, Vicki.¹⁴⁵ Weaver was eventually found guilty of failing to appear in court on the

¹³⁸ Arizona Counter-Terrorism Information Center, “Sovereign Citizens and Militia Information,” August 19, 2008, p. 1.

¹³⁹ Lane Crothers, “The Cultural Foundations of the Modern Militia Movement,” *New Political Science*, vol. 24, no. 2 (2002), p. 231. Hereinafter: Crothers, “The Cultural.”

¹⁴⁰ Federal Bureau of Investigation, “Domestic Terrorism: Focus on Militia Extremism,” September 22, 2011, http://www.fbi.gov/news/stories/2011/september/militia_092211/militia_092211.

¹⁴¹ Lane Crothers, *Rage on the Right: The American Militia Movement from Ruby Ridge to Homeland Security* (Lanham, MD: Rowman and Littlefield, 2003), p. 57. Hereinafter: Crothers, *Rage on the Right*.

¹⁴² Crothers, “The Cultural,” pp. 226-228.

¹⁴³ *Ibid.*, p. 228.

¹⁴⁴ *Ibid.*, pp. 230-231. See also Michael Barkun, “Appropriated Martyrs: The Branch Davidians and the Radical Right,” *Terrorism and Political Violence*, vol. 19, no. 1 (2007), p. 120. Hereinafter: Barkun, “Appropriated Martyrs.” See also Steven M. Chermak, *Searching for a Demon: The Media Construction of the Militia Movement*, (Boston: Northeastern University Press, 2002).

¹⁴⁵ Stuart A. Wright, *Patriots, Politics, and the Oklahoma City Bombing* (New York: Cambridge University Press, 2007), pp. 142-148. Hereinafter: Wright, *Patriots*. Weaver has been described as a survivalist who believed in the (continued...)

gun charges that played a role in the standoff. In October 1993, he was sentenced to 18 months in jail and a \$10,000 fine. In 1995, Weaver received a \$3.1 million settlement in a wrongful death suit filed against the U.S. government.¹⁴⁶ The events at Ruby Ridge helped precipitate the militia movement, whose members tend to view Randy Weaver as a hero and demonize the federal government.¹⁴⁷

- The militia movement also emerged because of the 51-day standoff between federal law enforcement and a religious sect named the Branch Davidians near Waco.¹⁴⁸ On February 28, 1993, an unsuccessful attempt by ATF agents to arrest the sect's leader, David Koresh, initiated the events near Waco. He was wanted on suspicion of federal firearms and explosives violations.¹⁴⁹ Four ATF agents and six Branch Davidians died in a gunfight during the operation.¹⁵⁰ Protracted discussions followed between federal negotiators and Koresh. These failed. On April 19, federal agents assaulted the Davidian compound, which caught on fire. At least 75 Branch Davidians perished in the assault.¹⁵¹

If the incidents involving the Weavers and the Branch Davidians helped form the militia movement, Timothy McVeigh's bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, helped usher in a temporary decline.¹⁵² In the bombing's aftermath, militia groups received greater law enforcement scrutiny.¹⁵³ The bombing claimed 168 lives, and until 9/11 was the largest single act of terrorism on U.S. soil. The militia movement included 441 groups in 1995. By 2000, this number was reportedly down to 72.¹⁵⁴ Although McVeigh's bombing cannot fully account for a dip in militia activity, it impacted the movement by causing some groups to temper their rhetoric while others grew more extreme, and militias became more marginalized.¹⁵⁵

The militia movement has experienced a recent resurgence. One watchdog group has attributed this partly to a rise in anti-government anger since 2008.¹⁵⁶ According to another organization, the number of militias in the United States jumped from 42 in 2008 to 334 in 2011 (see **Figure 1**).

(...continued)

Christian Identity religion. See Barkun "Appropriated Martyrs," p. 118. He has also been described as holding white supremacist beliefs and was not a militia member. See Crothers, *Rage on the Right*, pp. 78-79.

¹⁴⁶ Crothers, *Rage on the Right*, p. 90.

¹⁴⁷ Wright, *Patriots*, pp. 149-152; Crothers, *Rage on the Right*, pp. 92-97; Barkun, "Appropriated Martyrs," pp. 120-121.

¹⁴⁸ Crothers, *Rage on the Right*, p. 104.

¹⁴⁹ Department of Justice, *Report to the Deputy Attorney General on the Events at Waco, Texas*, October 8, 1993, <http://www.justice.gov/publications/waco/wacoexec.html>. The Branch Davidian sect emerged from the Seventh-Day Adventist Church and was formed in 1929. The two severed official ties with one another in 1934. David Koresh was not a militia member. See Crothers, *Rage on the Right*, pp. 100-101.

¹⁵⁰ Crothers, *Rage on the Right*, p. 105.

¹⁵¹ Crothers, *Rage on the Right*, p. 110.

¹⁵² McVeigh was not a militia member, but he interacted with others who were.

¹⁵³ Devlin Barrett and Eileen Sullivan, "FBI Sees Little Chance of Copycat Militia Plots," *Associated Press*, March 31, 2010.

¹⁵⁴ Potok, "The Year," p. 42.

¹⁵⁵ Crothers, *Rage on the Right*, p. 138, 147.

¹⁵⁶ Anti-Defamation League, *Rage Grows in America: Anti-Government Conspiracies, the Resurgence of the Militia Movement*, November 16, 2009, http://www.adl.org/special_reports/rage-grows-in-America/militia-movement.asp.

The recent resurgence may exhibit a key difference from its precursor. Social networking websites have encouraged looser organization of smaller, largely web-based cells.¹⁵⁷

Several examples highlight how some militia adherents have allegedly engaged in criminal activity since 9/11.

- In November 2011, the FBI arrested four retirees, Samuel J. Crump, Ray H. Adams, Dan Roberts, and Frederick W. Thomas, who allegedly formed a fringe militia group and planned violent attacks on government officials. The group, based in northern Georgia, purportedly had ties to an unnamed militia organization. According to DOJ, the quartet “discussed multiple criminal activities, ranging from murder; theft; manufacturing and using toxic agents; and assassinations in an effort to undermine federal and state government and to advance their interests.”¹⁵⁸ Between June and November 2011, Roberts and Thomas met with an FBI undercover agent to negotiate the purchase of matériel for the plot: “a silencer for a rifle and conversion parts to make a fully automatic rifle, as well as explosives.”¹⁵⁹ In October, plotters reportedly discussed making ricin, a deadly poison derived from castor beans.¹⁶⁰ In April 2012, Roberts and Thomas pled guilty to conspiring to obtain an unregistered explosive device and silencer.¹⁶¹
- In June 2012, three individuals were found guilty in Anchorage, AK of conspiracy and firearms charges related to a scheme purportedly led by Francis “Schaeffer” Cox.¹⁶² He and his followers allegedly plotted “a potential retaliatory response to any attempt by law enforcement to arrest Cox, who had an outstanding bench warrant for not attending a trial over a misdemeanor weapons charge.”¹⁶³ They were members of the Alaska Peacemaker’s Militia based in

¹⁵⁷ Ibid.

¹⁵⁸ Department of Justice, press release, “North Georgia Men Arrested, Charged in Plots to Purchase Explosives, Silencer and to Manufacture a Biological Toxin,” November 1, 2011, <http://www.fbi.gov/atlanta/press-releases/2011/north-georgia-men-arrested-charged-in-plots-to-purchase-explosives-silencer-and-to-manufacture-a-biological-toxin>.

¹⁵⁹ Ibid.

¹⁶⁰ Craig Schneider, “Documents: Men with Castor Beans, Guns Worried about Getting Caught,” *Atlanta Journal-Constitution*, November 6, 2011, <http://www.ajc.com/news/documents-men-with-castor-1218644.html>.

¹⁶¹ Department of Justice, press release, “North Georgia Men Plead Guilty to Plot to Purchase Explosives and a Silencer,” April 10, 2012, http://www.fbi.gov/atlanta/press-releases/2012/north-georgia-men-plead-guilty-to-plot-to-purchase-explosives-and-a-silencer?utm_campaign=email-Immediate&utm_medium=email&utm_source=atlanta-press-releases&utm_content=86514.

¹⁶² Department of Justice, press release, “Guilty Verdicts in USA v. Cox, Barney, and Vernon,” June 19, 2012, <http://www.fbi.gov/anchorage/press-releases/2012/guilty-verdicts-in-usa-v.-cox-barney-and-vernon>.

¹⁶³ Department of Justice, press release, “Superseding Indictment Returned by Federal Grand Jury Against Fairbanks-Area Men for Conspiracy to Kill Federal Officers,” January 23, 2012, <http://www.fbi.gov/anchorage/press-releases/2012/superseding-indictment-returned-by-federal-grand-jury-against-fairbanks-area-men-for-conspiracy-to-kill-federal-officers>. Sam Friedman, “Details Emerge in Alleged Plot to Kill Alaska State Troopers, Judge,” *Fairbanks Daily News-Miner*, March 3, 2011, http://www.newsminer.com/view/full_story/12322747/article-Details-emerge-in-alleged-plot-to-kill-Alaska-State-Troopers-judge?instance=home_news_window_left_top_2. Cox has also been described as a sovereign citizen (discussed below). See Sam Friedman, “The Schaeffer Cox File: The Trail of a Young Man,” *Fairbanks Daily News-Miner*, April 10, 2011, http://www.newsminer.com/view/full_story/12739189/article-The-Schaeffer-Cox-File-The-trail-of-a-young-man?instance=home_most_popular2; For a related case see Department of Justice, press release, “Salcha Couple Pleads Guilty to Conspiracy to Murder Federal Officials,” August 27, 2012, <http://www.fbi.gov/anchorage/press-releases/2012/salcha-couple-pleads-guilty-to-conspiracy-to-murder-federal-officials>; Department of Justice, press release, “Couple Charged with Conspiracy to Murder Judge and Federal (continued...)”.

Fairbanks, AK and also held sovereign citizen beliefs. The plotters supposedly codenamed their plan “241 (two for one),” because they reputedly intended to kill two government officials for every militia member killed in the operation.¹⁶⁴

The above alleged activities are not necessarily indicative of trends toward violence in the larger militia movement, and in one prominent case, DOJ failed to convince the presiding judge of serious charges revolving around a purported violent plot. In March 2012, a federal judge acquitted members of a Michigan Militia group known as the Hutaree on charges of seditious conspiracy or rebellion against the United States and conspiring to use weapons of mass destruction. The judge also cleared the accused Hutaree members of weapons crimes related to the conspiracies.¹⁶⁵

The case garnered headlines in March 2010, when nine Hutaree members were indicted for allegedly preparing to violently confront U.S. law enforcement.¹⁶⁶ Their supposed plotting included the murder of a local law enforcement officer and an attack on fellow officers who gathered in Michigan for the funeral procession. According to DOJ, the Hutaree discussed the use of explosives against the funeral procession.¹⁶⁷ Audio recordings by an undercover FBI agent of reputed Hutaree leader David Brian Stone capture him discussing the New World Order and how, “it’s time to strike and take our nation back so we will be free of tyranny.... The war will come whether we are ready or not.”¹⁶⁸ According to DOJ, the group had a hit list that included federal judges, among others.¹⁶⁹ However, during the trial an Assistant U.S. Attorney acknowledged that the Hutaree had not formed a “specific plan” to attack government targets.¹⁷⁰ U.S. District Judge Victoria Roberts stated that, “The court is aware that protected speech and mere words can be

(...continued)

Firearms Crimes, Two Others Indicted for Conspiracy to Possess Destructive Devices and Illegal Weapons,” March 17, 2011, <http://www.fbi.gov/anchorage/press-releases/2011/couple-charged-for-conspiracy-to-murder-judge-and-federal-firearms-crimes>.

¹⁶⁴ For examples of other militia adherents involved in crime, see Meghann M. Cuniff, “Health Problems Reduce Militia Leader’s Sentence,” *The Spokesman-Review*, August 11, 2011, <http://www.spokesman.com/stories/2011/aug/11/health-problems-reduce-militia-leaders-sentence/>; Bill Morlin, “Idaho Militia Leader Sentenced for Weapons, Bombs,” *Hatewatch*, Southern Poverty Law Center, August 9, 2011, <http://www.splcenter.org/blog/2011/08/09/idaho-militia-leader-sentenced-for-weapons-bombs/?ondntsrc=MBQ110870HTW&newsletter=HW081111>; David Cole, “Militia Member Sentenced on Federal Firearms and Explosives Charges,” *Coeur d’Alene Press*, August 9, 2011, http://www.cdapress.com/news/local_news/article_0cb55774-c2dc-11e0-9136-001cc4c03286.html; Federal Bureau of Investigation, “Preventing Terrorist Attacks on U.S. Soil: The Case of the Wrong Package Falling into the Right Hands,” April 9, 2004, <http://www.fbi.gov/news/stories/2004/april/krar040904>; Scott Gold, Case Yields Chilling Signs of Domestic Terror Plot,” *Los Angeles Times*, January 7, 2004.

¹⁶⁵ Ed White, “Michigan Militia Members Cleared of Conspiracy,” *Associated Press*, March 27, 2012, http://abcnews.go.com/US/wireStory/critical-charges-dropped-michigan-militia-16013255?singlePage=true#T3MB5kd_lLc. Hereinafter: White, “Michigan Militia.”

¹⁶⁶ Department of Justice, press release, “Nine Members of a Militia Group Charged with Seditious Conspiracy and Related Charges,” March 29, 2010, <http://www.fbi.gov/detroit/press-releases/2010/de032910.htm>.

¹⁶⁷ *Ibid.*

¹⁶⁸ Corey Williams and Jeff Karoub, “Prosecutor: Undercover FBI Agent Infiltrated Militia,” *Associated Press*, March 31, 2010.

¹⁶⁹ Dan Harris, Emily Friedman, and Tahman Bradley, “Undercover Agent Key Witness Against Hutaree Militia Members,” *ABC News*, April 1, 2010, <http://abcnews.go.com/GMA/undercover-agent-credited-hutaree-militia-bust/story?id=10257584>.

¹⁷⁰ Robert Snell and Christine Ferretti, “Key Charges Dropped Against Hutaree Militia,” *Detroit News*, March 28, 2011, <http://www.detroitnews.com/article/20120328/METRO/203280376/Key-charges-dropped-against-Hutaree-militia?odysey=mod|newswell|text|FRONTPAGE|s>.

sufficient to show a conspiracy. In this case, however, they do not rise to that level.”¹⁷¹ Three Hutaree members pled guilty to firearms charges.¹⁷²

Sovereign Citizen Movement

The FBI defines the sovereign citizen movement as “anti-government extremists who believe that even though they physically reside in this country, they are separate or ‘sovereign’ from the United States. As a result, they do not accept any government authority, including courts, taxing entities, motor vehicle departments, or law enforcement.”¹⁷³ However, simply holding these views is not a criminal act, and numerous movement adherents solely exercise their beliefs via constitutionally protected activities.

The ideas behind the movement originated during the 1970s with a group known as the Posse Comitatus and enjoyed some popularity in extremist circles during the 1980s and 1990s.¹⁷⁴ Early on, the movement featured white supremacist elements, but this has not kept some African Americans from subscribing to its ideals in recent years.¹⁷⁵ In the 1990s, the movement attracted 250,000 followers and was marked by the FBI’s standoff with a group known as the Montana Freeman that lasted 81 days.¹⁷⁶ Current estimates suggest a membership of 300,000.¹⁷⁷

For the most part, the sovereign citizen movement is diffuse and includes few organized groups.¹⁷⁸ The FBI suggests that sovereigns “operate as individuals without established leadership

¹⁷¹ White, “Michigan Militia.”

¹⁷² See Department of Justice, Press Release, “Members of the Hutaree Militia Plead Guilty to Weapons Charges,” March 29, 2012, http://www.fbi.gov/detroit/press-releases/2012/members-of-the-hutaree-militia-plead-guilty-to-weapons-charges?utm_campaign=email-Immediate&utm_medium=email&utm_source=detroit-press-releases&utm_content=83489; Matthew Dolan, “Defendant in Michigan Militia Case Changes Plea to Guilty,” December 6, 2011, http://online.wsj.com/article/SB10001424052970204083204577080630555077796.html?mod=googlenews_wsj. When the Hutaree suspects were arrested in the case, some militia members in Michigan did not support the group’s alleged scheming. For example, a member of another militia group in Michigan provided information to authorities regarding the whereabouts of a fugitive Hutaree militia member. See Kirk Johnson, “Militia Draws Distinctions Between Groups,” *New York Times*, March 31, 2010, <http://www.nytimes.com/2010/04/01/us/01michigan.html>. Also, a militia leader from Michigan has said that the Hutaree case, “caused a rift in the militia movement about whether this is the sort of group we want to rally behind or if what they were doing was outside the scope of what’s acceptable.” See Robert Snell, “Militias Split over Defending Hutaree,” *Detroit News*, March 31, 2011.

¹⁷³ Federal Bureau of Investigation, “Domestic Terrorism: The Sovereign Citizen Movement,” April 13, 2010, http://www.fbi.gov/news/stories/2010/april/sovereigncitizens_041310. Hereinafter: Federal Bureau of Investigation, “Sovereign Citizen.”

¹⁷⁴ Anti-Defamation League, “Sovereign Citizen Movement,” http://www.adl.org/learn/ext_us/scm.asp?xpicked=4; Casey Sanchez, “Return of the Sovereigns,” *Intelligence Report*, Southern Poverty Law Center, no. 133 (spring 2009), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2009/spring/return-of-the-sovereigns>.

¹⁷⁵ Sarah Netter, “Anti-Government Sovereign Citizens Taking Foreclosed Homes Using Phony Deeds, Authorities Say,” *ABC News*, August 23, 2010, <http://abcnews.go.com/US/georgia-battling-sovereign-citizens-squatting-foreclosed-homes/story?id=11445382>. See Leah Nelson, “Sovereigns in Black,” *Intelligence Report*, Southern Poverty Law Center, no. 143 (Fall 2011), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2011/fall/-sovereigns-in-black>.

¹⁷⁶ Patrik Jonsson, “‘Sovereign citizens’: Is Jared Loughner a sign of revived extremist threat?” *Christian Science Monitor*, March 9, 2011, <http://www.csmonitor.com/USA/2011/0309/Sovereign-citizens-Is-Jared-Loughner-a-sign-of-revived-extremist-threat>.

¹⁷⁷ *Ibid.*

¹⁷⁸ One sovereign citizens group is the “Republic for the united States of America” (RuSA) which is based in Alabama. RuSA is a successor to a group known as the Guardians of the Free Republics (GFR), which in 2010 mailed letters to the governors of all 50 U.S. states urging them to leave office. See Southern Poverty Law Center, “Sovereign (continued...)”

and only come together in loosely affiliated groups to train, help each other with paperwork [critical to some of their schemes], or socialize and talk about their ideology.”¹⁷⁹ The movement involves leaders described as “gurus” who proselytize online, in print publications, or via in-person seminars. These gurus rouse followers into believing a conspiracy theory in which the legitimate federal government has been replaced by a government designed to take away the rights of ordinary citizens.¹⁸⁰ This shares the same broad interplay between concepts of legitimate and illegitimate rule seen in the New World Order and WSE theories about ZOG. Gurus can also promote illegal techniques that individuals can use to supposedly cut their ties to the federal government or avoid its reach, particularly when it comes to taxation.¹⁸¹

Sovereign citizens reject the legitimacy of much of the U.S. legal system.¹⁸² Many believe that the 14th Amendment “shifted the nation from its original common-law roots with states’ rights to a federal corporation that legally enslaved everyone.”¹⁸³ According to movement members, the amendment ushered in an illegitimate federal government by supposedly abrogating individual rights and replacing them with a system that “grant[ed] privileges through contracts such as marriage and driver’s licenses, gun permits, and property codes.”¹⁸⁴

By ignoring all sorts of laws, avoiding taxes, disregarding permit requirements, and destroying government-issued identification documents, some sovereign citizens have tried to cut formal ties with what they perceive as an illegitimate regime.¹⁸⁵ Sovereigns have filed court documents stating that they are not U.S. citizens.¹⁸⁶ They have also created bogus financial documents to harass or defraud their enemies. (For more information, see the “Paper Terrorism”: Liens, Frivolous Lawsuits, and Tax Schemes” section in this report).

Sovereign citizens have in some instances created fictitious entities and used fake currency, passports, license plates, and driver licenses. In 2009, a federal jury found three men guilty of conspiring to use and sell fraudulent diplomatic credentials and license plates that they believed allowed “their customers [to] enjoy diplomatic immunity and [to] no longer ... pay taxes or be

(...continued)

President,” *Intelligence Report*, Southern Poverty Law Center, no. 143 (Fall 2011), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2011/fall/-sovereign-president>.

¹⁷⁹ Federal Bureau of Investigation, Counterterrorism Analysis Section, “Sovereign Citizens: A Growing Domestic Threat to Law Enforcement,” *FBI Law Enforcement Bulletin*, (September 2011), <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2011>. Hereinafter: FBI Counterterrorism Analysis Section, “Sovereign Citizens.”

¹⁸⁰ Anti-Defamation League, *The Lawless Ones: The Resurgence of the Sovereign Citizen Movement*, August 9, 2010, pp. 2-6, http://www.adl.org/learn/sovereign_movement/sovereign_citizens_movement_report.pdf. Hereinafter: Anti-Defamation League, *The Lawless*.

¹⁸¹ *Ibid.*, p. 6.

¹⁸² However, this reportedly does not keep some sovereign citizen extremists from cashing government paychecks. See J.J. McNabb, “Working for the Man: Anti-Government Extremists Who Cash Government Paychecks,” *Forbes*, March 5, 2012, <http://www.forbes.com/sites/jjmacnab/2012/03/05/working-for-the-man-anti-government-extremists-who-cash-government-paychecks/2/>.

¹⁸³ Tom Morton, “Sovereign Citizens Renounce First Sentence of 14th Amendment,” *Casper Star-Tribune*, April 17, 2011, http://trib.com/news/local/casper/article_a5d0f966-7ed0-549f-a066-b1b2c91f9489.html.

¹⁸⁴ *Ibid.*

¹⁸⁵ Anti-Defamation League, *The Lawless*, pp. 4-5.

¹⁸⁶ Lance Griffin, “Sovereigns’ Gain Attention of Law Enforcement,” *Dothan Eagle*, May 21, 2011, <http://www2.dothanegale.com/news/2011/may/21/3/sovereigns-gain-attention-law-enforcement-ar-1872889/>.

subject to being stopped, detained, or arrested by law enforcement personnel.”¹⁸⁷ In 2003, Ronald K. Delorme developed the Pembina Nation Little Shell Band of North America¹⁸⁸ into a sovereign citizen group.¹⁸⁹ It is a sham Native American tribe that anyone can join to try and avoid taxes and government-imposed costs, such as auto registration fees. For example, news reports indicate that in June 2010, a sheriff’s deputy in Florida pulled over John McCombs when the law enforcement official noticed a Pembina Nation Little Shell license plate on the motorcycle McCombs was driving. According to publicly available sources, McCombs presented a fraudulent letter of diplomatic immunity and an invalid Pembina Nation Little Shell vehicle registration.¹⁹⁰

Some sovereign citizen fraud appears to be motivated by economic opportunism rather than ideology.¹⁹¹ This includes “pyramid schemes, other investment schemes, bogus trust scams, real estate fraud, and various types of tax frauds [as well as] more esoteric scams ... ranging from immigration fraud to malpractice insurance fraud.”¹⁹² In November 2011, husband and wife Monty and Patricia Ervin were convicted in federal court of conspiring to defraud the United States as well as three counts of tax evasion. In addition, the federal jury convicted Patricia of structuring transactions to avoid bank reporting requirements.¹⁹³ The couple allegedly had not filed federal income tax returns between 2000 and 2008, denied their U.S. citizenship, and dubbed themselves “sovereign” when the IRS investigated.¹⁹⁴ The Ervins earned more than \$9 million from investment properties they owned.¹⁹⁵ A group of self-proclaimed sovereign citizens in North Georgia was indicted in March 2011 for using sovereign schemes to allegedly steal millions of dollars worth of real estate.¹⁹⁶

In a few recent cases, avowed sovereign citizens have been involved in violent altercations with law enforcement officers. According to a September 2011 FBI publication, since 2000 “lone-offender sovereign-citizen extremists have killed six law enforcement officers,” and the Bureau sees sovereign citizens as a growing threat to U.S. law enforcement.¹⁹⁷

- Perhaps the most publicized example of alleged sovereign violence directed at police occurred in 2010. In May of that year, two self-professed sovereign

¹⁸⁷ Department of Justice, press release, “Jury Convicts Three Men of Conspiracy To Use Fake Diplomatic Identification,” August 31, 2009, <http://www.state.gov/m/ds/rls/128533.htm>.

¹⁸⁸ The group is not a federally recognized tribe.

¹⁸⁹ Anti-Defamation League, *The Lawless*; Chris Gerbasi, “Tribal Claims Causing Charlotte Controversy,” *Sarasota Herald Tribune*, July 25, 2010; “Punta Gorda Man Arrested for Driving with Pembina Nation Plate,” *WINK News*, June 1, 2010, <http://www.winknews.com/Local-Florida/2010-06-01/Punta-Gorda-man-arrested-for-driving-with-Pembina-Nation-plate>.

¹⁹⁰ *Ibid.*

¹⁹¹ For a discussion of redemption as a scam, see Federal Bureau of Investigation, *Common Fraud Schemes*, <http://www.fbi.gov/scams-safety/fraud>.

¹⁹² Anti-Defamation League, *The Lawless*, p. 24.

¹⁹³ Department of Justice, press release, “Self-Proclaimed ‘Governor’ of Alabama and Wife Convicted of Tax Fraud,” November 4, 2011, <http://www.justice.gov/opa/pr/2011/November/11-tax-1459.html>. Hereinafter: Department of Justice, “Self-Proclaimed.”

¹⁹⁴ *Ibid.*; *United States v. Patricia Ervin and Monty Ervin*, Superseding Indictment, 1:11-CR-07-MHT, District Court, Middle District of Alabama, February 17, 2011.

¹⁹⁵ Department of Justice, “Self-Proclaimed.”

¹⁹⁶ Megan Matteucci, “12 ‘sovereign citizens’ indicted,” *Atlanta Journal-Constitution*, March 15, 2011, <http://www.ajc.com/news/dekalb/12-sovereign-citizens-indicted-873458.html>.

¹⁹⁷ FBI Counterterrorism Analysis Section, “Sovereign Citizens.”

citizens were involved in a violent confrontation with West Memphis, TN, police officers. During a traffic stop, Joe Kane fired an AK-47 assault rifle and killed two officers. Kane and his father Jerry fled the scene. Law enforcement sighted their vehicle in a nearby parking lot 90 minutes later. The duo died in the ensuing shootout, which also wounded two more officers.¹⁹⁸ The FBI had investigated Jerry Kane five years before the murders because he was allegedly traversing the United States peddling what the FBI termed a “debt elimination scheme.”¹⁹⁹

In June 2012, the FBI issued a bulletin suggesting that some sovereign extremists may be moving away from more spontaneous violence simply in *reaction* to encounters with police and are potentially preparing for conflict in advance, “making more specific plans to interfere with state and local law enforcement officers during traffic stops and, in some cases, intentionally initiating contact with law enforcement.”²⁰⁰

Other cases have garnered attention. For example, in July 2011 James M. Tesi allegedly shot at a local police officer trying to arrest him near Fort Worth, TX. Tesi was reportedly wounded in the altercation. Outstanding “arrest warrants for speeding, driving without a license in possession, and failure to appear” prompted the attempted apprehension.²⁰¹ Court documents described in news reporting noted that Tesi linked himself to a sovereign citizen group.²⁰² In February 2012, Tesi was found “guilty of aggravated assault on a public servant with a deadly weapon.”²⁰³ In June 2011, a police officer in Page, AZ, shot and killed William Foust while responding to a domestic violence 911 call. The shooting reportedly occurred during a physical struggle in which Foust attempted to “gain control of” the police officer’s Taser.²⁰⁴ According to a press account, Foust had declared his sovereign citizen status in court proceedings in Kenab, UT (about 75 miles from Page), related to a speeding ticket.²⁰⁵

¹⁹⁸ Cindy Wolff, “West Memphis Police Sued by Widow of Man Killed in Shootout,” *The Commercial Appeal*, April 21, 2011, <http://www.commercialappeal.com/news/2011/apr/21/west-memphis-police-sued-by-kanes-widow/>; Kristina Goetz, Cindy Wolff, “Grieving West Memphis Chief Raises National Curtain on Sovereign Citizens,” *The Commercial Appeal*, April 17, 2011, <http://www.commercialappeal.com/news/2011/apr/17/west-memphis-police-chief-sovereign-citizens/>.

¹⁹⁹ Scott Knoll, “The Warning That Never Came: What the FBI Knew About Jerry Kane,” *WREG*, March 2, 2011, <http://www.wreg.com/wreg-fbi-file-reveals-feds-investigated-kane-story,0,4377626.story>.

²⁰⁰ Federal Bureau of Investigation, *Recent Sovereign Citizen Extremist Targeting of Law Enforcement Highlights Potential for Violence during Traffic Stops*, June 1, 2012.

²⁰¹ Domingo Ramirez Jr., “Man in ‘Sovereign Citizen’ Group is Wounded in Shootout,” July 22, 2011, <http://www.star-telegram.com/2011/07/21/3238352/man-in-sovereign-citizen-group.html>.

²⁰² *Ibid.*

²⁰³ Steve Norder, “‘Sovereign Citizen’ Gets 35 Years for Assault on Officer,” *Fort Worth Star-Telegram*, February 1, 2012, <http://www.star-telegram.com/2012/01/31/3702338/sovereign-citizen-found-guilty.html>.

²⁰⁴ Todd Glasenapp and Larry Hendricks, “Page Officer Kills Man in DV Incident,” *Arizona Daily Sun*, June 21, 2011, http://azdailysun.com/news/local/crime-and-courts/article_61e27d9d-6d47-5655-8a71-d28b846d8e3e.html.

²⁰⁵ *Ibid.* For other violent plots with alleged sovereign ties, see Alyssa Newcomb, “Suspects in Louisiana Cop Killings Linked to Sovereign Citizens Movement,” *ABC News*, August 19, 2012, <http://abcnews.go.com/US/alleged-louisiana-cop-shooters-linked-sovereign-citizen-movement/story?id=17038353#.UL4plddrq1g>; J.J. MacNabb, “Sovereign Extremist Injured in Texas Bomb Explosion,” *Forbes*, July 3, 2012, <http://www.forbes.com/sites/jjmacnab/2012/07/03/sovereign-extremist-injured-in-texas-bomb-explosion/>.

Black Separatist Extremists

DOJ includes black separatism in its list of movements that potentially spawn domestic terrorists.²⁰⁶ However, most black separatists solely engage in constitutionally protected behavior. Since 9/11, there has been little public discussion of federal investigations involving black separatist extremists. One group exhibiting what can be described as black separatist views, the New Black Panther Party for Self Defense (NBPP), received national scrutiny over voter intimidation allegations involving members of its Philadelphia chapter during the 2008 federal general election.

The NBPP emerged in the early 1990s, and it is not tied to the Black Panthers from the 1960s.²⁰⁷ Watchdog groups have described the NBPP as “a virulently racist and anti-Semitic organization whose leaders have encouraged violence against whites, Jews, and law enforcement officers,”²⁰⁸ as well as “the largest organized anti-Semitic and racist black militant group in America.”²⁰⁹ The NBPP, which denies that it is a hate group, engages in “high-profile” rhetoric at rallies or demonstrations intended to encourage confrontation with authorities. The group’s actions occur “on behalf of the poor or disadvantaged, involving the ready display of firearms.”²¹⁰ As an example of the rhetoric the group uses, an NBPP representative characterized the March 2011 shooting death of a drug suspect in Jacksonville, FL, as “a violent act of terrorism” committed by police.²¹¹ Soon after the shooting, the Jacksonville Sheriff’s Office said that the confrontation involved undercover officers serving a search warrant at an apartment. Officers claimed that inside the apartment, the victim—an alleged drug dealer with a criminal record—was holding a firearm.²¹²

In 2008, the Philadelphia, PA, chapter of the NBPP was involved in a case that generated public controversy. A 2009 civil suit filed by DOJ claimed that two NBPP members wearing the group’s paramilitary uniforms loitered around the entrance to a 2008 federal general election polling station in Philadelphia. One of the NBPP members allegedly carried a nightstick. According to DOJ, some poll watchers feared for their safety because of this activity. Philadelphia police officers responding to claims of voter intimidation removed the nightstick-wielding NBPP member and allowed the other to remain (the latter was a certified poll watcher). Police asked people at the polling station whether they had been threatened by the two individuals. All those questioned replied that they had not. However, at least one individual claimed that the presence of the two NBPP members had been intimidating.²¹³ The NBPP disavowed the actions of its two

²⁰⁶ Department of Justice, *White Paper*, p. 59.

²⁰⁷ D.J. Mulloy, “New Panthers, Old Panthers, and the Politics of Black Nationalism in the United States,” *Patterns of Prejudice*, vol. 44, no. 3 (2010), pp. 217, 219, 229-236. Hereinafter: Mulloy: “New Panthers.”

²⁰⁸ Southern Poverty Law Center, “New Black Panther Party,” <http://www.splcenter.org/get-informed/intelligence-files/new-black-panther-party>.

²⁰⁹ Anti-Defamation League, “New Black Panther Party for Self Defense,” June 1, 2011, http://www.adl.org/main/Extremism/new_black_panther_party.htm.

²¹⁰ Mulloy: “New Panthers,” p. 223, 233.

²¹¹ “Black Panthers Protest Police Shooting,” October 14, 2011, <http://www.news4jax.com/news/Black-Panthers-Protest-Police-Shooting/-/475880/1962744/-/qs5j0xz/-/index.html>; “Black Panthers Protest Police Shooting,” *First Coast News*, March 19, 2011, <http://www.firstcoastnews.com/rss/article/197113/3/Black-Panthers-Protest-Police-Shooting>.

²¹² *Ibid.*

²¹³ Department of Justice, Office of Professional Responsibility, Report, *Investigation of Dismissal of Defendants in United States v. New Black Panther Party for Self-Defense, Inc. et al.*, March 17, 2011, pp. 6-8. Hereinafter: DOJ, (continued...)

members.²¹⁴ In May 2009, DOJ voluntarily dismissed claims against defendants in the case, and a July 2009 letter from 10 members of Congress to DOJ's Inspector General questioned the decision to do so. DOJ's Office of Professional Responsibility (OPR) investigated, and in March 2011, OPR issued a report which argued that DOJ officials did not act inappropriately regarding the matter.²¹⁵

Anti-Abortion Extremists

The vast majority of anti-abortion activists engage in constitutionally protected activity. However, anti-abortion extremism involves crime committed in the name of the anti-abortion movement. Sixty-six instances of "extreme violence" targeting abortion providers and clinics occurred in the United States from 1997 through 2010, according to one group that supports abortion rights and tracks criminal activity intended to limit access to abortion services.²¹⁶ These cases involved shootings, bombings, arson incidents, and acid attacks.²¹⁷ Since 1993, eight clinic workers have been murdered by anti-abortion extremists in the United States.²¹⁸ Because of a wave of violence focused on abortion providers in the 1980s and early 1990s, Congress passed and President Clinton signed into law the Freedom of Access to Clinic Entrances Act (FACE Act) (18 U.S.C. §248) in 1994.²¹⁹ As with other types of domestic terrorism investigations, it is unclear exactly which incidents of violence perpetrated against abortion providers the FBI considers terrorist acts.

The 2009 murder of George Tiller, an abortion provider, received sizeable public attention. On January 29, 2010, Scott Roeder was convicted of first-degree murder and two counts of aggravated assault for killing Tiller. Roeder shot Tiller while the latter was at church on May 31, 2009. Roeder was sentenced to "life in prison with no possibility of parole for 50 years."²²⁰

(...continued)

OPR, *Investigation of Dismissal*.

²¹⁴ Mulloy: "New Panthers," p. 217-218.

²¹⁵ DOJ, OPR, *Investigation of Dismissal*, pp. 1-3.

²¹⁶ National Abortion Federation, "Clinic Violence," http://www.prochoice.org/about_abortion/violence/history_extreme.asp. See also "NAF Violence and Disruption Statistics," http://www.prochoice.org/pubs_research/publications/downloads/about_abortion/stats_table2010.pdf.

²¹⁷ Ibid.

²¹⁸ NARAL Pro-Choice America Foundation, press release, "Anti-Choice Violence and Intimidation," January 1, 2011, <http://www.naral.org/media/fact-sheets/abortion-anti-choice-violence.pdf>.

²¹⁹ This is not a terrorism-related statute. In fact, DOJ's Civil Rights Division, prosecutes both criminal and civil cases involving the FACE Act. See <http://www.justice.gov/crt/about/crm/overview.php>; <http://www.justice.gov/crt/about/spl/face.php>. The FACE Act (18 U.S.C. §248), "protects the exercise of free choice in obtaining reproductive health services, and the exercise of First Amendment religious freedoms. Section 248 makes it unlawful for a person to use force, threat of force, or physical obstruction to intentionally injure or intimidate a person because he/she is or has been obtaining or providing reproductive health services. Section 248 also makes it unlawful for a person to use force, threat of force, or physical obstruction to intentionally injure or intimidate a person because he/she is lawfully exercising the right of religious freedom at a place of worship. Finally, Section 248 makes it unlawful for a person to intentionally damage or destroy the property of a facility because it provides reproductive health services, or because it is a place of worship. Section 248 also prohibits anyone from attempting to commit any of the above."

²²⁰ Ron Sylvester, "Scott Roeder Gets Hard 50 in Murder of Abortion Provider George Tiller," *Wichita Eagle*, April 1, 2010, <http://www.kansas.com/2010/04/01/1249310/roeder-to-be-sentenced-thursday.html>. Hereinafter: Sylvester, "Scott Roeder." Roeder reportedly also adhered to anti-government beliefs beginning in the 1990s. See Ron Sylvester, Abortion Issue Front and Center in Roeder Murder Trial," January 10, 2010, *Wichita Eagle*, <http://www.kansas.com/2010/01/10/1130385/abortion-issue-front-and-center.html#storylink=cpy>.

A number of other unrelated schemes targeting abortion clinics have been uncovered since Roeder's arrest. These incidents appear to involve individuals largely operating alone.

- In January 2012, Bobby Joe Rogers was charged in the firebombing of a Pensacola, FL, abortion clinic on New Year's Day 2012. The bombing destroyed the clinic, which had been targeted in the past.²²¹ In February 2012, a federal grand jury indicted him on two counts—arson and damaging a reproductive health facility.²²² He pled guilty to the charges in July 2012.²²³
- In May 2011, Ralph Lang was arrested after allegedly accidentally firing his handgun through the door of the hotel room in Madison, WI. He was reportedly planning to kill abortion providers in the area.²²⁴

One underground network that supports attacks on abortion clinics is the Army of God (AOG).²²⁵ The loosely structured organization openly promotes anti-abortion violence.²²⁶ However, its members deny that they are terrorists. They also deny that attacks against clinics and abortion providers constitute violent activity, because they see it as “Godly work.”²²⁷ AOG first made headlines with the 1982 kidnapping of a doctor and his wife, both of whom ran an abortion clinic in Illinois. Three individuals who claimed membership in AOG were responsible.²²⁸ The group disseminates a manual that “is a ‘how to’ for abortion clinic violence. It details methods for blockading entrances, attacking with butyric acid, arson, bomb making, and other illegal activities. The manual contains anti-abortion language as well as anti-government and anti-gay/lesbian language. The manual begins with a declaration of war on the abortion industry.”²²⁹

²²¹ “Man Indicted for Abortion Clinic Firebombing,” *Associated Press*, February 23, 2012.

²²² Department of Justice, press release, “Arson Indictment Returned Regarding American Family Planning Clinic,” February 23, 2012, <http://www.fbi.gov/jacksonville/press-releases/2012/arson-indictment-returned-regarding-american-family-planning-clinic>.

²²³ Department of Justice, “Man Pleads Guilty to Arson of Reproductive Health Facility in Pensacola,” July 19, 2012, <http://www.fbi.gov/jacksonville/press-releases/2012/man-pleads-guilty-to-arson-of-reproductive-health-facility-in-pensacola>.

²²⁴ Kevin Murphy, “Feds Mull Felony Charge for Suspect Ralph Lang of Marshfield in Abortion Clinic Shooting Plot,” *Marshfield News*, May 28, 2011; Department of Justice, press release, “Wisconsin Man Charged with FACE Act Violations,” May 26, 2011, <http://www.justice.gov/opa/pr/2011/May/11-crt-695.html>. For other examples of individuals involved in abortion-related violence, see Department of Justice, press release, “Man Pleads Guilty to Civil Rights Violation in Connection with Arson at Planned Parenthood and Vandalism of Mosque in Madera, California,” October 7, 2011, <http://www.justice.gov/opa/pr/2011/October/11-crt-1336.html>. Mower also threw a brick at a mosque in Madera. Ryan Seals, “Update: Concord Man Charged in Plot to Bomb Abortion Clinic,” *Greensboro News and Record*, September 9, 2010, http://www.news-record.com/content/2010/09/09/article/concord_man_charged_with_plotting_to_bomb_nc_abortion_clinic; “Man Guilty of Bombing Plot Gets 30 Months,” *Salisbury Post*, March 2, 2011, <http://www.salisburypost.com/news/030211-moose-sentencing-today-qcd>.

²²⁵ National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Terrorist Organization Profile: Army of God,” http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=28. Hereinafter: START, “Army of God.”

²²⁶ Mireille Jacobson and Heather Royer, “Aftershocks: The Impact of Clinic Violence on Abortion Services,” National Bureau of Economic Research, Working Paper No. 16603, (January 7, 2010), p. 6.

²²⁷ Jennifer Jefferis, *Armed for Life: The Army of God and Anti-Abortion Terror in the United States* (Santa Barbara, CA: Praeger, 2011), p. xvi. Hereinafter: Jefferis, *Armed for Life*.

²²⁸ *Ibid.*, p. 23. The victims were released unharmed after eight days of captivity. See, “Abortion Opposition Stressed in Kidnapping Trial in Illinois,” *New York Times*, January 26, 1983.

²²⁹ START, “Army of God.”

Eric Rudolph, who in the late 1990s bombed an abortion clinic near Atlanta, GA, and one in Birmingham, AL, “published his writings on the Army of God website.”²³⁰

Protected Activities vs. Terrorism—Divergent Perceptions of the ALF

The boundary between constitutionally protected legitimate protest and terrorist activity has received much attention in public discussions of domestic terrorism. As an example of this, the next several sections of this report explore such considerations regarding the ALF.

A Serious Domestic Concern or “Green Scare?”

U.S. law enforcement, some business groups, and some scientists—among others—have stressed that animal rights extremists (and eco-terrorists) are a security and law enforcement concern. In 2008, the FBI stated that animal rights extremists and eco-terrorists together posed a serious domestic terrorism threat for several reasons, including the number of crimes attributed to animal rights extremists and eco-terrorists (between 1,800 and 2,000 incidents accounting for more than \$110 million²³¹ in damages from 1979 to early 2009), the broad pool of victims (such as large pharmaceutical corporations, scientific laboratories, ski resorts, automobile dealerships, individual researchers, and lumber companies), and the movement’s rhetoric and destructive tactics.²³² In March 2012, the FBI suggested that the threat from eco-terrorists may be declining in recent years.²³³

As articulated by some scientific researchers, the monetary toll on legitimate businesses and laboratories in the United States exacted by animal rights and eco extremists is compounded by less tangible issues. For example, animal rights extremists and eco-terrorists have impacted the

²³⁰ Beau Seegmiller, “Radicalized Margins: Eric Rudolph and Religious Violence,” *Terrorism and Political Violence*, vol. 19, no. 4 (October 2007), p. 524. The 1998 bombing in Birmingham killed a police officer and injured a nurse. On May 31, 2003, Rudolph was arrested and charged with the clinic bombings, bombing the Centennial Olympic Park during the 1996 summer Olympic games in Atlanta (claiming one life), and attacking a gay club—Atlanta’s Otherside Lounge—in 1997. Rudolph admitted to the bombing spree in April 2005. He claimed that the 1996 attack at Centennial Olympic Park was intended to shame the U.S. government for what Rudolph saw as its support of abortion rights. See “Rudolph Pleads Guilty in Series of Bombings,” *Associated Press* at *MSNBC*, April 13, 2005, http://www.msnbc.msn.com/id/7486021/ns/us_news-crime_and_courts/t/rudolph-pleads-guilty-series-bombings/#.TwN9CUdO3y0; “Rudolph Agrees to Plea Agreement,” *CNN*, April 12, 2005, http://articles.cnn.com/2005-04-08/justice/rudolph.plea_1_emily-lyons-eric-robert-rudolph-atlanta-attacks?_s=PM:LAW.

²³¹ ELF claims that it has caused over \$150 million in damages, although the geographic range and timeframe for this figure are unknown. Earth Liberation Front.org, “What Is the Earth Liberation Front?” <http://www.earthliberationfront.org/elffaq.html>. Hereinafter: ELF, “What Is the Earth?” See also <http://www.animalliberationfront.com/ALFront/ELF/ELFPRESSOffice.htm>.

²³² There is some imprecision in the FBI’s public statements regarding the number of crimes committed by animal rights extremists and eco-terrorists. In April 2009, the FBI estimated that “to date [animal rights and eco-] extremists have been responsible for more than 1,800 criminal acts.” Ten months earlier, in June 2008, the FBI placed the number of criminal acts at “over 2,000 since 1979.” See Michael J. Heimbach, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, press conference, April 21, 2009, <http://www.fbi.gov/news/speeches/new-most-wanted-terrorist-announced>. Hereinafter: Heimbach, press conference. See also FBI, “Putting Intel.” The \$110 million figure remained the same in both publicly released documents.

²³³ Juliet Eilperin, “As Eco Terrorism Threat Wanes, Governments Keep Eyes on Activists,” *Washington Post*, March 11, 2012, http://www.washingtonpost.com/national/health-science/as-eco-terrorism-wanes-governments-still-target-activist-groups-seen-as-threat/2012/02/28/gIQA4A3R_story.html. Hereinafter: Eilperin, “As Eco Terrorism.”

work of scientists. In some cases, special equipment and research materials have been destroyed in attacks. The consequences of criminal activity in the name of movements such as the ALF can also be more personal. Two advocates of animal research conducted strictly according to federal regulations have noted that the actions of animal rights extremists have pushed some scientists to quit lab work involving animals. Often, this work relates to products and procedures that some maintain cannot feasibly be marketed without animal testing.²³⁴ In 2006, a UCLA professor of behavioral neuroscience declared he was stopping his research on monkeys because of what he described as harassment by animal rights groups.²³⁵ Additionally, animal rights extremists are said to be driving out students from research programs.²³⁶

Critics of U.S. efforts to fight animal rights extremism and eco-terrorism have suggested that the threat is overblown by law enforcement and that the government's pursuit of purported extremists perpetuates a "green scare," chilling the exercise of protected speech by protesters.²³⁷ Some say that the government conflates property crime with terrorism.²³⁸ Others add that people engaged in what the government describes as animal rights extremism or eco-terrorism do not deserve the terrorist label.

Animal Enterprise Terrorism Act (P.L. 109-374)

The Animal Enterprise Terrorism Act (P.L. 109-374; AETA) expanded the federal government's legal authority to combat animal rights extremists who engage in criminal activity. Signed into law in November 2006, it amended the 1992 Animal Enterprise Protection Act (P.L. 102-346; AEPA). Namely, the AETA

Amends the federal criminal code to revise criminal prohibitions against damaging or interfering with the operations of an animal enterprise to include intentional damage or loss to any real or personal property and intentional threats of death or serious bodily injury against individuals (or their family members, spouses, or intimate partners) who are involved with animal enterprises.²³⁹

The AETA expanded the AEPA to include both successful and attempted conspiracies. It also prohibits intentionally placing a person in "reasonable fear" of death or serious bodily injury while damaging or interfering in the operations of an animal enterprise. The AETA revised and

²³⁴ Conn and Parker, *The Animal*, pp. xii, xvi. See also 21 C.F.R. §314.610 (regarding approval based on evidence of effectiveness from studies in animals).

²³⁵ Samantha Henig, "UCLA Professor Halts Monkey Research," *Chronicle of Higher Education*, vol. 53, no. 2 (September 1, 2006), p. 21.

²³⁶ Michael Conn and James Parker, "Winners and Losers in the Animal Research Wars," *American Scientist*, vol. 96, no. 3 (May-June 2008), p. 184.

²³⁷ See Will Potter, *Green Is the New Red: An Insider's Account of a Social Movement Under Siege*, (San Francisco: City Lights Books, 2011), p. 61.

²³⁸ Coalition to Abolish the AETA, "AETA v. AEPA: A Side-by-Side Comparison," October 16, 2008, <http://abolishtheaeta.org/web/aeta-v-aepa-a-side-by-side-comparison/>; Center for Constitutional Rights, factsheet, "The Animal Enterprise Terrorism Act (AETA)," [http://ccrjustice.org/learn-more/faqs/factsheet%3A-animal-enterprise-terrorism-act-\(aeta\)](http://ccrjustice.org/learn-more/faqs/factsheet%3A-animal-enterprise-terrorism-act-(aeta)).

²³⁹ P.L. 109-374, CRS summary. Instead of damage and interference, the AEPA focused on the "physical disruption to the functioning of an animal enterprise." According to AETA, "animal enterprise" means: "(A) a commercial or academic enterprise that uses or sells animals or animal products for profit, food or fiber production, agriculture, education, research, or testing; (B) a zoo, aquarium, animal shelter, pet store, breeder, furrier, circus, or rodeo, or other lawful competitive animal event; or (C) any fair or similar event intended to advance agricultural arts or sciences."

increased monetary and criminal penalties. It also stipulates that it does not prohibit First Amendment-protected activity.

DOJ successfully prosecuted individuals on charges relating to animal enterprise terrorism for the first time under the AEPA in 2006 (the case had been built before the AETA had been signed into law).²⁴⁰ Six individuals were convicted for what DOJ described as “their roles in a campaign to terrorize officers, employees, and shareholders of HLS [Huntingdon Life Sciences, a research corporation that performs animal research and has U.K. and U.S. facilities].”²⁴¹ These individuals belonged to an animal rights campaign named Stop Huntingdon Animal Cruelty (SHAC)²⁴² and the entity SHAC USA, Inc. SHAC involves both legal protests and criminal activity against HLS.

Reportedly, the six incited threats, harassment, and vandalism and on this basis were convicted of violating the AEPA.²⁴³ DOJ has noted that SHAC’s stated mission was to work “outside the confines of the legal system.”²⁴⁴ DOJ proved in court that the group managed websites that encouraged others “to direct their intimidation, harassment, and violence against HLS and its targeted employees, as well as secondary targets—companies and employees who did business with HLS.”²⁴⁵

DOJ has also successfully applied the AETA. For example, on February 14, 2011, Scott DeMuth was sentenced to six months in prison on one count of misdemeanor conspiracy to commit animal enterprise terrorism. He was involved in a raid that released about 200 ferrets at a Minnesota farm in 2006. Activists had claimed the action in the name of the ALF.²⁴⁶ In another case, William James Viehl and Alex Hall were sentenced to 24 months and 21 months in prison, respectively,

²⁴⁰ Department of Justice, press release, “Three Militant Animal Rights Activists Sentenced to Between Four and Six Years in Prison,” September 21, 2006.

²⁴¹ *Ibid.* See also “The SHAC 7,” <http://www.shac7.com/case.htm>.

²⁴² An undercover British television report on the treatment of animals at a British company, Huntingdon Life Sciences (HLS), sparked the creation of Stop Huntingdon Animal Cruelty (SHAC) in the United Kingdom in 1999. Active in a number of countries around the world, including the United States, the campaign has tried to compel business and financial firms to cut ties to HLS. It has involved both legal protests and crime. John P. Martin, “Animal Rights and Wrongs,” *Newark Star-Ledger*, November 28, 2004; Anti-Defamation League, *Ecoterrorism*. For more on SHAC from a movement perspective, see “History of the Animal Liberation Front,” http://www.animalliberationfront.com/ALFront/Premise_History/ALF_History.htm. The SHAC campaign made its way to the United States in 2000. See Heimbach, press conference.

²⁴³ Four of the six were guilty of other charges related to the case as well. Department of Justice, “Militant Animal Rights Group, Six Members Convicted in Campaign to Terrorize Company, Employees, and Others,” March 2, 2006, http://www.justice.gov/usao/nj/press/files/shac0302_r.htm. Hereinafter: Department of Justice, “Militant Animal Rights.” Anti-Defamation League, “Animal Rights Group Sentenced for Inciting Violence and Stalking,” September 22, 2006, <http://www.adl.org/NR/exeres/7FBDB1FE-9176-4802-8704-54F8EAC3C215,18AA02A5-13A1-44F3-B4D4-6176E1ECC36C.frameless.htm>. Hereinafter: Anti-Defamation League, “Animal Rights Group.”

²⁴⁴ Department of Justice, *White Paper*, p. 60.

²⁴⁵ *Ibid.* The convictions in the case were upheld by a federal appeals court in 2009. See Lisa Coryell, “Convictions of Animal Rights Activists Upheld,” *Times of Trenton*, October 14, 2009, http://www.nj.com/mercer/index.ssf/2009/10/convictions_of_animal_rights_a.html. Subsequently, the U.S. Supreme Court refused to review the case. See Center for Constitutional Rights, “U.S. v. SHAC 7,” <http://ccrjustice.org/us-v-SHAC7>; Will Potter, “Supreme Court Will Not Hear SHAC 7 Case,” March 7, 2011, <http://www.greenisthenewred.com/blog/shac-7-supreme-court/4447/>.

²⁴⁶ Ryan J. Foley, “Minn. Man Gets 6 Months for Raid on Ferret Farm,” *Associated Press*, February 14, 2011. Jennifer Kotila, “Minneapolis Man To Be Sentenced for Releasing HL Ferrets He Thought Were Mink,” *Delano Herald Journal*, (Minnesota) December 20, 2010, <http://www.herald-journal.com/archives/2010/stories/latzig-ferrets-scott-demuth.html>.

under AETA. The duo had released 650 minks, destroyed breeding records, and vandalized structures at the McMullin Ranch in South Jordan, UT, in 2008.²⁴⁷

DOJ has experienced at least one setback in its application of the AETA. In February 2009, the FBI announced the arrests of what it described as “four animal rights extremists.” The four (two women, two men, all in their 20s) allegedly violated the AETA by using “force, violence, or threats to interfere with the operation of the University of California.”²⁴⁸ The incidents leading to the indictment included protests at the houses of researchers from the University of California, Berkeley and University of California, Santa Cruz. According to the FBI’s press release, in one instance, three of the indicted individuals tried to forcibly enter the home of a researcher, whose husband was hit by an object while confronting the protesters.²⁴⁹ In July 2010, a federal judge dismissed the indictment against the four. According to the ruling, the indictment failed to specifically describe crimes allegedly committed by the defendants.²⁵⁰ Opponents of the prosecution stress that the case involved over-broad application of AETA to First Amendment-protected behaviors.²⁵¹

Criticisms of federal government efforts to counter animal rights extremists have focused on the AETA itself and First Amendment-related issues. Opponents of the AETA suggest that it expanded the AEPA too much by making it easier to prosecute individuals who wage protest campaigns against secondary or tertiary targets—companies or people (such as insurers) indirectly tied to an animal enterprise.²⁵² Opponents also take issue with the inclusion of “reasonable fear” in the AETA, suggesting that protected speech or activities may possibly be interpreted as provoking “reasonable fear” in some instances. Echoing critiques of the AETA, one observer emphasizes that while activities linked to U.S.-based animal rights extremists have caused significant property damage, none of these criminal acts has physically harmed people. This critic suggests that describing vandalism or arson as *terrorism* and not ordinary *crime* dampens constitutionally protected protest activity by people who support animal rights or radical environmentalism but do not engage in criminal activity.²⁵³ In essence, this position argues that the U.S. government is encouraging a “green scare” by labeling the activity of movements such as the ALF and the ELF as terrorism or extremism.²⁵⁴ After serving 40 months in prison for her involvement with SHAC USA, Lauren Gazzola argued that she was not a terrorist, claiming, “I hadn’t hurt anyone or vandalized any property. In fact, the indictment didn’t allege that I’d

²⁴⁷ Dennis Romboy, “Man Who Raided South Jordan Mink Farm Sentenced,” *Deseret News*, July 1, 2010, <http://www.deseretnews.com/article/700044577/Man-who-raided-South-Jordan-mink-farm-sentenced.html>; Department of Justice, press release, “Viehl Pleads Guilty to Damaging, Interfering with Animal Enterprise in Connection with McMullin Mink Farm Incident,” September 3, 2009, <http://www.justice.gov/usao/ut/press/releases/viehl%20cop.pdf>.

²⁴⁸ Federal Bureau of Investigation, press release, “Four Extremists Arrested for Threats and Violence Against UC Researchers,” February 20, 2009, <http://sanfrancisco.fbi.gov/pressrel/pressrel09/sf022009.htm>.

²⁴⁹ *Ibid.*

²⁵⁰ “S.C. Animal Activists Won’t Face Charges,” *The Monterey County Herald*, July 14, 2010.

²⁵¹ Will Potter, “Breaking: AETA 4 Case Dismissed, But Re-Indictment Possible,” *GreenIsTheNewRed.com*, July 12, 2010, <http://www.greenisthenewred.com/blog/aeta-4-case-thrown-out-dismissed/3015/>; Bill Quigley and Rachel Meeropol, “Victory for Animal Rights Dissent,” *Huffington Post*, July 16, 2010, http://www.huffingtonpost.com/bill-quigley/victory-for-animal-rights_b_648852.html. Hereinafter: Quigley and Meeropol, “Victory for Animal.”

²⁵² The AETA makes it illegal to damage or interfere with the operations of an animal enterprise. Presumably this covers tertiary targets.

²⁵³ Will Potter, “The Green Scare,” *Vermont Law Review*, vol. 33, no. 4 (June 2009), pp. 672-673.

²⁵⁴ *Ibid.*; Quigley and Meeropol, “Victory for Animal.”

committed any independent crime at all, only that I'd 'conspired' to publish a website that advocated and reported on protest activity against a notorious animal testing lab in New Jersey."²⁵⁵

The U.S. Code's definition of "domestic terrorism" has been seen by some as potentially chilling to legitimate animal rights and environmental protest activities.²⁵⁶ As mentioned, the current delineation of domestic terrorism in the U.S. Code includes criminal acts "dangerous to human life" that appear to intend to intimidate or coerce a civilian population or influence governmental policy via intimidation or coercion. This line of reasoning suggests that the crimes committed by animal rights extremists and eco-terrorists cannot be compared to clearly violent attacks by groups such as Al Qaeda. An opposing commentary stresses that such discussion is irrelevant and

miss[es] the mark. The ALF ideology encourages members to instill fear in those who engage in the activities that the ALF opposes: fear of harm to themselves and their families, and fear of personal and professional economic loss. Additionally, these arguments assume that "true terrorism" is fundamentally different from animal rights terrorism. While it is true that animal rights terrorism, as a whole, does not engage in the same scale of violence as other extremist groups, those working in academia, research, agriculture, and food service industries are no less fearful when their homes and workplaces are firebombed; violent tactics can instill fear even when they are used infrequently.²⁵⁷

Assessing Domestic Terrorism's Significance

Domestic terrorist attacks have come nowhere near the devastation of 9/11. However, it is worth noting that (as mentioned above) Timothy McVeigh's bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, claimed 168 lives and injured more than 500 others. It ranks as the second-deadliest terrorist attack on U.S. soil, behind only the devastation wrought by Al Qaeda on 9/11. Domestic terrorists feature prominently among the concerns of some law enforcement officers. For example, Los Angeles Deputy Police Chief Michael P. Downing recently described violent Islamists such as Al Qaeda, Hezbollah, and Hamas as Los Angeles's main terrorist threats "along with three other terrorist categories: black separatists, white supremacist/sovereign citizen extremists, and animal rights terrorists."²⁵⁸ In one 2008 study, state police agencies "overwhelmingly reported" dangerous domestic extremist groups present in their jurisdictions.²⁵⁹ Of course, as one expert reminds us, most followers of extremist viewpoints

²⁵⁵ Lauren Gazzola, "Animal Rights Activists Like Me Aren't Terrorists," *EGP News*, January 12, 2012, <http://egpnews.com/?p=33714>.

²⁵⁶ American Civil Liberties Union, "How the USA PATRIOT Act Redefines 'Domestic Terrorism,'" December 6, 2002, <http://www.aclu.org/national-security/how-usa-patriot-act-redefines-domestic-terrorism>. For an additional view suggesting that the activities of movements such as the ALF and the ELF should not be treated as terrorism, see DeMond Shondell Miller, Jason David Rivera, and Joel C. Yelin, "Civil Liberties: The Line Dividing Environmental Protest and Ecoterrorists," *Journal for the Study of Radicalism*, vol. 2, no. 1 (2008), pp. 109-123.

²⁵⁷ Grubbs, "Saving Lives," pp. 364-365.

²⁵⁸ Bill Gertz, "L.A. Police Use Intel Networks Against Terror," *Washington Times*, April 11, 2011, <http://www.washingtontimes.com/news/2011/apr/11/la-police-use-intel-networks-against-terror/?page=all#pagebreak>.

²⁵⁹ "Far Right Domestic Terrorism on Par with Foreign Threat, Experts Say," CNN, July 25, 2011, <http://www.cnn.com/2011/US/07/25/domestic.extremism/>.

pose no threat: “Most of them are not going to do anything but bore their relatives and friends with ridiculous papers and treatises.”²⁶⁰

Five themes speak to the possible threat posed by domestic terrorists. First, domestic terrorists likely have been responsible numerous incidents since 9/11, and there appears to be growth in anti-government extremist activity as measured by watchdog groups in the last several years. Second, a large number of those labeled as domestic terrorists do not necessarily use major terrorist tactics such as bombings or airplane hijackings. Third, domestic terrorists—much like their violent jihadist analogues—are often Internet savvy and use the medium as a resource for their operations. Fourth, domestic terrorism can be seen as a somewhat decentralized threat often involving lone wolves and movements operating under the model of leaderless resistance. Finally, prison has been highlighted as an arena in which terrorist radicalization can occur, and WSE plays a role in the activities of several U.S. prison gangs. Sovereign citizen theories have also taken root in U.S. prisons.

Counting Incidents

There is no publicly-available list of domestic terrorist incidents (foiled plots or attacks) kept by the U.S. government. This makes it especially challenging for anyone trying to develop a sense of this particularly diverse threat.²⁶¹ However, a September 2011 study by the New America Foundation and Syracuse University’s Maxwell School of Public Policy found 114 individuals involved in non-jihadist terrorist acts in the 10 years following 9/11. The study did not limit its findings to animal rights extremists, eco-terrorists, anarchist extremists, sovereign citizens, unauthorized militias, black separatists, white supremacists, and anti-abortion extremists. It included incidents by what it described as left-wing and right-wing terrorists.²⁶²

Some U.S. government sources suggest levels of domestic terrorist activity. Examples of such sources include the following:

- An unclassified 2008 DHS report includes a table that lists *selected* criminal acts perpetrated by people involved in the animal rights extremist and eco-terrorist movements. This list counts 74 criminal acts between 9/11 and March 2008.²⁶³
- As noted, the FBI estimated that animal rights extremist and eco-terrorists together committed between 1,800 and 2,000 criminal incidents accounting for more than \$110 million in damages from 1979 to early 2009.²⁶⁴ In 2012, the FBI

²⁶⁰ Ibid.

²⁶¹ From 2004 to early 2012, the National Counterterrorism Center’s Worldwide Incidents Tracking System (WITS) publicly captured information on terrorist incidents (attacks) worldwide, including in the United States. It is no longer available. Prior to WITS, the FBI published regular reports of such activity. See <http://www.fbi.gov/stats-services/publications>.

²⁶² Peter Bergen et al. *Right- and Left-Wing Terrorism Since 9/11*, New America Foundation, September 10, 2011, <http://homegrown.newamerica.net/overview>. Hereinafter: Bergen et al. *Right- and Left-Wing*.

²⁶³ Department of Homeland Security, *Ecoterrorism: Environmental and Animal-Rights Militants in the United States*, Universal Adversary Dynamic Threat Assessment, May 7, 2008. Table 1 from the report is a “compilation of material from ALF and ELF communiqués and publications, media reports, and law enforcement” listing *selected* criminal acts perpetrated by the ALF and the ELF from 1984 to March 2008. Table 1 from the DHS report is not a comprehensive list of crimes tied to the ALF and the ELF. Hereinafter: Department of Homeland Security, *Ecoterrorism*.

²⁶⁴ Heimbach, press conference; Federal Bureau of Investigation, “Putting Intel.”

also publicly discussed a decline in eco-terrorism, especially after a wave of successful prosecutions in 2007. The bureau reportedly attributes the perceived dip to activists possibly viewing “a Democratic administration as more sympathetic to their goals and [thus] be less inclined to take radical steps.”²⁶⁵

- An unclassified FBI intelligence bulletin estimates that 53 acts of violence were committed by what it calls “white supremacist extremists” between 2007 and 2009 in the United States. Victims included other white supremacists, African Americans, and Latinos. Most of the incidents involved assaults. The bulletin bases these findings on law enforcement and media reporting.²⁶⁶
- In February 2012, the FBI announced that sovereign citizen convictions increased from 10 in 2009 to 18 in both 2010 and 2011.²⁶⁷

Domestic terrorists have been responsible for killing Americans.

- The study by the New America Foundation and Syracuse University’s Maxwell School of Public Policy counted “[a]t least 14 people ... killed in right- and left-wing terrorism-related incidents [in the 10 years since 9/11].”²⁶⁸
- On January 29, 2010, Scott Roeder was convicted of first-degree murder and two counts of aggravated assault for killing abortion provider George Tiller.²⁶⁹
- Described as a neo-Nazi and white supremacist, James von Brunn reportedly shot and killed a security guard at the U.S. Holocaust Memorial Museum in Washington, DC, in June 2009. In January 2010, the 89-year-old von Brunn died in federal prison, before he could be tried.²⁷⁰

Additionally, a key caveat regarding the violence involved in domestic terrorist activity may be of importance. Many domestic terrorist incidents have been linked to either animal rights extremists or eco-terrorists. As highlighted elsewhere in this report, many animal rights extremists and eco-terrorists claim to avoid violent acts that directly target people. The attacks by these individuals can often be described as property crimes involving arson or vandalism.

Growth in Hate Groups and Anti-Government Extremism

Beyond counting terrorist incidents, the Southern Poverty Law Center (SPLC)²⁷¹ has noted both a steady rise in the number of hate groups from 2000-2011 and a marked expansion in the militia

²⁶⁵ Eilperin, “As Eco Terrorism.”

²⁶⁶ Federal Bureau of Investigation, *White Supremacist Extremist Violence*, pp. 1-2. The FBI bulletin defines “acts of violence” to include “arson; assaults and murders; and acts designed to threaten or intimidate due to a person’s ethnicity, religious beliefs, or lifestyle.” See Federal Bureau of Investigation, *Rage and Racism* p. 5.

²⁶⁷ Patrick Temple-West, “Anti-Government Extremists Opposed to Taxes and Regulations Pose a Growing Threat to Local Law Enforcement Officers in the United States, the FBI Warned on Monday,” *Reuters*, February 6, 2012, <http://www.reuters.com/article/2012/02/07/us-usa-fbi-extremists-idUSTRE81600V20120207>.

²⁶⁸ Bergen et al. *Right- and Left-Wing*.

²⁶⁹ Sylvester, “Scott Roeder.”

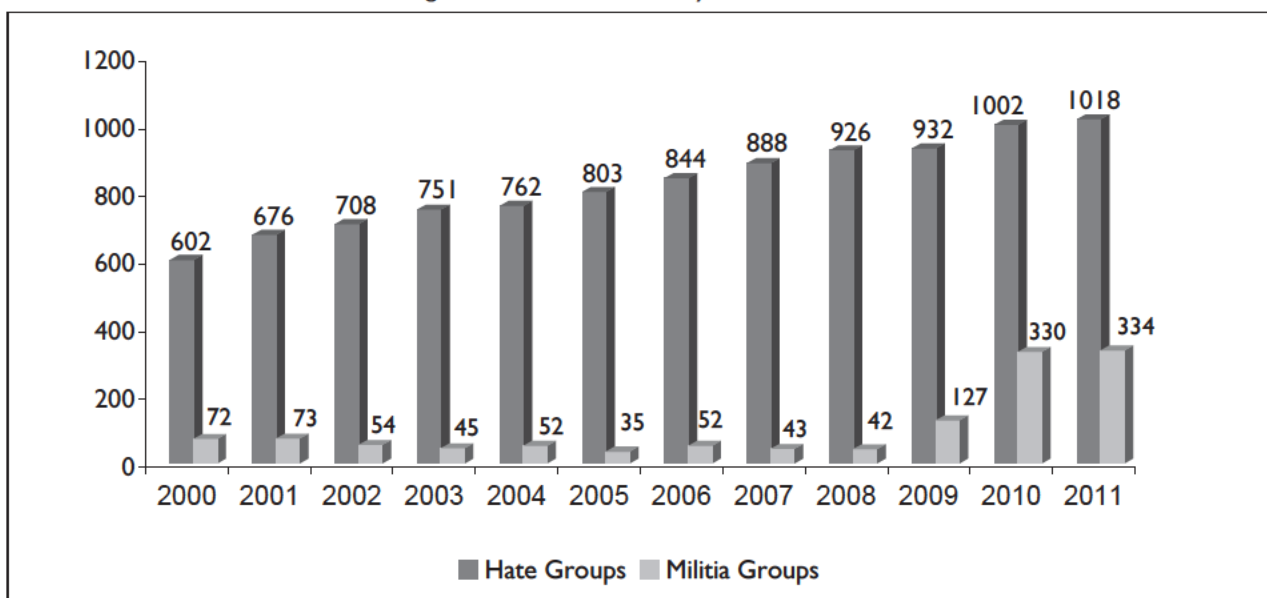
²⁷⁰ Anti-Defamation League, “James von Brunn: An ADL Backgrounder,” http://www.adl.org/main_Extremism/von_brunn_background.htm.

²⁷¹ The Southern Poverty Law Center has been criticized regarding its labeling of the Family Research Council, as a hate group for its opposition to gay rights. See Family Research Council, press release, “FRC, Members of Congress, (continued...) ”

movement (discussed elsewhere in this report) over the same period. Between 2009 and 2011, militia groups resurged to levels not seen since the 1990s.²⁷² The SPLC's figures likely capture a range of activity broader than that described by DOJ and the FBI as domestic terrorism. Regardless, the SPLC argues that the rise is "driven by resentment over the changing racial demographics of the country, frustration over the government's handling of the economy, and the mainstreaming of conspiracy theories and other demonizing propaganda aimed at various minorities."²⁷³ SPLC also assesses that 2010 was the first year ever that the number of hate groups topped 1,000 (Figure 1).

Figure 1. Hate Groups and Militia Groups, 2000-2010

According to the Southern Poverty Law Center



Source: Mark Potok, "The Year in Hate and Extremism," Southern Poverty Law Center, *Intelligence Report*, no. 145 (Spring 2012).

Notes: The Southern Poverty Law Center includes Ku Klux Klan, neo-Nazi, white nationalist, racist skinhead, Christian Identity, neo-Confederate, black separatist, and general hate groups in its hate group category. The organization goes on to elaborate that "Christian Identity describes a religion that is fundamentally racist and anti-Semitic. Black Separatist groups are organizations whose ideologies include tenets of racially based hatred. Neo-Confederate groups seek to revive many of the racist principles of the antebellum South. White Nationalist groups espouse white supremacy or white separatism but generally avoid anti-Semitism. General Hate groups espouse ideologies of hatred and include the sub-categories of Anti-Gay groups, Anti-Immigrant groups, Holocaust Denial groups, Racist Music labels, [and] Radical Traditionalist Catholic groups (which reject core Catholic teachings and espouse anti-Semitism)." The SPLC describes patriot groups and militias as anti-government, "engaging in groundless conspiracy theorizing or advocat[ing] or adher[ing] to extreme anti-

(...continued)

Governors, and Conservative Leaders Release Open Letter Calling for Civil Debate, End to Character Assassination," December 15, 2010, <http://www.frc.org/get.cfm?i=PR10L07&f=RF07B02>; Mark Potok, "SPLC Responds to Attack by FRC, Conservative Republicans," December 15, 2010, <http://www.splcenter.org/blog/2010/12/15/splc-responds-to-attack-by-frc-conservative-republicans/>; Sean Lengell, *Washington Times*, "Family Research Council Labeled a 'Hate Group,'" November 24, 2010, <http://www.washingtontimes.com/news/2010/nov/24/frc-labeled-a-hate-group/>.

²⁷² Ibid., p. 42.

²⁷³ Potok, "The Year," p. 41.

government doctrines.” The patriot or militia organizations counted by Southern Poverty Law Center do not necessarily “advocate or engage in violence or other criminal activities.” Neither are they necessarily racist.

“Non-Violent” Strategies

While some domestic terrorism suspects engage in violent plotting, others commit much different crimes that do not physically harm people. This latter group differs from their homegrown violent jihadist counterparts, who are often bent on killing or harming people. Two types of activities that avoid visiting violence upon people but are commonly associated with subjects of domestic terrorism investigations stand out. First, many animal rights extremists, eco-terrorists, and anarchist extremists believe in “direct action.” This typically involves what movement members would characterize as *non-violent but criminal* protest or resistance activities furthering the movement’s ideology. While direct action has a long legacy among anarchists, in recent years the ALF and the ELF have played a large role in articulating its meaning. Second, “paper terrorism” is a term used to describe some of the *non-violent* criminal activity committed by sovereign citizens involving the filing of fraudulent documents in the hopes of harassing enemies or bilking state or federal tax authorities.

Direct Action

Anarchist extremists, animal liberation extremists, and environmental extremists refer to much of their operational activity as “direct action.” This term has a long history, and it can be used to describe legitimate protest such as letter writing campaigns or work stoppages. However, this report uses “direct action” to describe criminal activities such as sabotage and arson.²⁷⁴

ALF and ELF members understand that criminality and direct action are one and the same. *The Animal Liberation Primer*, a movement resource, highlights criminality in the actions of supporters: “anyone working in the ALF is a criminal. You have to begin to think like a criminal.” ALF and ELF members also generally view direct action as nonviolent and heroic. Using politically charged language, the ALF allegedly styles itself along the lines of the Underground Railroad, freedom fighters in Nazi Germany, anti-Apartheid protestors, U.S. civil rights activists, and Palestinian groups opposing Israel.²⁷⁵ The ELF views constitutionally protected protest as “state sanctioned” and eschews such activity. The ELF, much like the ALF, also wraps itself in the mantle of reformers and describes itself as inheriting the spirit of Luddites, abolitionists, suffragists, and even the American revolutionary-era Boston Tea Party.²⁷⁶

²⁷⁴ According to the DOJ’s Office of the Inspector General, the FBI “generally” defines “direct action” as, “criminal activity designed to cause economic loss or to destroy property or operations.” See Department of Justice, Office of the Inspector General, Oversight and Review Division, *A Review of the FBI’s Investigations of Certain Domestic Advocacy Groups*, (September 2010), p. 97, <http://www.justice.gov/oig/special/s1009r.pdf>; Darren Thurston, *The ALF Primer*, n.d. p. 4. DOJ believes Thurston authored the *Primer*, although he is not attributed as an author in the document. Hereinafter: Thurston, *The ALF Primer*. See also *Guide to Direct Action*, 2010, http://www.animalliberationfront.com/ALFront/Activist%20Tips/Direct_Action-Guide.htm; Earth Liberation Front.org, “Earth Liberation Front Frequently Asked Questions,” Hereinafter: ELF, “FAQs.” See also http://www.animalliberationfront.com/ALFront/ELF/elf_faqs.pdf.

²⁷⁵ NAALPO, “History.”

²⁷⁶ ELF, “FAQs.”

The ALF: “Live Liberations” and “Economic Sabotage”

The ALF’s version of direct action is framed as what it considers to be “economic sabotage” or “ethical vandalism.” The ALF supports the destruction of property and intimidation of individuals and businesses considered by the movement to be involved in the exploitation of animals. Cells and individuals linked to the ALF also engage in trespassing and theft, or what they perceive as “live liberations” or “rescuing” animals from “the horrors of exploitation”²⁷⁷ and human use²⁷⁸ by stealing them from places such as legitimate research facilities or farms. Economic sabotage can be virtual. The North American Animal Liberation Press Office (NAALPO) has carried claims of cyber hacking incidents in the name of animal rights.²⁷⁹ NAALPO is one of the web-based vehicles used by ALF supporters to publicize criminal activities claimed on behalf of the movement.

The ELF: “Monkeywrenching”

Like the ALF, the ELF’s discussions of direct action also revolve around economic sabotage. The ELF rejects legal protest tactics partly for what it views as pragmatic reasons—“because they have been proven not to work, especially on their own.”²⁸⁰ Economic sabotage in the name of environmentalism has a long history, perhaps stretching back to the 1950s,²⁸¹ and has been called “monkeywrenching,” a term taken from a 1975 novel, *The Monkey Wrench Gang* by Edward Abbey. The book depicts such activity.²⁸² A guidebook that describes monkeywrenching offers what can be interpreted as a call to arms for would-be extremists:

It is time for women and men, individually and in small groups to act heroically in the defense of the wild, to put a monkeywrench into the gears of the machine that is destroying natural diversity. Though illegal, this strategic monkeywrenching can be safe, easy, and—most important—effective.²⁸³

The guidebook also defines monkeywrenching as nonviolent by stressing that it should never target people or “other forms of life.”²⁸⁴

Arson and Explosive Devices

Federal officials are especially concerned about the use of incendiary devices and explosives by animal rights extremists and eco-terrorists. In congressional testimony from 2005, then-ATF

²⁷⁷ NAALPO, “History.” A section of *The ALF Primer* describes both economic sabotage and live liberation as legitimate strategies. See Thurston, *The ALF Primer*, p. 2.

²⁷⁸ Conn and Parker, *The Animal*, p. xvii.

²⁷⁹ Communiqué, July 13, 2007, http://www.animalliberationpressoffice.org/communiques/2007/2007-07-13_lagrange_hls.htm.

²⁸⁰ ELF, “FAQs.”

²⁸¹ Bron Taylor, “The Tributaries of Radical Environmentalism,” *Journal for the Study of Radicalism*, vol. 2, no. 1 (2008), p. 45.

²⁸² Edward Abbey, *The Monkey Wrench Gang*, 3rd ed. (Salt Lake City, UT: Dream Garden Press, 1985).

²⁸³ Dave Foreman, “Strategic Monkeywrenching,” in *Ecodefense: A Field Guide to Monkeywrenching*, ed. Dave Foreman and Bill Haywood, 3rd ed. (Chico, CA: Abzug Press, 1993), p. 8. Hereinafter: Foreman, “Strategic Monkeywrenching.” Foreman was a founder of Earth First! See Anti-Defamation League, *Ecoterrorism*.

²⁸⁴ Dave Foreman, “Strategic Monkeywrenching,” p. 9.

Deputy Assistant Director Carson Carroll stated that the “most worrisome” trend regarding animal rights extremists and eco-terrorists was their “willingness to resort to incendiary and explosive devices.”²⁸⁵

This pronouncement came on the heels of two related incidents that occurred near San Francisco, CA, and involved explosive devices. An entity called the Revolutionary Cells of the Animal Liberation Brigade claimed responsibility for both attacks, which the FBI has also linked to a man named Daniel San Diego. In August 2003, two ammonium nitrate pipe bombs exploded at the campus of the biotechnology firm Chiron but caused little damage and no injuries. In October 2003, a reputed 10-pound ammonium nitrate bomb damaged the offices of Shaklee, a health, beauty, and household product company. No one was injured. The perpetrator(s) believed that both companies did business with Huntingdon Life Sciences (the same firm targeted by SHAC and discussed above). A related communiqué stressed that, “all customers and their families are considered legitimate targets.”²⁸⁶

One commentator has suggested that the combination of “fire” as a tactic and instilling “fear” as a goal ensures eco-terrorists will continue to warrant the terrorist label.²⁸⁷ Both animal rights extremists and eco-terrorists have histories of using incendiary devices to damage or destroy property—the Vail, CO, fire (mentioned elsewhere in this report) setting a prominent example for extremists. In fact, one of the hallmark publications circulated in extremist circles is a handbook on how to fashion incendiary devices titled *Arson Around with Auntie ALF*.²⁸⁸ A recent example underscores this focus on arson.

- In January 2012, NAALPO issued a communiqué in which “unnamed activists” claimed responsibility for setting fires that damaged 14 tractor trailer rigs at the Harris Ranch, a cattle feedlot in Coalinga, CA. The perpetrators used containers of accelerant, kerosene-soaked rope, and digital timers to set the blazes. According to the communiqué, the fires apparently embodied a reaction to “the horrors and injustices of factory farming”²⁸⁹

²⁸⁵ Statement of Carson Carroll, p. 43.

²⁸⁶ Stacy Finz, “Militants Say They Planted Shaklee Bomb,” *San Francisco Chronicle*, October 1, 2003, http://articles.sfgate.com/2003-10-01/bay-area/17512148_1_pipe-bombs-shaklee-chiron; Stacy Finz, Bernadette Tansey, “2 Bombs Shatter Biotech Firm’s Windows,” August 29, 2003, <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/08/29/MN173487.DTL&type=printable>. The FBI assessed that the devices may have been intended to harm people. The second Chiron bomb was timed to explode after the first, “an apparent strike at first responders,” while the Shaklee bomb was wrapped in nails, “to significantly increase its lethality to anyone in the area at the time of the detonation.” See U.S. Congress, Senate Committee on Environment and Public Works, “Statement of John E. Lewis, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation,” *Eco-Terrorism Specifically Examining Stop Huntingdon Animal Cruelty (“SHAC”)*, 109th Cong., 1st sess., October 26, 2005, 109-1005 (Washington: GPO, 2008), p. 7. In April 2009, the FBI placed Daniel San Diego on its Most Wanted Terrorists List for his involvement in the bombings. See Heimbach, press conference. The Bureau also tied him to SHAC. He had slipped away from FBI surveillance in October 2003. See Federal Bureau of Investigation, “New Most Wanted Terrorist,” April 21, 2009, http://www.fbi.gov/wanted/wanted_terrorists/daniel-andreas-san-diego. Hereinafter: FBI, “New Most Wanted”; “Daniel Andreas San Diego,” *America’s Most Wanted*, <http://www.amw.com/fugitives/case.cfm?id=25800>.

²⁸⁷ Grubbs, “Saving Lives,” p. 370.

²⁸⁸ Auntie ALF, Uncle ELF, and the Anti-Copyright Gang, *Arson-Around with Auntie ALF: Your Guide for Putting the Heat on Animal Abusers Everywhere*, 2001. Hereinafter: *Arson-Around*.

²⁸⁹ See http://www.animal liberationpressoffice.org/communiques/2012/2012-01-10_harrisranch.htm; Henry K. Lee, “14 Cattle Trucks Burned in Arson at Harris Ranch,” *San Francisco Chronicle*, January 11, 2012; <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/01/10/BABM1MN8BU.DTL>. For other examples, see Peter Young, “Fire and Explosions Rock Oregon Mink Farm,” July 28, 2010, <http://www.animal liberationpressoffice.org/> (continued...)

Some ELF adherents have focused on targets they perceive as emblematic of urban sprawl²⁹⁰ or the excesses of industrialized society. Since 2000, a number of ELF actions have involved the torching of housing projects as well as activities such as the damaging and destruction of sports utility vehicles and other emblems of industrialized society and urban sprawl.²⁹¹ Between August and October 2002, three individuals tied to the ELF damaged construction vehicles and sports utility vehicles, and vandalized fast food restaurants in Virginia. In one incident, these individuals vandalized two homes under construction, spray painting “sprawl” on one of the structures. In November 2005, the ELF claimed responsibility for fires set in five townhomes under construction in Hagerstown, MD.²⁹² Similar activity has occurred on the West Coast.²⁹³

Guidelines

Both the ALF and the ELF have established guidelines and posted them on the web for cells or lone wolves to follow. The guidelines are straightforward and short for both movements (see **Figure 2**). A key point in the guidelines for both the ALF and the ELF is to avoid harming any animal, human and non-human.²⁹⁴ The ALF’s guidelines also stipulate that individuals professing affiliation with the movement must be vegetarians or vegans.

Interestingly, the ALF employs a number of caveats in its understanding of violence. On the one hand, it supports intimidation as a tactic. On the other, the movement does not see intimidation as potentially involving violence.²⁹⁵ The ALF also views arson as “violence against property,” not people.²⁹⁶ Beyond this, ALF does not greatly elaborate on its notion of violence.

(...continued)

press_releases/2010/pr_2010_07_27_astoriafarm.htm; J.M. Brown, “A Year after Firebombings, No Arrests, Though Awareness Remains among Scientists,” *Santa Cruz Sentinel*, August 2, 2009; John Coté, “Firebombings Suggest New Tactic for Animal Activists,” *San Francisco Chronicle*, August 5, 2008; Shanna McCord, “FBI to Take Over Santa Cruz Firebombs Case,” *Monterey County Herald*, August 4, 2008; Anti-Defamation League, “‘Justice Department’ Claims Responsibility for Threats against UCLA Animal Researcher,” December 3, 2010, http://www.adl.org/learn/extremism_in_america_updates/movements/ecoterrorism/justice_department_ucla.htm. Hereinafter: Anti-Defamation League, “Justice Department.”

²⁹⁰ Brad Knickerbocker, “Firebrands of ‘Ecoterrorism’ Set Sights on Urban Sprawl,” *Christian Science Monitor*, August 6, 2003, <http://www.csmonitor.com/2003/0806/p01s02-ussc.html>. Hereinafter: Knickerbocker, “Firebrands.”

²⁹¹ Anti-Defamation League, “Radical Environmentalist Group Suspected in San Diego Arson,” August 8, 2003, http://www.adl.org/learn/news/San_Diego_Arson.asp; Knickerbocker, “Firebrands”; Chris Dixon, “Arrest in Vandalism of S.U.V.s,” *New York Times*, <http://www.nytimes.com/2004/03/10/us/national-briefing-west-california-arrest-in-vandalism-of-suv-s.html?ref=earthliberationfront>.

²⁹² Federal Bureau of Investigation, *Terrorism 2002-2005*, http://209.235.0.153/publications/terrorism/terrorism2002_2005.htm.

²⁹³ “Activists Topple Towers, Claim Dangers of AM Radio Waves,” *CNN.com*, September 4, 2009, http://articles.cnn.com/2009-09-04/justice/washington.towers.terrorism_1_elf-radio-station-radio-waves?_s=PM:CRIME; “Officials: No Explosive Devices Found at Scene of Seattle-Area House Fires,” *Fox News*, March 4, 2008, <http://www.foxnews.com/story/0,2933,334875,00.html>; Debera Carlton Harrell, Aubrey Cohen, and Paul Shukovsky, “‘Street of Dreams’ Houses Torched; Eco-Terrorists Suspected,” *Seattle Post-Intelligencer*, March 4, 2008; “Camano Island Mansion Fire Ruled Ecoterrorist Arson,” *KOMO News.Com*, January 20, 2006, <http://www.komonews.com/news/archive/4175026.html>.

²⁹⁴ For ALF guidelines, see <http://www.animalliberationpressoffice.org/Background.htm>. For ELF guidelines, see http://www.animalliberationfront.com/ALFront/ELF/elf_faq.pdf.

²⁹⁵ *Ibid.*

²⁹⁶ See North American Animal Liberation Front, “Frequently Asked Questions About the North American Animal Liberation Press Office,” <http://www.animalliberationpressoffice.org/faq.htm#7>.

Figure 2. ALF and ELF Guidelines

Animal Liberation Front	Environmental Liberation Front
<p>To Liberate animals from places of abuse, i.e. laboratories, factory farms, fur farms, etc., and place them in good homes where they may live out their natural lives, free from suffering.</p> <p>To inflict economic damage to those who profit from the misery and exploitation of animals.</p> <p>To reveal the horror and atrocities committed against animals behind locked doors, by performing direct actions and liberations.</p> <p>To take all necessary precautions against harming any animal, human and non-human.</p> <p>Any group of people who are vegetarians or vegans and who carry out actions according to these guidelines have the right to regard themselves as part of the Animal Liberation Front.</p>	<p>To cause as much economic damage as possible to a given entity that is profiting off the destruction of the natural environment and life for selfish greed and profit,</p> <p>To educate the public on the atrocities committed against the environment and life,</p> <p>To take all necessary precautions against harming life.</p>

Source: CRS graphic based on ALF and ELF guidelines.

Notes: For ALF guidelines, see <http://www.animalliberationpressoffice.org/Background.htm>. For ELF guidelines, see http://www.animalliberationfront.com/ALFront/ELF/elf_fa.pdf

Exceptions

Some animal rights extremists support violence. For example, in February 2012 Meredith Lowell was arrested for allegedly using a Facebook page she created (under an assumed name) to solicit a hit man to kill “someone who is wearing fur.”²⁹⁷ In the investigation, the FBI used an undercover employee to pose as a hit man and communicate with Lowell online. She was arrested before anyone could be harmed.²⁹⁸

An animal rights extremist entity named the “Justice Department” believes in the efficacy of violence against humans.²⁹⁹ Founded in the United Kingdom in 1993, the “Justice Department” has been described as an offshoot of the ALF.³⁰⁰ In 1999, the first incident claimed in its name on U.S. soil involved the mailing of more than 80 envelopes containing razor blades allegedly positioned to cut recipients. Some of the razors may have been covered in rat poison. The letters were received by animal researchers, hunting guides, and others in the United States and Canada.³⁰¹ In November 2010, individuals asserting ties to the “Justice Department” mailed two communiqués to NAALPO. The missives claimed that “Justice Department” extremists had

²⁹⁷ James Ewinger, “Cleveland Heights Woman Charged with Using Facebook to Hire Killer,” *Cleveland Plain Dealer*, February 21, 2012, http://blog.cleveland.com/metro/2012/02/heights_woman_charged_with_usi.html.

²⁹⁸ Ibid.

²⁹⁹ North American Animal Liberation Press Office, press release, “Liberationist Group ‘Justice Department’ Increasingly Vocal on Animal Abuse,” November 23, 2010, http://www.animalliberationpressoffice.org/press_releases/2010/pr_2010_11_23_jd.htm. Hereinafter: NAALPO, “Liberationist Group.”

³⁰⁰ Anti-Defamation League, “Justice Department.”

³⁰¹ Ibid.; Southern Poverty Law Center, “Eco-Violence: The Record,” *Intelligence Report*, Southern Poverty Law Center, no. 107 (Fall 2002), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2002/fall/from-push-to-shove/eco-violence-the-rec>.

mailed AIDS-tainted razors to two scientists at the University of California, Los Angeles.³⁰² One of the communiqués read:

We are the past generation of animal liberationists, but we will now be the future, striking at the heart of the vivisection industry, and if we have to go back to egg timers and incense [sic] sticks then we will. Mark our words, we will destroy all who fall into our focus.³⁰³

Presumably, allusion to egg timers and incense sticks suggests timing devices and fuses for explosive or incendiary devices.³⁰⁴

“Paper Terrorism”: Liens, Frivolous Lawsuits, and Tax Schemes

Sovereign citizens have committed non-violent crimes based on their ideological underpinnings.³⁰⁵ These are often bundled under the concept of “paper terrorism.”³⁰⁶ This concept can include forging documents (fake money orders and bad personal checks, for example), failing to pay taxes, phony tax filings, and presenting sham legal arguments in court. Sovereign citizens have filed fraudulent property liens against their foes.³⁰⁷ Some sovereigns hold illegal courts and target officials with fake criminal indictments. They can also “issue warrants for judges and police officers.”³⁰⁸

Retaliatory Filings

While these acts may not be violent, they are frequently “designed to intimidate or defraud targeted individuals, private institutions, or government entities.”³⁰⁹ Thus, some sovereigns saddle their opponents with time-consuming legal efforts to wipe out sham retaliatory court filings. As a

³⁰² NAALPO, “Liberationist Group.”

³⁰³ Ibid.

³⁰⁴ *Arson-Around*, pp. 16-17 describes assembly of an incendiary device incorporating incense sticks as a fuse. Incense sticks have been used as fuses for incendiary devices by ELF and ALF activists. See Federal Bureau of Investigation, *Terrorism 2000-2001*, 2004, p. 4, <http://www.fbi.gov/stats-services/publications/terror/terrorism-2000-2001> for an example of an ELF incident. For additional examples involving the cell known as “The Family” active with both the ALF and the ELF, see *U.S. v. Dibee et al.* Kitchen timers are discussed in William Rodgers and Stanislas Meyerhoff, *Setting Fires with Electrical Timers: An Earth Liberation Front Guide*, May 2001, pp. 15-17. Although the document lists no authors, DOJ believes that Rodgers and Meyerhoff wrote it. They were members of “The Family” which also used kitchen timers in its incendiary devices. See *United States v. Joseph Dibee et. al*, Indictment, CR 06-60011-AA, District Court, District of Oregon, January 19, 2006.

³⁰⁵ Department of Homeland Security and the Federal Bureau of Investigation, *Sovereign Citizen Group Calls for Removal of U.S. Governors*, March 29, 2010, p. 2. Hereinafter: “*Sovereign Citizen Group Calls*.”

³⁰⁶ For an example of the use of this oft-used term, see Department of Justice, press release, “Member of Anti-Government Movement Pleads Guilty to Laundering Money for FBI Undercover Agents,” March 25, 2011, <http://www.fbi.gov/lasvegas/press-releases/2011/lv032511.htm>.

³⁰⁷ One source has defined a lien as “a claim encumbrance or charge on property for payment of a debt or obligation.” Liens can be consensual or nonconsensual. They can be statutory or derive from common law. An example of a nonconsensual common law lien is “when a mechanic refuses to return a car until repairs are paid for.” See Robert Chamberlain and Donald P. Haider-Markel, “‘Lien on Me’: State Policy Innovation in Response to Paper Terrorism,” *Political Research Quarterly*, vol. 58, no. 3 (September 2005), p. 450.

³⁰⁸ Ibid.; Federal Bureau of Investigation, “Sovereign Citizen.” See also Christopher A. Young, “Minnesota Has New Weapons in the Fight Against ‘Paper Terrorism,’” *Hennepin Lawyer*, August 28, 2007, <http://hennepin.timberlakepublishing.com/article.asp?article=1148>.

³⁰⁹ “*Sovereign Citizen Group Calls*,” p. 2.

result, sovereign foes incur court fees and their credit ratings potentially suffer. In some cases, these proceedings arise from what most citizens might consider fairly mundane run-ins with law enforcement authorities. Some sovereigns do not necessarily see violations like parking tickets and trespassing arrests as run-of-the-mill. They can react to such encounters with police by challenging the very authority and jurisdiction of U.S. law enforcement and by harassing officials with dubious liens, for example.

- In November 2011, Kenneth W. Leaming, from Spanaway, WA, was arrested for allegedly issuing billions of dollars in frivolous liens to intimidate public officials enforcing laws against sovereign citizens. Reportedly, he had been tied to other sovereign citizen adherents and groups. Also, he purportedly planned to harass the children of U.S. Supreme Court Chief Justice John Roberts.³¹⁰

Redemption

Sovereign citizen guru Roger Elvick is the reputed founder of “redemption,”³¹¹ a concept that blurs the line between sovereign citizen ideology and pure scam. Redemption suggests that when the United States left the gold standard during the Great Depression, the nation found a way to monetize people. According to the theory, each child who is born in the United States and has a birth certificate also has a U.S. Treasury account “valued from \$630,000 to more than \$3 million”³¹² viewed as collateral against the nation’s debts. Redemption supporters hold that by filing certain forms with state or federal authorities, people can draw money from these accounts. To do so, they occasionally attempt to pass bogus checks.³¹³

On a broad level, redemption can be viewed as an ideologically driven tactic meant to illegally wrangle money from the U.S. government via the IRS. According to DOJ, in some instances this involves the filing of “a series of false IRS forms, including tax returns, amended returns, and

³¹⁰ Levi Pulkkinen, “FBI: Spanaway ‘Sovereign Citizen’ Planned to Track Down Justice’s Children,” *Seattle Post-Intelligencer*, November 28, 2011, <http://www.seattlepi.com/local/article/FBI-Spanaway-sovereign-citizen-planned-to-2299295.php>; Anti-Defamation League, “Little Shell Pembina Band,” http://www.adl.org/learn/ext_us/little_shell.asp?learn_cat=extremism&learn_subcat=extremism_in_america&xpicked=3&item=little_shell. For other examples, see Rick Montgomery, “Sovereign Citizens: Crackpots, Crooks, or Defenders of Liberty?” *Kansas City Star*, November 26, 2011, <http://www.kansascity.com/2011/11/26/3288115/sovereign-citizens-bulldogs-guarding.html>.

³¹⁰ Marnie Eisenstadt, “Fringe Group Terrorizes Small-Town Officials with False Liens,” *The Post Standard*, May 23, 2011; Rick Montgomery, “Sovereign Citizens: Crackpots, Crooks, or Defenders of Liberty?” *Kansas City Star*, November 26, 2011, <http://www.kansascity.com/2011/11/26/3288115/sovereign-citizens-bulldogs-guarding.html>; Marnie Eisenstadt, “Fringe Group Terrorizes Small-Town Officials with False Liens,” *The Post Standard*, May 23, 2011; “Two Admit Scheme to Defraud Public Employees,” *Daily Freeman*, January 14, 2011, <http://www.dailyfreeman.com/articles/2011/01/14/blotter/doc4d2fb54d3189f270459164.txt>; Michael Virtanen, “NY Man’s Sentencing Put Off in Liens Case,” *Associated Press*, July 12, 2011.

³¹¹ “His ‘Straw Man’ Free, a Scammer Finds the Rest of Him Isn’t,” *Intelligence Report*, Southern Poverty Law Center, Issue 118, (Summer 2005), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2005/summer/patriots-for-profit>. Hereinafter: Southern Poverty Law Center, “His Straw Man Free.”

³¹² FBI Counterterrorism Analysis Section, “Sovereign Citizens.”

³¹³ Elvick promoted his ideas in the 1980s, and was jailed for much of the 1990s as well as in the next decade because of passing bad checks, forgery, extortion, and corruption. See *Ibid.*; Southern Poverty Law Center, “His Straw Man Free”; For a description of redemption, see Institute for Intergovernmental Research, *Investigating Terrorism*, pp. 70-71.

Forms 1099 (including Form 1099-OID) or Forms W-2, to request fraudulent tax refunds based on phony claims of large income tax withholding.”³¹⁴

In addition, DOJ describes some redemption adherents as scammers who dupe customers into filing false IRS forms to redeem money via the purported secret accounts the government holds for its citizens.³¹⁵ One guru recently pled guilty to money laundering charges.³¹⁶ In another case, in December 2009 Audie Watson received a 14-year prison sentence for his involvement in an immigration benefit fraud scheme that sold membership in the Pembina Nation Little Shell Band to illegal aliens. Watson and co-conspirators charged individuals \$1,500 and couples \$2,000. They conned clients into believing that membership could be used to avoid removal from the United States.³¹⁷

- In March 2011, DOJ announced that the U.S. District Court for the Western District of Missouri had permanently barred Gerald A Poynter “from preparing tax returns for others and from promoting” a redemption scam.³¹⁸ Poynter informed his customers that he could obtain tax refunds for them, charged them for his services, and then produced fraudulent IRS forms claiming \$64 million in refunds for 165 customers.³¹⁹

The Internet and Domestic Terrorists

In the counterterrorism world, there has been much concern regarding violent jihadist use of the Internet.³²⁰ However, domestic terrorists also are computer savvy and active online. One count suggested that 657 U.S.-based hate websites existed in 2010.³²¹ A web presence may help extremist groups—sometimes relatively small, with rosters in the 100s or fewer—educate their

³¹⁴ Department of Justice, press release, “Government Files Seven Lawsuits Nationwide to Block Alleged Scheme Involving Fraudulent Tax-Refund Claims,” October 28, 2009, <http://www.justice.gov/opa/pr/2009/October/09-tax-1161.html>.

³¹⁵ Ibid.

³¹⁶ Carri Greer Thevenot, “Idaho Man Pleads Guilty to Money Laundering,” *Las Vegas Review-Journal*, March 25, 2011, <http://www.lvrj.com/news/sovereign-movement-leader-pleads-guilty-to-money-laundering-118685369.html>.

³¹⁷ Immigration and Customs Enforcement, press release, “South Florida Man Sentenced to 14 Years in Prison for Immigration Fraud,” December 8, 2009, <http://www.ice.gov/news/releases/0912/091208miami.htm>.

³¹⁸ Department of Justice, press release, “Federal Court Shuts Down Missouri Tax Preparer Who Promoted Tax Scam,” March 28, 2011, <http://www.justice.gov/tax/txdv11382.htm>. For the injunction, see http://www.justice.gov/tax/Poynter_Injunction.pdf.

³¹⁹ Ibid.

³²⁰ For example, see Edna Erez, Gabriel Weimann, and A. Aaron Weisburd, “Jihad, Crime, and the Internet: Content Analysis of Jihadist Forum Discussions,” October 31, 2011, Report submitted to the National Institute of Justice in fulfillment of requirements for Award Number 2006-IJ-CX-0038; Akil N. Awan, “The Virtual Jihad: An Increasingly Legitimate Form of Warfare,” *CTC Sentinel*, vol. 3, no. 5 (May 2010), p. 11, <http://www.ctc.usma.edu/sentinel/CTCSentinel-Vol3Iss5.pdf>; Gilbert Ramsay, “Relocating the Virtual War,” *Defence Against Terrorism Review*, vol. 2, no. 1 (Spring 2009), p. 34, http://www.tmmm.tsk.tr/publications/datr3/03_Gilbert%20Ramsay.pdf; Tim Stevens, “Regulating the ‘Dark Web’: How a Two-Fold Approach Can Tackle Peer-to-Peer Radicalisation,” *The RUSI Journal*, vol. 154, no. 2 (April 2009), p. 29; Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenge* (Washington, DC: United States Institute of Peace Press, 2006); Maura Conway, “Terrorism and Mass Communication: Nitro to the Net,” *The World Today*, vol. 60, no. 8/9 (Aug/Sep 2004), pp. 19-22, http://doras.dcu.ie/513/1/nitro_to_net_2004.pdf.

³²¹ Potok, “The Year,” p. 50. This count included web pages “from Ku Klux Klan, Neo-Nazi, White Nationalist, Racist Skinhead, Christian Identity, Neo-Confederate, Black Separatist, and General Hate groups.”

existing membership and forge a group identity. Also, in many instances they can use websites to focus on outsiders to propagandize, socialize, and recruit new adherents.³²² A few domestic terrorists also have exploited the web to harm their targets.

White supremacists have long been using computer technology to communicate and interact. As one study has suggested, white supremacists “were among the very early users of the electronic communication network that eventually evolved into the Internet.”³²³ Among a variety of findings, the study indicated that white supremacist extremist websites were possibly an effective recruiting tool that the groups exploited. Membership forms are available on some sites. Others exhibit multimedia material, and some actually retail items such as music and video games.³²⁴ The Internet allows individuals and groups to connect with one another and to disseminate ideology.³²⁵ It also enables groups to manage how others perceive them. Many white supremacist sites claim that their sponsoring groups are non-violent and not even racist.³²⁶

Some white supremacists may be unwilling to affirm their views in public spaces such as work, school, or in street demonstrations. To them, the virtual realm is an important antidote. As one study has suggested, “free spaces” in both the real and virtual worlds—where conflict with non-believers will be minimized—are important for adherents. In them they can “meet, articulate, and support their views.”³²⁷ Supremacists can turn to virtual free spaces to receive indoctrination into movement culture, key narratives outlining movement grievances, adopt ideologies, and “talk of violence against ‘racial enemies.’”³²⁸

Much of this online ideological activity involves constitutionally protected speech. A number of examples stand out.

- The ALF and the ELF have their long-established guidelines posted on the web for independent groups or individuals to follow.³²⁹ Movement websites virtually connect like-minded individuals. As mentioned elsewhere in this report, key ideological texts are also made available online.³³⁰ The websites of animal rights extremists and eco-terrorists also post press releases publicizing crimes perpetrated on behalf of the movements.³³¹

³²² Jeffrey Kaplan, Leonard Weinberg, and Ted Oleson, “Dreams and Realities in Cyberspace: White Aryan Resistance and the World Church of the Creator,” *Patterns of Prejudice*, vol. 37, no. 2 (2003), pp. 149-150.

³²³ Phyllis B. Gerstenfeld, Diana R. Grant, Chau-Pu Chiang, “Hate Online: A Content Analysis of Extremist Internet Sites,” *Analysis of Social Issues and Public Policy*, vol. 3, no. 1, (2003), p. 29. Hereinafter: Gerstenfeld et. al., “Hate Online.”

³²⁴ Ibid.

³²⁵ See Josh Adams and Vincent J. Roscigno, “White Supremacists, Oppositional Culture, and the World Wide Web,” *Social Forces*, vol. 84, no. 2 (December 2005), pp. 759-778.

³²⁶ Gerstenfeld et. al., “Hate Online,” pp. 33-41.

³²⁷ Pete Simi, Robert Futrell, “Cyberculture and the Endurance of White Power Activism,” *Journal of Political and Military Sociology*, vol. 34, no. 1 (Summer 2006), p. 117. Hereinafter: Simi and Futrell, “Endurance.”

³²⁸ Ibid., 122-126, 131. Some free spaces exist in the real world. Examples include the privacy of the home, supremacist events such as conferences, isolated compounds or communities, and ideologically-focused musical concerts.

³²⁹ See <http://www.animalliberationpressoffice.org/Background.htm>; ELF, “What Is the Earth?”

³³⁰ Anti-Defamation League, *Ecoterrorism: Extremism in the Animal Rights and Environmentalist Movements*, http://www.adl.org/learn/ext_us/ecoterrorism.asp. Hereinafter: Anti-Defamation League, *Ecoterrorism*.

³³¹ See <http://www.animalliberationfront.com/>; <http://www.animalliberationpressoffice.org/>; and (continued...)

- Reverend Donald Spitz administers the Army of God's website.³³² Among other things, the site includes lists of people who support "violent opposition to abortion" as well as listing people incarcerated because of anti-abortion crimes they committed.³³³
- The National Socialist Movement sponsors its own social networking site, the "New Saxon Social Network."³³⁴

Some domestic terrorists also engage in cyber attacks. According to DOJ, an animal rights extremist cell (SHAC USA, Inc.) active between 2001 and 2004 listed online the personal information—names, addresses, phone numbers—of workers at a firm it was targeting. (The business uses animals in its research.) The extremist cell likely devised the list to help focus the activities of the group's online followers. In some cases, the published information included the names of spouses and children of employees, license plate numbers, churches attended by the employees, as well as the schools their children attended. The websites used by the extremist cell also posted suggestions for action by supporters—including what it described as the "top 20 terror tactics."³³⁵ Supporters across the United States vandalized victims' homes and automobiles and engaged in cyber attacks against the research firms and other companies tied to it, among other activities.³³⁶

In January 2009, in an unclassified assessment available on the Internet, DHS stated that "leftwing" extremists were likely to increasingly use cyber attacks. The assessment noted that animal rights extremists engaged in cyber attacks such as "deletion of user accounts, flooding a company's server with e-mails, and other types of e-mail assaults intended to force businesses to exhaust resources."³³⁷

A Decentralized Threat

Domestic terrorism can be described as a decentralized threat. As this report has already suggested, domestic terrorism suspects generally operate on their own or in small, independent

(...continued)

<http://www.earthliberationfront.org/>.

³³² Jefferis, *Armed for Life*, p. 53.

³³³ Ibid., p. 77.

³³⁴ See <http://newsaxon.org/>.

³³⁵ Department of Justice, *White Paper*, p. 60; *United States v. Stop Huntingdon Animal Cruelty USA, Inc., et. al*, Superseding Indictment, CR 04-373, District Court, District of New Jersey, n.d. <http://www.justice.gov/usao/nj/press/files/pdf/shacind2.pdf>. Hereinafter: Department of Justice, *United States v. Stop Huntingdon*. The "top 20 terror tactics" included activity such as: "demonstrations at one's [a target's] home using a loudspeaker; abusive graffiti, posters and stickers on one's car and house; invading offices and, damaging property and stealing documents; chaining gates shut, and blocking gates; physical assault including spraying cleaning fluid into one's eyes; smashing the windows of one's house while the individual's family was at home; flooding one's home while the individual was away; vandalizing one's car; firebombing one's car; bomb hoaxes; threatening telephone calls and letters including threats to kill or injure one's partner or children; e-mail bombs in an attempt to crash computers; sending continuous black faxes causing fax machines to burn out; telephone blockades by repeated dialing to prevent the use of the telephone; and arranging for an undertaker to call to collect one's body."

³³⁶ According to the superseding indictment in the case, the cell also placed reports of intimidation and vandalism on its websites to encourage its followers. See Department of Justice, *United States v. Stop Huntingdon*.

³³⁷ Department of Homeland Security, *Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade*, January 26, 2009.

cells. In other words, they do not necessarily belong to organizations with cohesive, well-articulated leadership structures or cadres.

However, independently acting domestic terrorism suspects are not necessarily isolated, adrift, and cut off from any outside contact or influence. Some take ideological cues from broader movements or groups espousing extremist ideas. These groups or movements publicly disavow violent criminal behavior and engage in constitutionally protected activities. This dynamic—the interplay between above-ground groups or movements proffering extremist dogma or ideology (protected speech) that is then consumed and acted upon by independent underground groups or cells who commit crimes—is a critical feature of domestic terrorism.

Leaderless Resistance

Within the domestic terrorism realm, the notions of decentralized activity received attention in the 1980s and early 1990s when white supremacist Louis Beam circulated his theories of “leaderless resistance.”³³⁸ He saw leaderless resistance as a means to transform the white supremacy movement. Beam described it as a means of avoiding law enforcement infiltration of white supremacist groups, and he suggested *two levels* of leaderless movement activity. First, on an operational level, militant, underground, ideologically motivated cells or individuals (lone wolves) engage in movement-related illegal activity without any centralized direction or control from an organization that maintains traditional leadership positions and membership rosters. Second, on another level, the above-ground public face (the “political wing”) of the movement propagandizes and disseminates ideology—engaging in protected speech. In this system, underground cells or lone wolves would be responsible for their own actions, and the public face of the movement would not be held accountable.³³⁹

Online comments from the leadership of the neo-Nazi National Socialist Movement (NSM) offer a specific example of an above-ground movement avoiding violence and the terrorist label. The NSM’s leader has posted the following statement on the group’s website:

I want it made perfectly clear to all of our members, supporters, prospective members, readers, etc. that the National Socialist Movement condemns illegal actions and in such we do not endorse any acts of violence or terrorism. The NSM is a White Civil Rights Movement that adheres to Political activism, and a legal means to restore America to its former glory. Acts of violence or terrorism against America, or its Citizens is unacceptable, and not tolerated within the ranks of the National Socialist Movement.³⁴⁰

³³⁸ He was a Ku Klux Klan (KKK) and Aryan Nations activist.

³³⁹ Paul Jooose, “Leaderless Resistance and Ideological Inclusion: The Case of the Earth Liberation Front,” *Terrorism and Political Violence*, vol. 19, no. 3 (September 2007), pp. 351-368. Hereinafter: Jooose, “Leaderless Resistance.” Fred Burton, “The Challenge of the Lone Wolf,” *STRATFOR*, May 30, 2007, http://www.stratfor.com/challenge_lone_wolf; Hereinafter: Burton, “The Challenge.” Southern Poverty Law Center, “Louis Beam,” <http://www.splcenter.org/get-informed/intelligence-files/profiles/louis-beam>; Anti-Defamation League, “Louis Beam,” http://www.adl.org/learn/ext_us/beam.asp?xpicked=2&item=beam. Beam secretly discussed leaderless resistance among white supremacists and anti-government extremists as early as 1983. See Wright, *Patriots*, p. 87. Forms of leaderless resistance likely have a long history. For example, late-nineteenth-century anarchists can be seen as having engaged in a type of leaderless resistance in their rejection of organized authority. See Jean-Marc Flükiger, “The Radical Animal Liberation Movement: Some Reflections on Its Future,” *Journal for the Study of Radicalism*, vol. 2, no. 2 (2009), pp. 112. Hereinafter: Flükiger, “The Radical.” See also Ramón Spaaij, “The Enigma of Lone Wolf Terrorism: An Assessment,” *Studies in Conflict and Terrorism*, vol. 33, no. 9 (2010), p. 859. Hereinafter: Spaaij, “The Enigma.”

³⁴⁰ Jeff Schoep, “CDR Jeff Schoep Denounces Violence & Domestic Terrorism,” <http://www.nsm88.org/> (continued...)

“The Turner Diaries”

One of the key texts read by neo-Nazis and anti-government extremists is *The Turner Diaries*, a 1978 novel by William Pierce, the deceased founder of the neo-Nazi group National Alliance.³⁴¹ This book can be seen as an above-ground product that motivates underground cells or individuals to commit crimes. The book has partly inspired a number of violent acts by white supremacist extremists and anti-government extremists.

The Turner Diaries predates the widespread acceptance of the “leaderless resistance” concept. However, its lasting place in the neo-Nazi and anti-government extremist movements highlights how leaderless resistance works. Peirce’s book has been described as “the most widely read book among far-right extremists.”³⁴² The novel reflects the author’s own racist religious philosophies.³⁴³ Perhaps 500,000 copies of the book have been sold.³⁴⁴ In it, Pierce emphasized that the current racial order of things had to be cataclysmically destroyed and reborn in accordance with white supremacist ideals.³⁴⁵ To convey this message, he devised his book as the edited diaries of neo-Nazi character Earl Turner. As such, Turner’s story is annotated by a fictionalized editor, one Andrew Macdonald. The novel describes Turner leading a terrorist group whose actions trigger a race war that results in the overthrow of the government—controlled by Jews in Pierce’s construction. Turner also initiates a nuclear war that wipes out earth’s non-white human inhabitants. The atomic apocalypse allows for the rebirth of a revitalized white race.³⁴⁶

The book has informed the activities of domestic terrorists. In September 1983, white supremacist Robert Mathews formed a small underground group known as The Order. Its inspiration came from passages in *The Turner Diaries*. The group planned for and engaged in what it viewed as a revolution.³⁴⁷ Over the next 15 months, The Order went on a violent crime spree. Among other crimes, it robbed banks, armored cars, electronic stores, a truck stop, and a video store, and allegedly gave some of the spoils to Richard Butler, who was at the time the leader of the WSE group Aryan Nations. The Order also bombed a synagogue and murdered a Jewish talk show host, Alan Berg, before it was dismantled by federal law enforcement.³⁴⁸

(...continued)

commandersdesk/.

³⁴¹ Renee Brodie, “The Aryan New Era: Apocalyptic Realizations in *The Turner Diaries*,” *Journal of American Culture*, vol. 21, no. 3, (fall 1998), pp. 13-22.

³⁴² Anti-Defamation League, “*The Turner Diaries*,” 2005, http://www.adl.org/learn/Ext_US/turner_diaries.asp.

³⁴³ See Brad Whitsel, “*The Turner Diaries* and Cosmotheism: William Pierce’s Theology,” *Nova Religio: The Journal of Alternative and Emergent Religions*, vol. 1, no. 2 (April 1998), pp. 183-197. Hereinafter: Whitsel, “*The Turner Diaries*.”

³⁴⁴ Freilich, Chermak, and Caspi, “Critical Events,” p. 505. Another estimate dating back to 2001 places the number sold at 300,000. See Rob McAlear, “Hate, Narrative, and Propaganda in *The Turner Diaries*,” *The Journal of American Culture*, vol. 32, no. 3 (September 2009), p. 192. Hereinafter: McAlear, “Hate, Narrative.”

³⁴⁵ George Michael, “The Revolutionary Model of Dr. William L. Pierce,” *Terrorism and Political Violence*, vol. 15, no. 3 (Autumn 2003), p. 75.

³⁴⁶ Whitsel, “*The Turner Diaries*,” p. 185; Terence Ball and Richard Dagger, “*The Turner Diaries*: Neo-Nazi Scripture,” *PS: Political Science and Politics*, vol. 30, no. 4, (December 1997), pp. 717-718. McAlear, “Hate, Narrative,” p. 196.

³⁴⁷ Wright, *Patriots*, pp. 87-88; Anti-Defamation League, “Richard Scutari,” http://www.adl.org/learn/ext_us/scutari.asp?xpicked=2&item=scutari. Hereinafter: Anti-Defamation League, “Scutari.” Zeskind, *Blood and Politics*, pp. 96-100.

³⁴⁸ Balch, “The Rise and Fall,” 87, 109; Wright, *Patriots*, p. 86-89.

Anti-government extremist Timothy McVeigh, an avid reader of the book, had passages from the *Turner Diaries* with him when he was arrested. The 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City mimicked one described in the novel and involved a small cell of underground conspirators.³⁴⁹ Sales of the book allegedly rose after the bombing.³⁵⁰

The ALF, the ELF

The concept of leaderless resistance has been mirrored by other extremist movements in the United States. Both the ALF and the ELF have rejected recognizable leadership structures or hierarchies and follow a leaderless resistance model instead, making their activities more difficult for law enforcement to investigate.³⁵¹ According to the model, above-ground elements in the movements provide guidelines and an ideological platform that underground individuals (lone wolves) or independent cells can draw upon to motivate their own criminal actions. Exercising First-Amendment rights, the above-ground components of the ALF and the ELF lawfully communicate shared identities largely via websites. As one scholar has suggested for the ELF, this possibly creates a broad consensus focused on a very specific cause and avoids internecine conflicts over ideological fine points.³⁵² Much like the NSM, the above-ground elements of the ALF take pains to distinguish themselves from criminal activity. For example, NAALPO states:

Disclaimer: The Animal Liberation Press Officers do not engage in illegal activities, nor do they know any individuals who do. Rather, the Press Office receives and posts communiqués from anonymous parties and provides comment to the media.³⁵³

Additionally, the above-ground literature of both the ALF and the ELF suggests that independent cells avoid communication with one another.³⁵⁴ This leaderless format is followed to avoid law enforcement infiltration and is based on models used by other domestic terrorists. As one scholar has suggested, this parallels franchising in the business world.³⁵⁵

Lone Wolves

Some domestic terrorists are “lone wolves.” This can be seen as a form of leaderless resistance. One scholar has offered a succinct conceptualization:

Lone wolf terrorism involves terrorist attacks carried out by persons who (a) operate individually, (b) do not belong to an organized terrorist group or network, and (c) whose *modi operandi* are conceived and directed by the individual without any direct outside command hierarchy.³⁵⁶

³⁴⁹ McAlear, “Hate, Narrative,” p. 192; Wright, *Patriots*, pp. 6, 10.

³⁵⁰ Freilich, Chermak, and Caspi, “Critical Events,” p. 505.

³⁵¹ Ackerman, “Beyond Arson,” p. 151.

³⁵² Joesse, “Leaderless Resistance,” p. 352, 354.

³⁵³ NAALPO, “History.”

³⁵⁴ Thurston, *The ALF Primer*, p. 1. See also *United States v. Joseph Dibee et. al*, Indictment, CR 06-60011-AA, District Court, District of Oregon, January 19, 2006; Leader and Probst, “The Earth Liberation Front,” pp. 37-58.

³⁵⁵ Flükiger, “The Radical,” pp. 111-119.

³⁵⁶ *Ibid.*, p. 856.

Lone wolves have committed crimes in the names of a number of domestic terrorism movements. For example, according to the FBI, when it comes to violence attributed to white supremacist extremism, lone wolves play a prominent role. Lone wolves filter in and out of WSE groups. They can either get dismissed from these groups because of their “violent tendencies” or voluntarily leave because they find the organizations too passive.³⁵⁷ There is little research on the lone wolf phenomenon and no universally accepted definition of the term.³⁵⁸

The above definition stresses how lone wolves operate. Just as critical is what they believe. Lone wolves can hew to broader ideological causes and use them to justify their actions.³⁵⁹ This suggests that lone wolves potentially adopt the ideas of broader terrorist movements while not claiming formal membership in them. Divining exactly what “formal membership” constitutes leads to debate regarding whether or not some individuals acted as lone wolves or part of larger movements. For example:

- On January 29, 2010, Scott Roeder was convicted of first-degree murder and two counts of aggravated assault for killing abortion provider George Tiller.³⁶⁰ Roeder allegedly had “connections with militant abortion foes but few formal ties with known groups.”³⁶¹ Some supporters of abortion rights consider his contacts among anti-abortion adherents as evidence of possible conspiracy.³⁶² Meanwhile, some anti-abortion activists have stressed that Roeder was a lone wolf.³⁶³ He remains the only person convicted of Tiller’s murder.

Because lone wolves are not plugged into terrorist organizations, distinguishing them from individuals who commit hate crimes can also be difficult.³⁶⁴ In these cases, as mentioned above, the FBI likely attempts to determine whether the motives involved were personal (hate crime) and not focused on broader ideologies (domestic terrorism).

The Law Enforcement Challenges Posed by Lone Wolves

Lone wolves present particular challenges to law enforcement. Because lone wolves, by definition, operate alone, it can be difficult for law enforcement to assess exactly which radicalized individuals intend to turn their beliefs into action and pursue terrorist activity. One former FBI counterterrorism official has said:

The lone wolf is arguably one of the biggest challenges to American law enforcement. How do you get into the mind of a terrorist? The FBI does not have the capability to know when a

³⁵⁷ Federal Bureau of Investigation, *Rage and Racism*, p. 8.

³⁵⁸ Spaaij, “The Enigma,” pp. 855-856.

³⁵⁹ Ibid.

³⁶⁰ Sylvester, “Scott Roeder.”

³⁶¹ Judy L. Thomas, “Was Suspect in Tiller Case a Lone Wolf?” *The Kansas City Star*, June 14, 2009. Hereinafter: Thomas, “Was Suspect?”

³⁶² Amanda Robb, “Not a Lone Wolf,” *Ms. Magazine*, vol. 20, no. 2 (Spring 2010), pp. 26-31.

³⁶³ Thomas, “Was Suspect?”

³⁶⁴ Eric Boehlert, “Terrorism or Hate Crime?” *Salon.com*, April 17, 2003, http://dir.salon.com/story/news/feature/2003/04/17/terrorist_act/index.html.

person gets up in middle America and decides: ‘I’m taking my protest poster to Washington or I’m taking my gun.’³⁶⁵

Aside from intent, it is also hard to assess the operational capability of potential lone wolf terrorists—knowledge of explosives, familiarity with firearms, or experience in surveillance, for example.³⁶⁶ Lone wolves do not participate in terrorist networks or training camps that can be infiltrated or whose communications can be traced. They do not rehearse their schemes or practice their criminal skills with conspirators who can potentially act as cooperating witnesses. To attempt to overcome these issues, the FBI asserted in 2009 that it was “beginning an extensive study on identified lone offenders to come up with indicators and behavior predictors that investigators can use to assess suspects.”³⁶⁷

Not all of the news for law enforcement regarding lone wolves is necessarily dire. They have weaknesses. Their lack of tradecraft may make it harder for lone wolves to engage in large-scale attacks. Likewise, lone wolves do not necessarily experience the reinforcement of a closely knit terrorist social network. They cannot rely on others to assist them in any type of complicated plot.³⁶⁸

Regardless, lone wolf attacks can be lethal. For example, according to one scholarly examination, between 1990 and April 2009, “far-rightists” have been responsible for the deaths of 42 law enforcement officers—most from state and local agencies in the United States. Most of the incidents involved firearms, *and most of the assailants acted alone*.³⁶⁹ Other instances of fatalities have been documented as well. Aside from the 2010 actions of Scott Roeder and the 2009 shooting involving James von Brunn (discussed elsewhere), suspected lone wolves were involved in at least two fatal shooting incidents in 2009, according to media sources and watchdog groups. The individuals involved in these incidents held white supremacist beliefs.

- Richard Poplawski shot and killed three Pittsburgh police officers in April 2009. He has been described as a “white supremacist” lone wolf.³⁷⁰ He had posted anti-government messages on racist websites.³⁷¹
- On January 21, 2009, Keith Luke allegedly shot and killed two Cape Verdean immigrants and raped and shot a third. Police arrested him before he could attack

³⁶⁵ Gary Fields and Evan Perez, “FBI Seeks to Target Lone Extremists,” *Wall Street Journal*, June 15, 2009, <http://online.wsj.com/article/SB124501849215613523.html>.

³⁶⁶ Scott Stewart and Fred Burton, *Lone Wolf Lessons*, STRATFOR, June 3, 2009, http://www.stratfor.com/weekly/20090603_lone_wolf_lessons?ip_auth_redirect=1. Hereinafter: Stewart and Burton, *Lone Wolf*. See also Steven M. Chermak, Joshua D. Freilich & Joseph Simone Jr., “Surveying American State Police Agencies About Lone Wolves, Far-Right Criminality, and Far-Right and Islamic Jihadist Criminal Collaboration,” *Studies in Conflict and Terrorism*, vol. 33 no. 11 (2010).

³⁶⁷ Federal Bureau of Investigation, “Domestic Terrorism.”

³⁶⁸ Stewart and Burton, *Lone Wolf*.

³⁶⁹ START, press release, “Background Information: Far-Right Attacks on U.S. Law Enforcement,” April 2009, http://www.start.umd.edu/start/media/Far-Right_Attacks_on_US_Law_Enforcement_PressRelease.pdf. The scholars who developed the information in the press release defined “far-right ideology” as “principles such as fierce nationalism, anti-globalization, suspicions of centralized Federal authority, support for conspiracy theories, and reverence for individual liberties (including gun ownership).”

³⁷⁰ McNulty et al., “Jury Decides.” See also Anti-Defamation League, “Richard Poplawski.”

³⁷¹ Hamill, “Man Accused.”

a synagogue, as he planned.³⁷² Luke purportedly informed police that he had decided to go on his spree after reading about “the demise of the white race” on a neo-Nazi website.³⁷³ He reputedly said that he was “fighting for a dying race” and that he had been planning the attack for six months.³⁷⁴

The shootings perpetrated by Roeder and von Brunn had been described by the federal government as terrorist acts.³⁷⁵ It is unclear whether the Poplawski and Luke cases are considered as such.

Lone wolves do not necessarily have to focus on gun-related crimes. Kevin Harpham’s case illustrates as much. On March 9, 2011, law enforcement officers arrested Kevin Harpham (discussed elsewhere) and charged him in connection to a bomb concealed in a backpack and placed along the route of a Martin Luther King, Jr. Day March in Spokane, WA. In September 2011, Harpham pled guilty to committing a federal hate crime and attempting to use a weapon of mass destruction.³⁷⁶ Media reports and watchdog groups have indicated that Harpham had ties to white supremacists. Allegedly, he was a member of the neo-Nazi National Alliance in 2004. The group denied that he was still a member. Harpham had also been in contact with Paul Mullet, leader of a white supremacist group active in Athol, ID. Mullet said that he and Harpham spoke many times but that the latter never joined Mullet’s group.³⁷⁷ Harpham reportedly made postings on white supremacist websites and read *The Turner Diaries*.³⁷⁸

³⁷² John Ellement, “DA Says Racism Drove Brockton Killings, Rape,” *Boston Globe*, January 23, 2009, http://www.boston.com/news/local/massachusetts/articles/2009/01/23/da_says_racism_drove_brockton_killings_rape/?page=1.

³⁷³ Phillip Martin, “Man Will Face Charges After Police Standoff,” *WGBH*, April 4, 2011, <http://www.wgbh.org/articles/-2503>.

³⁷⁴ Maureen Boyle, “Prosecutor: Suspect in double slaying in Brockton hatched an ‘Evil Plan of Mass Murder and Rape,’” *Brockton Enterprise*, January 22, 2009, updated June 9, 2010, <http://www.enterpriseneews.com/archive/x1898857767/Shots-fired-at-Brockton-police-cruiser#ixzz1K05tOtW6>.

³⁷⁵ Both von Brunn and Roeder were included in the National Counterterrorism Center’s open-source Worldwide Incidents Tracking System (WITS) database (now unavailable) that compiled worldwide terrorist incidents between 2004 and early 2012. Poplawski and Luke were not.

³⁷⁶ Department of Justice, press release, “Attempted Bomber Pleads Guilty to Federal Hate Crime and Weapons Charge,” September 7, 2011, http://www.justice.gov/usao/wae/news/2011/2011_09_07_Harpham_Plea.html; Department of Justice, press release, “Attempted Bomber Arrested,” March 9, 2011, <http://seattle.fbi.gov/dojpressrel/pressrel11/se030911.htm>.

³⁷⁷ See Southern Poverty Law Center, “Spokane Bombing Arrest Details Emerge,” March 9, 2011, <http://www.splcenter.org/blog/2011/03/09/update-spokane-bombing-arrest-details-emerge/>. Hereinafter: Southern Poverty Law Center, “Spokane Bombing.” Thomas Clouse and Meghann M. Cuniff, “White Supremacist Arrested in MLK Bomb Plot,” *Spokesman-Review*, March 10, 2011, <http://www.spokesman.com/stories/2011/mar/10/arrest-in-bomb-plot/>; Hereinafter: Clouse and Cuniff, “White Supremacist”; Joel Millman and Evan Perez, “Suspect Is Arrested in Spokane Bomb Case,” *Wall Street Journal*, March 10, 2011, <http://online.wsj.com/article/SB10001424052748704132204576190820122057388.html>. Hereinafter: Millman and Perez, “Suspect Is Arrested.”

³⁷⁸ Federal Bureau of Investigation, press release, “MLK Parade Bomber,” January 13, 2012, http://www.fbi.gov/news/stories/2012/january/hatecrime_011312/hatecrime_011312?utm_campaign=email-Immediate&utm_medium=email&utm_source=seattle-top-stories&utm_content=62754; Jessica Robinson, “Court Documents Reveal Evolution Of MLK Day Bomber’s Racist Beliefs,” *Northwest News Network*, December 1, 2011, <http://kuow.org/northwestnews.php?storyID=143023416>; Department of Justice, press release, “Colville, Wash., Man Indicted for Federal Hate Crime in Attempted Bombing of the MLK Unity March,” April 21, 2011, <http://www.justice.gov/opa/pr/2011/April/11-crt-509.html>; “FBI: Bomb Found on MLK March Route,” *MSNBC*, January 18, 2011, http://www.msnbc.msn.com/id/41139894/ns/us_news-crime_and_courts/.

Also, lone wolf activity is not solely the domain of purported white supremacists. Another case illustrates the kind of attack a domestic lone wolf animal rights extremist can commit:

- In November 2010, Walter Bond pled guilty to two felonies stemming from an April 2010 arson that destroyed a store known as the Sheepskin Factory in Glendale, CO.³⁷⁹ Speaking from jail, Bond condemned the business, which sold sheepskin products, as engaging in “blood trade” and drawing profits “from the death and exploitation of suffering animals.”³⁸⁰ Bond worked alone. A web posting claimed the arson “in defense and retaliation for all the innocent animals that have died cruelly at the hands of human oppressors.”³⁸¹ Apparently, Bond strongly identified with the notion of being a lone wolf. The ATF, working with a confidential informant, recorded Bond discussing the fire and the fact that he actually used the nickname “Lone Wolf.”³⁸² In a jailhouse letter, Bond stated, “I used the name ‘ALF Lone Wolf’ in the media to convey to my ALF brothers and sisters worldwide (whoever they are) the power of acting alone.”³⁸³

Prison Radicalization

As some experts have pointed out, prison offers an environment in which individuals can potentially radicalize³⁸⁴ on the way to becoming terrorists. This issue has loomed large among experts examining international terrorism.³⁸⁵ A scholar of the prison radicalization phenomenon in the United Kingdom notes that jail time potentially jump starts the radicalization process for individuals who are at risk of radicalizing. Prison brings together disaffected people who may be receptive to anti-social messages offering “clear, albeit intolerant, solutions to complex problems

³⁷⁹ Yesenia Robles, “Vegan Activist Pleads Guilty to Torching Sheepskin Factory,” *Denver Post*, November 19, 2010, http://www.denverpost.com/news/ci_16653821. Hereinafter: Robles, “Vegan Activist.”

³⁸⁰ “Suspect in Arson at Sheepskin Factory in Glendale Decries Animal ‘Blood Trade,’” *Denver Post*, August 6, 2010, http://www.denverpost.com/news/ci_15691097.

³⁸¹ Robles, “Vegan Activist.”

³⁸² *United States v. Walter Bond*, Criminal Complaint, MJ-01120-MJW, District Court, District of Colorado, July 23, 2010. Hereinafter: *U.S. v. Walter Bond*.

³⁸³ Walter Bond, “I Am the ALF ‘Lone Wolf,’” December 4, 2010, http://www.animalliberationpressoffice.org/essays/2010-12_bond_lonewolf.htm. He was also convicted for two other arsons. See “Walter Bond Sentenced to 7 years for two ALF Arsons,” <http://www.animalliberationfrontline.com/walter-bond-sentenced-to-seven-years-for-animal-liberation-front-arsons/>; Scott Stewart, “Escalating Violence from the Animal Liberation Front,” *STRATFOR*, July 29, 2010, http://www.stratfor.com/weekly/20100728_escalating_violence_animal_liberation_front?ip_auth_redirect=1. See also *U.S. v. Walter Bond*.

³⁸⁴ For this report, “radicalization” describes the process of acquiring and holding radical or extremist beliefs. “Terrorism” describes violent or illegal action taken on the basis of radical or extremist beliefs.

³⁸⁵ Neumann, *Prisons and Terrorism*. James Brandon, “The Danger of Prison Radicalization in the West,” *Combating Terrorism Center Sentinel*, vol. 2, no. 12 (December 2009), p. 4, <http://www.ctc.usma.edu/posts/the-danger-of-prison-radicalization-in-the-west>. Hereinafter: Brandon, “The Danger of Prison.” Greg Hannah, Lindsay Clutterbuck, and Jennifer Rubin, *Radicalization or Rehabilitation: Understanding the Challenges of Extremist and Radicalized Prisoners*, RAND Europe, Cambridge, U.K., 2008, http://www.rand.org/pubs/technical_reports/2008/RAND_TR571.pdf; U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Prison Radicalization: Are Terrorist Cells Forming in U.S. Cell Blocks?* 109th Cong., 2nd sess. September 19, 2006, S. Hrg. 109–954 (Washington: GPO, 2007), pp. 1–6, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:30597.pdf; George Washington University Homeland Security Policy Institute (HSPI) and The University of Virginia Critical Incident Analysis Group (CIAG), “Out of the Shadows: Getting Ahead of Prisoner Radicalization,” HSPI and CIAG, Washington, DC. September 2006, http://www.healthsystem.virginia.edu/internet/ciag/publications/out_of_the_shadows.pdf.

of identity and belonging.”³⁸⁶ In other words, some disaffected prisoners may discover and adopt terrorist ideals as they try to find meaning behind bars, potentially establishing bonds with like-minded people in jail. Another study of government policies on prison radicalization in 15 countries (including the United States) concludes that “[w]hether or not one believes that prisons have become Al Qaeda’s ‘universities’ or ‘finishing schools’ there can be no question that prisons matter.”³⁸⁷ They matter because they have figured largely in the development of many previous radical movements around the globe. Prisons also unsettle prisoners who “are more likely than elsewhere to explore new beliefs and associations.”³⁸⁸

Some prison gangs delve into radical or extremist ideologies that also motivate domestic terrorists, and in a number of instances, these ideologies are integral to fashioning cohesive group identities within prison walls. It must be reiterated, however, that even for gangs exhibiting these ideological dimensions, criminal enterprises such as drug trafficking—not radical beliefs—largely drive their activities. The largest white supremacist prison gangs illustrate this.

Several gangs in America’s penal institutions subscribe to white supremacist beliefs, views broadly shared by some domestic extremist groups such as the National Socialist Party, the National Alliance, Aryan Nations, and racist skinheads. A national-level gang of this ilk with approximately 15,000 members in and out of prison, the Aryan Brotherhood, has factions within facilities managed by the California Department of Corrections and the Federal Bureau of Prisons.³⁸⁹ The Nazi Low Riders, a regional-level gang with a membership estimated between 800 and 1,000, exists in correctional facilities on the West Coast and in the Southwest.³⁹⁰ Another white supremacist gang with a prison and street presence, Public Enemy Number One—largely a local-level organization with between 400 and 500 members—is mostly active in California with scattered groups outside of the state.³⁹¹

These three groups may espouse racial hatred, but they are largely guided by the profit motive, not extremism.³⁹² For example, one expert has described the Aryan Brotherhood’s ideological underpinnings as “mostly just a good recruiting tool and a way to maintain structure and discipline. These guys are more about making money than starting any kind of white revolution.”³⁹³ As another indicator of the primacy of profit, members of all three white

³⁸⁶ James Brandon, “The Danger of Prison” p. 4.

³⁸⁷ Neumann, *Prisons and Terrorism*, p. 7.

³⁸⁸ Ibid.

³⁸⁹ Department of Justice “Prison Gangs and Photos,” <http://www.justice.gov/criminal/ocgs/gangs/prison.html>; “Member of Aryan Brotherhood Booked in Slidell,” *Associated Press State and Local Wire*, October 6, 2009; David Holthouse, “Smashing the Shamrock,” *Intelligence Report*, Southern Poverty Law Center, Issue 119, (Fall 2005), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2005/fall/smashing-the-shamrock?page=0,1>. Hereinafter: Holthouse, “Smashing.”

³⁹⁰ Ibid. For the description of the Aryan Brotherhood as a “national” prison gang, the Nazi Low Riders as a “regional” prison gang, and Public Enemy Number One as a “local” prison gang, see National Drug Intelligence Center, *Attorney General’s Report to Congress on the Growth of Violent Street Gangs in Suburban Areas*, (April 2008), Appendix B, <http://www.justice.gov/ndic/pubs27/27612/appendb.htm#start>.

³⁹¹ Ibid. See also Pete Simi, Lowell Smith, and Ann M. S. Reeser, “From Punk Kids to Public Enemy Number One,” *Deviant Behavior*, vol. 29, no. 8 (2008), pp. 753-774. Hereinafter: Simi et al., “From Punk.”

³⁹² Freilich, Chermak, and Caspi, “Critical Events,” p. 508; Holthouse, “Smashing”; Camille Jackson, “Nazi Low Riders,” *Intelligence Report*, Southern Poverty Law Center, Issue 114, (Summer 2004), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2004/summer/nazi-low-riders>.

³⁹³ Holthouse, “Smashing.”

supremacist groups often set aside their racism and “have working relationships with Hispanic street gangs and non-white prison gangs such as the Mexican Mafia, due to a shared interest in criminal activity, particularly the drug trade.”³⁹⁴ However, members of racist gangs do commit hate crimes. For example, in 1998 “[t]wo of the three men who murdered James Byrd Jr., a black man, by tying him to their pickup truck and dragging him over three miles of road near Jasper, Texas, were ex-cons who belonged to the [Aryan] Brotherhood.”³⁹⁵

One study has estimated that “hundreds, possibly thousands” of sovereign citizens have been incarcerated in the United States since the 1990s, where some have continued to practice their beliefs and even pass their knowledge on to other prisoners.³⁹⁶ An unknown number of prisoners have converted to the movement’s ideology, while others have simply used sovereign tactics.³⁹⁷ The following cases suggest how this may occur.

- In September 2010, Marlon T. Moore pled guilty to one count of filing a false claim with the IRS, requesting a fraudulent refund of \$9,087,987.95.³⁹⁸ Prior to his 2010 guilty plea, he had become a sovereign citizen during a six-year stint in prison on drug-related money laundering charges.³⁹⁹
- In 1992, James T. McBride discovered sovereign citizen ideology while in a Michigan prison on drug-related charges. After he left prison, among other things, he became a sovereign guru and operated a business that peddled sovereign ideas.⁴⁰⁰

Policy Considerations for Congress

Congress may choose to consider issues in three areas regarding the federal role in combating domestic terrorism: (1) assessing this threat’s scope, (2) the adequacy of domestic terrorism intelligence collection efforts, and (3) how domestic terrorism fits into the Obama Administration’s efforts to counter radicalization that may lead to terrorism.

Scoping the Threat

As this report suggests, at least three factors may make it hard for policymakers to form a baseline evaluation of the domestic terrorism threat from publicly available information. First, federal agencies employ varying terminology to describe the threat. Second, the federal

³⁹⁴ Anti-Defamation League, *PEN1, Public Enemy Number 1: California’s Fastest Growing Racist Gang*, (2007), p. 7, http://www.adl.org/learn/ext_us/peni_report.pdf; Simi et al., “From Punk,” p. 765.

³⁹⁵ Leah Nelson, “Fugitive with ties to Aryan Brotherhood Captured,” August 20, 2010, Southern Poverty Law Center, <http://www.splcenter.org/blog/2010/08/20/fugitives-with-ties-to-aryan-brotherhood-captured/>.

³⁹⁶ Anti-Defamation League, *The Lawless*, p. 12.

³⁹⁷ Anti-Defamation League, *The Lawless*, p. 13.

³⁹⁸ Department of Justice, press release, “Miami-Dade Man Pleads Guilty to Filing a False Claim with the IRS for More Than \$9 Million,” September 10, 2009.

³⁹⁹ Anti-Defamation League, *The Lawless*, p. 13. See also Tim Elfrink, “Did Fringe Movement Sovereign Citizens Trick a Miami Man into Filing a \$14 Trillion Tax Return?” *Miami New Times*, March 4, 2010.

⁴⁰⁰ Andrew Welsh-Huggins, “Sovereign Citizens—A 21st Century Counter Culture,” *Associated Press*, available from MSNBC, August 12, 2010, http://www.msnbc.msn.com/id/38668124/ns/us_news-life/t/sovereign-citizens-st-century-counter-culture/.

government lacks a public and official method for either designating specific domestic groups as terrorists or formally and openly describing particular extremist movements as threats. Finally, there is no clear sense of how many domestic terrorism plots and attacks the government has investigated in recent years.

Terminology

The federal government has used broad conceptualizations to describe domestic terrorism. DOJ discusses the issue in terms of a handful of general “threats” such as animal rights extremists, eco-terrorists, anarchists, and anti-government extremists—not specific groups. Additionally, terms such as “terrorism” and “extremism” appear to be used interchangeably. Presumably, using the term “extremist” allows lawyers, policymakers, and investigators the flexibility to discuss terrorist-like activity without actually labeling it as “terrorism” and then having to prosecute it as such. However, this may lead to inconsistencies in the development and application of the law in the domestic terrorism arena. For example, policymakers may ponder why a specific terrorism statute covers ideologically motivated attacks against businesses that involve animals,⁴⁰¹ while there are no other domestic terrorism statutes as narrow in their purview covering a particular type of target and crime.

Designating Domestic Terrorist Groups

The federal government lacks a process for publicly designating domestic terrorist organizations. In other words, there is no official open-source roster of domestic groups that the FBI or other federal agencies target as terrorist organizations. *The lack of such a designation may spring partly from First Amendment concerns.* Such a list might discourage speech and expression related to the ideologies underpinning the activities of named groups. Regardless, this stands in stark contrast to the world of international counterterrorism, where the United States maintains a well-established—legally and procedurally proscribed—regimen regarding the identification of foreign terrorist organizations (FTOs).⁴⁰²

Official FTO designation benefits counterterrorism efforts in a number of ways. Most importantly, it facilitates the prosecution of those who provide material support⁴⁰³ to listed foreign terrorist groups. Arguably, because there is no domestic terrorism equivalent of FTO designation, it is more difficult to press material support charges against domestic terrorists. In 2010, one scholar was unable to identify any material support cases involving “a domestic terrorist group or its supporters.”⁴⁰⁴ According to the Department of State, FTO designation has other effects. It

⁴⁰¹ The Animal Enterprise Terrorism Act (P.L. 109-374).

⁴⁰² Department of State, “Foreign Terrorist Organizations.”

⁴⁰³ As described in U.S. Code, Title 18, Part I, Chapter 113B, 2339A and 2339B. For more information, see CRS Report R41333, *Terrorist Material Support: An Overview of 18 U.S.C. 2339A and 2339B*, by Charles Doyle. DOJ has used material support charges as a key component in its prosecutions against foreign terrorist organizations. See CRS Report R41416 for a discussion of a number of these cases targeting homegrown jihadists.

⁴⁰⁴ Heller, “Designating Domestic,” p. 70. It may be possible to use 18 U.S.C. 2339A to prosecute an individual engaged in domestic terrorism. This statute “restricts aid to perpetrators of terrorism in general.” See Benjamin Yaster, “Resetting Scales: An Examination of Due Process Rights in Material Support Prosecutions,” *New York University Law Review*, vol. 83, no. 4 (October, 2008), p. 1364; and *ibid*.

1. Supports [U.S.] efforts to curb terrorism financing and to encourage other nations to do the same. 2. Stigmatizes and isolates designated terrorist organizations internationally. 3. Deters donations or contributions to and economic transactions with named organizations. 4. Heightens public awareness and knowledge of terrorist organizations. 5. Signals to other governments our concern about named organizations.⁴⁰⁵

This description suggests that the absence of a designation regimen for domestic terrorist groups makes it harder for the federal government to discredit such groups and simultaneously strengthen public understanding of the domestic terrorist threat. Likewise, the lack of a list might make it more difficult for the federal government to communicate exactly what the threat is to its own agencies, let alone local or state entities.

While there is no official designation process for domestic terrorist *organizations*, as it stands, DOJ and the FBI have publicly named and discussed domestic terrorism *threats*—such as animal rights extremism or anarchist extremism—without illuminating exactly how they arrive at these categories. Federal lawmakers may opt to consider the feasibility of officially formalizing this process and/or opening it up to greater oversight. Ideally, an attempt to render this process less bureaucratically opaque would simultaneously (1) enhance federal efforts to combat domestic terrorism while (2) protecting civil rights and civil liberties. For example, such a list may potentially offer agencies outside of DOJ—including relevant players at the state and local level—formal opportunities to provide input into ranking domestic terrorism threats while enshrining mechanisms by which individuals who believe in the philosophies undergirding a designated threat could petition to have that threat “de-listed.”⁴⁰⁶ On the other hand, making this process more open may take away the FBI’s flexibility to rapidly adapt its domestic terrorism priorities, especially if threats quickly mutate.

A Public Accounting of Plots and Incidents

A publicly available official accounting of domestic terrorist plots and incidents may help policymakers understand the scope of the threat in lieu of a regimen designed to name domestic terrorism organizations. However, the federal government does not produce such a document. The National Counterterrorism Center’s (NCTC) Worldwide Incidents Tracking System (WITS) had provided an official record of terrorism incidents around the globe, including the United States. This was a publicly accessible database active from 2004 to early 2012. It included basic information regarding terrorist incidents. Prior to the advent of WITS, the FBI used to publish regular reports on terrorist activity in the United States.⁴⁰⁷

The lack of a publicly available federal accounting of domestic terrorism plots and attacks makes it especially difficult to determine the scope of this diverse threat, which, for example, can be investigated and prosecuted at the state or local, let alone federal, level. Also, the lines between domestic terrorism and other forms of criminality such as tax fraud or hate crimes can be blurry. A fuller accounting of domestic terrorism plots and attacks may call such prosecutorial flexibility into question. Such an accounting may reveal the instances in which FBI *investigated* individuals as domestic terrorists but DOJ did not *prosecute* them as such.

⁴⁰⁵ Department of State, “Foreign Terrorist Organizations.”

⁴⁰⁶ The FTO designation process has such provisions. See *ibid.*

⁴⁰⁷ See <http://www.fbi.gov/stats-services/publications/terrorism-2002-2005>.

Better Sense of Scope May Assist Policymakers

Regardless, a better sense of domestic terrorism's scope publicly proffered by the federal government may assist policymakers. It may be of policymaking value for executive branch agencies to release annual statistics on domestic terrorism prosecutions, naming individuals and movements involved. Congress may also consider requesting an even more detailed annual public report that counts and describes the domestic terrorist plots dismantled; the number of attacks investigated; and the federal, state, and local agencies involved. The lack of such an accounting makes it difficult for policymakers to exercise oversight by comparing the levels of domestic terrorist activity against items such as homegrown violent jihadist activity and other threats to the homeland. A regular public accounting could also help policymakers assess the effectiveness of the government's response to the domestic terrorist threat. It may also assist policymakers who wish to compare one domestic terrorist threat against another. Finally, without a clear, publicly available understanding of the domestic terrorist threat, it may be difficult to measure how much federal funding is allocated to this issue.

Intelligence

Intelligence collection efforts against foreign terrorist groups have received much scrutiny since 9/11. U.S. efforts to gather information versus domestic terrorism actors have not. Domestic terrorism does not feature in the Director of National Intelligence's National Intelligence Priorities Framework (NIPF), described as the "means to capture issues of critical interest to senior Intelligence Community (IC) customers and communicating those issues to the IC for action."⁴⁰⁸ Importantly, for intelligence gathering and program prioritization purposes, "there is no ... standard across federal agencies that can be applied to [domestic terrorism] cases."⁴⁰⁹ Also, there likely is no established standard for the collection of intelligence from state and local investigators.⁴¹⁰ Congress may choose to examine these issues as well as the scope of intelligence collection efforts focused on domestic terrorism.

By law, "NCTC serves as the primary organization in the United States Government ... for integrating and analyzing all intelligence pertaining to counterterrorism (except for information pertaining exclusively to domestic terrorism)."⁴¹¹ Because of its lead status for counterterrorism investigations in the homeland, the FBI arguably serves the parallel role for the domestic terrorist threat. The development of any *interagency* regimen for the collection and analysis of domestic terrorism information might start with the Bureau's capacities in this regard. Congress may wish to consider whether the FBI has allocated appropriate resources and expended enough effort in collection and analysis of domestic terrorism-related intelligence as well as the safeguarding of civil rights.

⁴⁰⁸ See <http://www.dni.gov/content/AT/NIPF.pdf>; Department of Justice, *FBI FY2012 Authorization and Budget Request for Congress*, February 2011, p. 4-24, <http://www.justice.gov/jmd/2012justification/pdf/fy12-fbi-justification.pdf>. Hereinafter: Department of Justice, *FBI FY2012 Authorization*.

⁴⁰⁹ Department of Justice, *FBI FY2012 Authorization*, p. 4-24.

⁴¹⁰ Aside from suspicious activity reporting. For more information on this, see CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Jerome P. Bjelopera.

⁴¹¹ See "About the National Counterterrorism Center," http://www.nctc.gov/about_us/about_nctc.html.

How Does Domestic Terrorism Fit into the U.S. Countering Violent Extremism Strategy?

In August 2011, the Obama Administration released a strategy for countering the radicalization of terrorists, also described as combating violent extremism (CVE).⁴¹² This document was fleshed out to a degree by the Administration's release in December 2011 of its "Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States."⁴¹³ The Administration's CVE strategy and plan revolve around countering the radicalization of all types of potential terrorists, but the radicalization of *violent jihadists* is its key focus. Regardless, domestic terrorism falls under the strategy's purview.

Federal CVE efforts often depend on government agencies cooperating with local groups. In fact, the Obama Administration's national CVE strategy highlights a "community-based approach" for the federal government. To this end, the strategy states that the federal government most effectively acts as a "facilitator, convener, and source of information."⁴¹⁴ As all of this may suggest, to date the bulk of federal-level CVE work has revolved around *community engagement*.⁴¹⁵ Congress may opt to ask the Administration which domestic terrorists it will focus on under the strategy and which communities it intends to engage regarding issues surrounding non-jihadist terrorism.

Author Contact Information

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism
jbjelopera@crs.loc.gov, 7-0622

⁴¹² *Empowering Local Partners to Prevent Violent Extremism in the United States*, August 2011, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf. Hereinafter: *Empowering Local Partners*.

⁴¹³ *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, December 2011, <http://www.whitehouse.gov/sites/default/files/sip-final.pdf>. Hereinafter: *Strategic Implementation Plan*.

⁴¹⁴ *Empowering Local Partners*, p. 3.

⁴¹⁵ See CRS Report R41416, for more information.



The Domestic Terrorist Threat: Background and Issues for Congress

Jerome P. Bjelopera

Specialist in Organized Crime and Terrorism

May 15, 2012

Congressional Research Service

7-5700

www.crs.gov

R42536

CRS Report for Congress

Prepared for Members and Committees of Congress

IA_00286

Summary

The emphasis of counterterrorism policy in the United States since Al Qaeda's attacks of September 11, 2001 (9/11) has been on jihadist terrorism. However, in the last decade, domestic terrorists—*people who commit crimes within the homeland and draw inspiration from U.S.-based extremist ideologies and movements*—have killed American citizens and damaged property across the country. Not all of these criminals have been prosecuted under terrorism statutes. This latter point is not meant to imply that domestic terrorists should be taken any less seriously than other terrorists.

The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) do not officially list domestic terrorist organizations, but they have openly delineated domestic terrorist “threats.” These include individuals who commit crimes in the name of ideologies supporting animal rights, environmental rights, anarchism, white supremacy, anti-government ideals, black separatism, and anti-abortion beliefs.

The boundary between constitutionally protected legitimate protest and domestic terrorist activity has received public attention. This boundary is especially highlighted by a number of criminal cases involving supporters of animal rights—one area in which specific legislation related to domestic terrorism has been crafted. The Animal Enterprise Terrorism Act (P.L. 109-374) expands the federal government's legal authority to combat animal rights extremists who engage in criminal activity. Signed into law in November 2006, it amended the 1992 Animal Enterprise Protection Act (P.L. 102-346).

Five discussion topics in this report may help explain domestic terrorism's significance for policymakers:

- **Level of Activity.** Domestic terrorists have been responsible for orchestrating more than two-dozen incidents since 9/11, and there appears to be a growth in anti-government extremist activity as measured by watchdog groups in the last several years.
- **Use of Nontraditional Tactics.** A large number of domestic terrorists do not necessarily use tactics such as suicide bombings or airplane hijackings.
- **Exploitation of the Internet.** Domestic terrorists—much like their jihadist analogues—are often Internet savvy and use the medium as a resource for their operations.
- **Decentralized Nature of the Threat.** Many domestic terrorists rely on the concept of *leaderless resistance*. This involves two levels of activity. On an operational level, militant, underground, ideologically motivated cells or individuals engage in illegal activity without any participation in or direction from an organization that maintains traditional leadership positions and membership rosters. On another level, the above-ground public face (the “political wing”) of a domestic terrorist movement may focus on propaganda and the dissemination of ideology—engaging in protected speech.
- **Prison Radicalization.** Prison has been highlighted as an arena in which terrorist radicalization can occur. Some prison gangs delve into radical or extremist ideologies that motivate domestic terrorists, and in a number of instances, these

ideologies are integral to fashioning cohesive group identities within prison walls. It must be reiterated, however, that even for gangs that exhibit these ideological dimensions, criminal enterprises such as drug trafficking—not radical beliefs—largely drive their activities.

Congress may choose to consider issues in three areas regarding the federal role in combating domestic terrorism. First is the issue of definitions. It is difficult to assess the scope of domestic terrorism because federal agencies use varying terms to describe it. Even more basically, there is no clear sense of how many domestic terrorist attacks have occurred or how many plots the government has foiled in recent years. Second, Congress may review the adequacy of domestic terrorism intelligence collection efforts. For intelligence gathering and program prioritization purposes, there is no standard set of intelligence collection priorities across federal agencies that can be applied to domestic terrorism cases. Also, there likely is no established standard for the collection of intelligence from state and local investigators—aside from suspicious activity reporting. Finally, it may be of value to explore how domestic terrorism fits into the Obama Administration's community outreach-driven strategy to quell terrorism-related radicalization in the United States. Congress may query the Administration on which brand of domestic terrorists it plans to focus on under the strategy and which local community groups it intends to engage regarding domestic terrorism issues.

Contents

Introduction.....	1
Domestic Terrorism Defined.....	2
What Is Domestic Terrorism?	3
Toward a Narrower Definition	4
Ambiguity Regarding “U.S.-Based Extremist Ideologies”	5
Factors Complicating the Descriptions of the Domestic Terrorism Threat	5
Counting Terrorism Cases	5
Sifting Domestic Terrorism from Other Illegal Activity	6
Extremism vs. Terrorism	7
The Lack of an Official Public List.....	9
Toward a Practical Definition: Threats Not Groups	10
Animal Rights Extremists and Environmental Extremists.....	11
Anarchist Extremists	13
White Supremacist Extremists	16
Anti-Government Extremists	22
Black Separatist Extremists.....	30
Anti-Abortion Extremists.....	32
Protected Activities vs. Terrorism—Divergent Perceptions of the ALF.....	34
A Serious Domestic Concern or “Green Scare?”	34
Assessing Domestic Terrorism’s Significance.....	38
Counting Incidents.....	39
Growth in Hate Groups and Anti-Government Extremism.....	41
“Non-Violent” Strategies.....	42
Direct Action	43
The ALF: “Live Liberations” and “Economic Sabotage”	43
The ELF: “Monkeywrenching”	44
“Paper Terrorism”: Liens, Frivolous Lawsuits, and Tax Schemes	48
The Internet and Domestic Terrorists	50
A Decentralized Threat	52
Leaderless Resistance.....	53
Lone Wolves.....	55
Prison Radicalization.....	59
Policy Considerations for Congress.....	61
Scoping the Threat.....	61
Terminology	62
Designating Domestic Terrorist Groups.....	62
A Public Accounting of Plots and Incidents.....	63
Intelligence	64
How Does Domestic Terrorism Fit into the U.S. Countering Violent Extremism Strategy?	65

Figures

Figure 1. Hate Groups and Militia Groups, 2000-2010	42
---	----

Figure 2. ALF and ELF Guidelines	47
--	----

Contacts

Author Contact Information.....	66
---------------------------------	----

Introduction

Since the terrorist attacks of September 11, 2001 (9/11), domestic terrorists—*people who commit crimes within the homeland and draw inspiration from U.S.-based extremist ideologies and movements*¹—have not received as much attention from federal law enforcement as their foreign counterparts inspired by Al Qaeda. This was not necessarily always the case. The FBI reported in 1999 that “[d]uring the past 30 years, the vast majority—but not all—of the deadly terrorist attacks occurring in the United States have been perpetrated by domestic extremists.”²

The U.S. government reacted to 9/11 by greatly enhancing its counterterrorism efforts. This report discusses how *domestic* terrorists broadly fit into this new counterterrorism landscape, a terrain that in the last 10 years has been largely shaped in response to terrorists inspired by *foreign* ideologies. This report focuses especially on how domestic terrorism is conceptualized by the federal government and issues involved in assessing this threat’s significance. Today (perhaps in part because of the government’s focus on international terrorist ideologies) it is difficult to evaluate the scope of domestic terrorist activity. For example, federal agencies employ varying terminology and definitions to describe it. Also, domestic terrorism-related intelligence collection efforts have not necessarily received the same attention as similar efforts to counter foreign threats. Beyond these issues, the Obama Administration’s community outreach-driven strategy to quell terrorism-related radicalization in the United States focuses on individuals inspired by Al Qaeda. How domestic terrorism fits into this strategy is unclear. Congress may opt to examine these and other issues related to domestic terrorism.

Domestic terrorists may not be the top federal counterterrorism priority, but they feature prominently among the concerns of some law enforcement officers. For example, Los Angeles Deputy Police Chief Michael P. Downing recently included “black separatists, white supremacist/sovereign citizen extremists, and animal rights terrorists” among his chief counterterrorism concerns.³ Also possibly contributing to domestic terrorism’s secondary status as a threat, a large number of those labeled as domestic terrorists do not necessarily use traditional terrorist tactics such as bombings or airplane hijackings. Additionally, many domestic terrorists do not intend to physically harm people but rather rely on alternative tactics such as theft, trespassing, destruction of property, and burdening U.S. courts with retaliatory legal filings.

¹ This conceptualization of the term “domestic terrorism” is derived from a number of U.S. government sources detailed in this report. They are further discussed below. This paper *will not* focus on homegrown violent jihadists. However, when referring to such actors, for this report, “homegrown” describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, permanent legal residents, or visitors radicalized largely within the United States. “Jihadist” describes radicalized Muslims using Islam as an ideological and/or religious justification for belief in the establishment of a global caliphate—a jurisdiction governed by a Muslim civil and religious leader known as a caliph—via violent means. Jihadists largely adhere to a variant of Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and follow the model of the immediate followers and companions of the Prophet Muhammad.

² Federal Bureau of Investigation, *Terrorism in the United States: 30 Years of Terrorism—A Special Retrospective Edition*, (2000) p. 16.

³ Bill Gertz, “L.A. Police Use Intel Networks Against Terror,” *Washington Times*, April 11, 2011, <http://www.washingtontimes.com/news/2011/apr/11/la-police-use-intel-networks-against-terror/?page=all#pagebreak>. See also: Joshua D. Freilich, Steven M. Chermak & Joseph Simone Jr. “Surveying American State Police Agencies About Terrorism Threats, Terrorism Sources, and Terrorism Definitions,” *Terrorism and Political Violence*, vol. 21, no. 3 (2009) pp. 450-475. Freilich, Chermak, and Simone found that domestic terrorist groups featured prominently among the concerns of U.S. state police officials.

While plots and attacks by foreign-inspired homegrown violent jihadists have certainly earned more media attention, domestic terrorists have been busy as well. It is worth noting that in terms of casualties on U.S. soil, an act of domestic terrorism is second only to the events of 9/11. Timothy McVeigh's bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, claimed 168 lives and injured more than 500 others. One estimate suggests that domestic terrorists are responsible for carrying out more than two dozen incidents⁴ since 2004, and there appears to be a growth in anti-government extremist activity as measured by watchdog groups in the last several years. Much like their jihadist counterparts, domestic terrorists are often Internet savvy and use the medium as a resource for their operations. Prison has been highlighted as an arena that can foster terrorist radicalization, and white supremacy—a set of beliefs held by white supremacist extremists—has long played a role in the activities of several U.S. prison gangs. Sovereign citizen anti-government ideas (that have inspired some domestic terrorists) have also circulated in U.S. prisons.

Terrorists are typically driven by particular ideologies. In this respect, domestic terrorists are a widely divergent lot, drawing from a broad array of philosophies and worldviews. These individuals can be motivated to commit crimes in the name of ideas such as animal rights, white supremacy, and opposition to abortion, for example. The expression of these worldviews—as opposed to violence in support of them—involves constitutionally protected activities.

Aware of the lines between constitutionally protected speech and criminality, domestic terrorists often rope themselves off from ideological (above-ground) elements that openly and often legally espouse similar beliefs. In essence, the practitioners who commit violent acts are distinct from the propagandists who theorize and craft worldviews that could be interpreted to support these acts. Thus, terrorist lone actors (lone wolves) or isolated small groups (cells) generally operate autonomously and in secret, all the while drawing ideological sustenance—not *direction*—from propagandists operating in the free market of ideas.

This report provides background regarding domestic terrorists—detailing what constitutes the domestic terrorism threat as suggested by publicly available U.S. government sources.⁵ It illustrates some of the key factors involved in assessing this threat and concludes by examining potential issues for Congress. This report does not discuss in detail either violent jihadist-inspired terrorism or the federal government's role in counterterrorism investigations. It is meant to be read in conjunction with CRS Report R41780, The Federal Bureau of Investigation and Terrorism Investigations; and CRS Report R41416, American Jihadist Terrorism: Combating a Complex Threat, which provide greater context in these areas.

Domestic Terrorism Defined

Two basic questions are key to understanding domestic terrorism. First, what exactly constitutes “domestic terrorism?” Answering this question is more complicated than it may appear. Some consider all terrorist plots occurring within the homeland as acts of domestic terrorism. According to this perspective, a bombing plot involving U.S. citizens motivated by a foreign terrorist group such as Al Qaeda constitutes domestic terrorism. While this conceptualization may be true at some level, a practical definition of domestic terrorism distilled from federal sources is much

⁴ Based on information from the National Counterterrorism Center's Worldwide Incident Tracking System.

⁵ This report does not presume the guilt of indicted individuals in pending criminal cases.

narrower. It suggests that domestic terrorists are Americans who commit ideologically driven crimes in the United States but lack foreign direction or influence—whether tactical or philosophical. This conceptualization excludes homegrown individuals directed or motivated by groups such as Al Qaeda. Second, what particular *groups* are considered domestic terrorist organizations? The U.S. government does not provide a precise, comprehensive, and public answer to this question. Rather, in broad terms, the Department of Justice (DOJ) has identified a number of general *threats* that embody this issue.

What Is Domestic Terrorism?

In the most general statutory terms, a domestic terrorist engages in terrorist activity that occurs in the homeland. The Federal Bureau of Investigation (FBI, the Bureau) has lead responsibility for terrorism investigations at the federal level.⁶

The FBI generally relies on two fundamental sources to define domestic terrorism. First, the Code of Federal Regulations characterizes “terrorism” as including “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”⁷ Second, 18 U.S.C. Section 2331(5) more narrowly defines “domestic terrorism” and differentiates it from international terrorism and other criminal activity.⁸ This definition comes from Section 802 of the USA PATRIOT Act (P.L. 107-52). According to 18 U.S.C. Section 2331(5), domestic terrorism occurs primarily within U.S. territorial jurisdiction, and domestic terrorism involves

(A) ... acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

(B) appear to be intended—

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping....⁹

⁶ 28 C.F.R. §0.85.

⁷ Ibid.

⁸ U.S. Congress, Senate Committee on Environment and Public Works, “Responses of John E. Lewis [then Deputy Assistant Director, Federal Bureau of Investigation] to Additional Questions from Senator Obama,” *Eco-Terrorism Specifically Examining the Earth Liberation Front and the Animal Liberation Front*, 109th Cong., 1st sess., May 18, 2005, S. Hrg. 109-947 (Washington: GPO, 2007), p. 41. Hereinafter: Responses of John E. Lewis.

⁹ 18 U.S.C. §2331(5).

Enforcement—Joint Terrorism Task Forces

Aside from the FBI, other federal agencies such as the Bureau of Alcohol Tobacco Firearms and Explosives (ATF) and the Internal Revenue Service (IRS) play a role in enforcement efforts to counter domestic terrorism. These agencies—as well as state and local law enforcement representatives—typically cooperate within the framework of Joint Terrorism Task Forces (JTTFs), multi-agency investigative units led by DOJ and the FBI across the country.¹⁰

JTTFs are teams of police officers, federal agents, analysts, linguists, SWAT experts, and other specialists who investigate terrorism and terrorism-related crimes. Seventy-one of the more than 100 JTTFs currently operated by DOJ and the FBI were created since 9/11. Over 4,400 federal, state, and local law enforcement officers and agents—more than four times the pre-9/11 total—work in them. These officers and agents come from more than 600 state and local agencies and 50 federal agencies.¹¹

The FBI considers JTTFs “the nation’s front line on terrorism.”¹² They “investigate acts of terrorism that affect the U.S., its interests, property and citizens, including those employed by the U.S. and military personnel overseas.”¹³ As this suggests, their operations are highly tactical and can involve developing human sources (informants) as well as gathering intelligence to thwart terrorist plots. JTTFs also offer an important conduit for the sharing of intelligence developed from FBI-led counterterrorism investigations with outside agencies and state and local law enforcement.¹⁴

Additionally, there is a National JTTF, which was established in July 2002 to serve as a coordinating mechanism with the FBI’s partners. Some 40 agencies are now represented in the National JTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners.¹⁵

Toward a Narrower Definition

The definitions cited above are too broad to capture what the FBI specifically investigates as “domestic terrorism.” Besides the statutory definitions regarding the crime of domestic terrorism, the FBI has historically emphasized particular qualities inherent to the *actors* who engage in domestic terrorism. According to the Bureau, domestic *terrorists* do not simply operate in the homeland, but they also *lack foreign direction*.¹⁶ In fact, the Bureau’s practical, shorthand definition of domestic terrorism is “Americans attacking Americans based on U.S.-based extremist ideologies.”¹⁷ The Department of Homeland Security (DHS) follows this construction.¹⁸

¹⁰ Federal Bureau of Investigation, “Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces,” http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jtfts.

¹¹ Ibid.

¹² Federal Bureau of Investigation, “Protecting America Against Terrorist Attack: A Closer Look at Our Joint Terrorism Task Forces,” May 2009, http://www.fbi.gov/page2/may09/jtfts_052809.html.

¹³ Brig Barker and Steve Fowler, “The FBI Joint Terrorism Task Force Officer,” *The FBI Law Enforcement Bulletin*, vol. 77, no. 11 (November 2008), p. 13.

¹⁴ Kevin Johnson, “FBI Issues More Top Secret Clearance for Terrorism Cases,” USA Today, August 12, 2010, http://www.usatoday.com/news/nation/2010-08-12-secret-clearances_N.htm; STRATFOR, A Decade of Evolution in U.S. Counterterrorism Operations, Special Report, December 2009, http://www.stratfor.com/memberships/150745/analysis/20091216_us_decade_evolution_counterterrorism_operations?ip_auth_redirect=1; CRS Report RL33033, *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*.

¹⁵ DOJ, “Joint Terrorism Task Force,” <http://www.justice.gov/jtff/>.

¹⁶ James F. Jarboe, [then Domestic Terrorism Section Chief, Counterterrorism Division] Federal Bureau of Investigation, Testimony Before the House Resources Committee, Subcommittee on Forests and Forest Health, February 12, 2002, <http://www.fbi.gov/news/testimony/the-threat-of-eco-terrorism>. Hereinafter: Jarboe, Testimony.

¹⁷ Federal Bureau of Investigation, “Domestic Terrorism in the Post-9/11 Era,” September 7, 2009, http://www.fbi.gov/news/stories/2009/september/domterror_090709. Hereinafter: Federal Bureau of Investigation, “Domestic Terrorism.”

¹⁸ See Department of Homeland Security, “Domestic Terrorism and Homegrown Violent Extremism Lexicon,” November 10, 2011. Hereinafter: Department of Homeland Security, “Domestic Terrorism and Homegrown.”

Ambiguity Regarding “U.S.-Based Extremist Ideologies”

On the surface, the FBI’s shorthand definition for domestic terrorism appears straightforward. However, there is inherent ambiguity to it. Namely, some of the “U.S.-based extremist ideologies” driving what the Bureau views as domestic terrorism have international roots and active followings abroad. The ideologies supporting eco-extremism and animal rights extremism (discussed below) readily come to mind, and people have long committed crimes in their names outside the United States.¹⁹ At least in part, their origins lay in the United Kingdom. Nazism—with its German origins and foreign believers—is an element within domestic white supremacist extremism. Anarchism, the philosophy followed by anarchist extremists, also has longstanding European roots. The racist skinhead movement traces its origins abroad—to the United Kingdom—as well. It is unclear exactly what the FBI means when it emphasizes U.S.-based ideologies in its framing of domestic terrorism.

Factors Complicating the Descriptions of the Domestic Terrorism Threat

A few more issues make it hard to grasp the breadth of domestic terrorist activity in the United States. First, counting the number of terrorist prosecutions in general has been difficult in the post-9/11 period. Second, there may be some ambiguity in the investigative process regarding exactly when criminal activity becomes domestic terrorism. Third, the federal government appears to use the terms “terrorist” and “extremist” interchangeably when referring to domestic terrorism. It is unclear why this is the case. Finally, and most importantly, which specific *groups* are and should be considered domestic terrorist organizations? The U.S. government does not provide a public answer to this question. Rather, the federal government defines the issue in terms of “threats,” not groups.

Counting Terrorism Cases

While statutory and practical federal definitions exist for “domestic terrorism,” there is little clear sense of the scope of the domestic terrorist threat based on publicly available U.S. government information. Most broadly, it has been said that in much of the post-9/11 period, the federal courts and DOJ may have applied different parameters when sorting, counting, and categorizing *all types* of terrorist prosecutions—let alone domestic terrorism cases.²⁰ A 2009 study (critiqued by DOJ) found that the U.S. Federal District Courts, DOJ’s National Security Division, and federal prosecutors rely on different criteria to determine whether or not specific cases involve terrorism at all.²¹

¹⁹ See Gary A. Ackerman, “Beyond Arson? A Threat Assessment of the Earth Liberation Front,” *Terrorism and Political Violence*, vol. 15, no. 4 (2003), pp. 155-156. Hereinafter: Ackerman, “Beyond Arson?”

²⁰ Transactional Records Access Clearinghouse (TRAC), *Who Is a Terrorist? Government Failure to Define Terrorism Undermines Enforcement, Puts Civil Liberties at Risk*, September 8, 2009, <http://trac.syr.edu/tracreports/terrorism/215/>. DOJ issued a press release that broadly challenged these findings and suggested that TRAC may have omitted certain statistics in its study. TRAC refuted these claims. For the interchange between DOJ and TRAC, see <http://trac.syr.edu/tracreports/terrorism/219/>.

²¹ Ibid.

A bit more narrowly, in many instances, individuals considered to be domestic terrorists by federal law enforcement may be charged under non-terrorism statutes, making it difficult to grasp from the public record exactly how extensive this threat is. Regarding the prosecution of domestic terrorism cases, DOJ has noted that, “[a]lthough we do have at least one specialized [federal] statute aimed at animal enterprise terrorism,²² domestic terrorism cases often involve firearms, arson or explosive offenses; crimes relating to fraud; and threats and hoaxes.”²³ In some instances, the crimes committed by people the FBI describes as domestic terrorism suspects do not violate federal law. When this occurs, the Bureau, “support[s] [its local] partners any way [it] can—sharing intelligence, offering forensic assistance, conducting behavioral analysis, etc.”²⁴ Thus, individuals considered domestic terrorists by federal law enforcement may not necessarily be federally charged as terrorists.

Sifting Domestic Terrorism from Other Illegal Activity

It may not be possible for investigators to describe the criminal activity involved early in an investigation as domestic terrorism. In these instances, investigators can work toward clarifying the motives of the suspects involved.²⁵ Domestic terrorism cases differ from ordinary criminal activity in key ways. Most importantly, unlike ordinary criminals—who are often driven by self-centered motives such as profit and tend to opportunistically seek easy prey—domestic terrorists are driven by a cause or ideology.²⁶ If the motives involved eventually align with the definition laid out in 18 U.S.C. Section 2331(5), presumably the case becomes a domestic terrorist investigation. In some instances, ideologically motivated actors can also collaborate with profit-driven individuals to commit crimes.

To further cloud matters, another category of criminal activity, hate crime, may appear to involve ideological issues.²⁷ However, as described by one federal official, a “hate crime” “generally involve[s] acts of personal malice directed at individuals” and is missing the broader motivations driving acts of domestic terrorism.²⁸ For investigators, distinguishing between “personal malice” and ideologically motivated actions may be difficult in specific cases. This suggests that sorting domestic terrorism from hate crimes depends on the degree of a suspect’s intent. Did the suspect articulate an ideology, belong to a domestic terrorist group, or follow an extremist movement? The grey area between domestic terrorism and hate crime hints that in some instances, suspects with links to domestic terrorist movements or ideologies supporting domestic terrorism may be

²² This likely refers to the Animal Enterprise Protection Act from 1992. In late 2006 shortly after the white paper’s publication, this act was amended by the Animal Enterprise Terrorism Act.

²³ Department of Justice, *Counterterrorism White Paper*, June 22, 2006, p. 59. Hereinafter: Department of Justice, *White Paper*.

²⁴ Federal Bureau of Investigation, “Domestic Terrorism.”

²⁵ Responses of John E. Lewis, pp. 41, 42.

²⁶ In some instances such as those involving white-supremacist prison gangs who espouse extremist beliefs, the profit motive may be paramount in their criminal activity. See Joshua D. Freilich, Steven M. Chermak, and David Caspi, “Critical Events in the Life Trajectories of Domestic Extremist White Supremacist Groups,” *Criminology and Public Policy*, vol. 8, no. 3 (August 2009), p. 508. Hereinafter: Freilich, Chermak, and Caspi, “Critical Events. See also: David Holthouse, “Smashing the Shamrock,” *Intelligence Report*, Southern Poverty Law Center, Issue 119, (Fall 2005), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2005/fall/smashing-the-shamrock?page=0,1>; Camille Jackson, “Nazi Low Riders,” *Intelligence Report*, Southern Poverty Law Center, Issue 114, (Summer 2004), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2004/summer/nazi-low-riders>.

²⁷ For more on hate crimes legislation, see CRS Report RL33403, *Hate Crime Legislation*, by William J. Krouse.

²⁸ Responses of John E. Lewis, p. 41.

charged with hate crimes.²⁹ It is unclear to what extent this influences how the government understands the threat posed by extremist movements that hold racist beliefs. If some individuals of this ilk commit crimes against police or judges, for example, is the government more apt to label this activity as terrorism while individuals sharing these same racist motivations but targeting ordinary citizens based on race, religion, disability, ethnic origin, or sexual orientation are charged with hate crimes?

The FBI's public description of the case of confessed would-be bomber Kevin Harpham exemplifies how difficult it may be to characterize acts as domestic terrorism. Initially the FBI viewed the case as domestic terrorism. In 2011, Harpham, allegedly motivated by white supremacist ideology, left a bomb—which never detonated—along the route of a parade in Spokane, WA, honoring Dr. Martin Luther King, Jr. The FBI's Northwest Joint Terrorism Task Force led the investigation.³⁰ In prepared public remarks framing the “current state of the terrorism threat” from April 2011, the FBI's Assistant Director for the Counterterrorism Division noted that Harpham's case was one of “several recent domestic terrorism incidents [that] demonstrate the scope of the threat.”³¹ Harpham eventually pled guilty to committing a federal hate crime and attempting to use a weapon of mass destruction.³² Thereafter, the Bureau described the case as the successful prevention of a “horrific hate crime.”³³

Extremism vs. Terrorism

Another concept that muddies discussion of domestic terrorism is “extremism.” The latter term is commonly applied to homegrown actors, whether they be domestic terrorists or adherents of ideologies forwarded by foreign groups such as Al Qaeda. National security expert Jonathan Masters has suggested that many law enforcement officials likely view “extremism” as largely synonymous with “terrorism.”³⁴ Masters has also found that there is a “lack of uniformity in the way *domestic terrorist* activities are prosecuted” in the United States.³⁵ Presumably, using the term “extremist” allows prosecutors, policymakers, and investigators the flexibility to discuss terrorist-like activity without actually labeling it as “terrorism” and then having to prosecute it as

²⁹ While this discussion focuses on intent, domestic terrorists can exhibit additional traits that distinguish them from other offenders. For example, as part of their involvement in ideological movements, domestic terrorists often are exposed to more tactical training—in weapons, explosives, arson, reconnaissance, paramilitary discipline—than many more ordinary criminals. See Anti-Defamation League, *Guidebook on Extremism for Law Enforcement*, (2007), p. 9. Hereinafter: Anti-Defamation League, *Guidebook*.

³⁰ Department of Justice, press release, “Attempted Bomber Arrested,” March 9, 2011, <http://seattle.fbi.gov/dojpressrel/pressrel11/se030911.htm>.

³¹ Mark F. Giuliano, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, prepared remarks delivered at the Washington Institute for Near East Policy, Stein Program on Counterterrorism and Intelligence, Washington, DC, April 14, 2011, <http://www.fbi.gov/news/speeches/the-post-9-11-fbi-the-bureaus-response-to-evolving-threats>.

³² Department of Justice, press release, “Attempted Bomber Pleads Guilty to Federal Hate Crime and Weapons Charge,” September 7, 2011, http://www.justice.gov/usao/wae/news/2011/2011_09_07_Harpham_Plea.html.

³³ Federal Bureau of Investigation, “MLK Parade Bomber,” January 13, 2012, http://www.fbi.gov/news/stories/2012/january/hatecrime_011312/hatecrime_011312?utm_campaign=email-Immediate&utm_medium=email&utm_source=seattle-top-stories&utm_content=62754; Department of Justice, press release, “Colville, Wash., Man Indicted for Federal Hate Crime in Attempted Bombing of the MLK Unity March,” April 21, 2011, <http://www.justice.gov/opa/pr/2011/April/11-crt-509.html>.

³⁴ Jonathan Masters, *Militant Extremists in the United States*, Council on Foreign Relations, Washington, DC, February 7, 2011, <http://www.cfr.org/terrorist-organizations/militant-extremists-united-states/p9236>.

³⁵ Ibid.

such. This flexibility is certainly an asset to prosecutors. They can charge subjects of FBI domestic terrorism investigations under a wider array of statutes and, as a result, not describe the subjects publicly as terrorists. However, for policymakers this flexibility makes it hard to determine the scope of the domestic terrorist threat. One cannot get a clear sense of scope if some individuals are charged and publicly described as terrorists, others are discussed as extremists, and still others enter the public record only as criminals implicated in crimes not necessarily associated with terrorism, such as trespassing, arson, and tax fraud.

What Is Extremism?

The FBI's public formulation of "extremism" suggests two components. First, extremism involves hewing to particular ideologies. Second, it also includes criminal activity to advance these ideologies.³⁶ Thus, according to this construction, an anarchist believes in a particular ideology—anarchism. An "anarchist extremist" is an anarchist who adopts criminal tactics.³⁷

One scholar has indicated a similar bifurcation: First, extremism refers to an ideology outside a society's key values, and for liberal democracies, such ideologies "support racial or religious supremacy and/or oppose the core principles of democracy and human rights." Second, extremism can refer to the use of tactics that ignore the rights of others to achieve an ideological goal.³⁸

"Homegrown Violent Extremists" Are Not Domestic Terrorists

The FBI and DHS have recently popularized the phrase "homegrown violent extremist" (HVE). It separates domestic terrorists from U.S.-based terrorists *motivated by the ideologies of foreign terrorist organizations*. (HVEs include some of the actors this report considers as "homegrown violent jihadists.") According to DHS and the FBI, a HVE is "a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization."³⁹

³⁶ Federal Bureau of Investigation, "Domestic Terrorism: Anarchist Extremism, A Primer," December 16, 2010, http://www.fbi.gov/news/stories/2010/november/anarchist_111610/anarchist_111610. The focus of this piece, as the title suggests, is anarchist extremism, not necessarily defining the term "extremism." Hereinafter: Federal Bureau of Investigation, "Anarchist Extremism." This type of formulation—extremism consists of adherence to ideologies *and* criminal activity committed in the name of these ideologies—is replicated in the definitions provided within Department of Homeland Security, "Domestic Terrorism and Homegrown."

³⁷ Making things more complex, the broader concept of "violent extremism" has been used by the Obama Administration. According to the administration, "violent extremists" are "individuals who support or commit ideologically-motivated violence to further political goals." See *Empowering Local Partners to Prevent Violent Extremism in the United States*, August 2011, p. 1, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

³⁸ Peter R. Neumann, *Prisons and Terrorism: Radicalisation and De-Radicalisation in 15 Countries*, International Centre for the Study of Radicalisation and Political Violence, London, 2010, p. 12, <http://www.icsr.info/publications/papers/1277699166PrisonsandTerrorismRadicalisationandDeradicalisationin15Countries.pdf>. In its *Guidebook on Extremism for Law Enforcement*, Hereinafter: Neumann, *Prisons and Terrorism*. The Anti-Defamation League has defined extremists as: "people who subscribe to extreme ideologies." The group goes on to say, "extreme ideologies are those that promote world views so radical that most other people will not agree with them." See Anti-Defamation League, *Guidebook*, p. 3.

³⁹ This definition appears to differ from the conceptualization of "homegrown jihadists" used in this report by (1) only (continued...)

According to the FBI and DHS, an HVE is not a domestic terrorist—they are two distinct categories of terrorist actors.⁴⁰

The Lack of an Official Public List

The federal government does not generate an official *and* public list of domestic terrorist organizations or individuals.⁴¹ The development of such a list may be precluded by civil liberties concerns (i.e. inclusion in a publicly available list may impinge on a group's exercise of free speech or its other constitutionally protected activities). However, a lack of official lists or processes to designate groups or individuals as domestic terrorists makes it difficult to assess domestic terrorism trends and evaluate federal efforts to counter such threats. An unnamed DHS official cited in a news report stated that “unlike international terrorism, there are no designated domestic terrorist groups. Subsequently, all the legal actions of an identified extremist group leading up to an act of violence are constitutionally protected and not reported on by DHS.”⁴² Constitutionality aside, the lack of a list may also contribute to a certain vagueness in the public realm about which groups the federal government considers domestic terrorist organizations. While the government does not provide an official and public list of domestic terrorist organizations, it does include domestic terrorists (along with international terrorists) in its Terrorist Screening Database, commonly known as the “Terrorist Watchlist.”⁴³

The government is much less vague regarding foreign terrorist organizations. They are officially designated as such according to a well-established legally and procedurally proscribed regimen. According to the Department of State's Bureau of Counterterrorism, as of January 2012 the Secretary of State had designated 49 foreign terrorist organizations according to Section 219 of the Immigration and Nationality Act, as amended.⁴⁴

(...continued)

including individuals *not* directed by a foreign organization and by (2) including all sorts of terrorists motivated by foreign ideologies, not just violent jihadists. See Department of Homeland Security and Federal Bureau of Investigation, Joint Intelligence Bulletin, “Use of Small Arms: Examining Lone Shooters and Small-Unit Tactics,” August 16, 2011, p. 3.

⁴⁰ Ibid.

⁴¹ See Christopher Bellavita, “Does the U.S. Have Any Domestic Terrorist Groups?” *Homeland Security Watch*, June 29, 2010, <http://www.hlswatch.com/2010/06/29/does-the-us-have-any-domestic-terrorist-groups/>. Hereinafter: Bellavita, “Domestic Terrorist Groups.” See also: R. Jeffrey Smith, “Homeland Security Department Curtails Home-Grown Terror Analysis,” *Washington Post*, June 7, 2011, http://www.washingtonpost.com/politics/homeland-security-department-curtails-home-grown-terror-analysis/2011/06/02/AGQEaDLH_story_1.html. Hereinafter: Smith, “Homeland Security.” David E. Heller, “Designating Domestic Terrorist Individuals or Groups,” (Master's Thesis, Naval Postgraduate School, 2010). Hereinafter: Heller, “Designating Domestic.”

⁴² Smith, “Homeland Security.”

⁴³ Federal Bureau of Investigation, Terrorist Screening Center, “Frequently Asked Questions,” http://www.fbi.gov/about-us/nsb/tsc/tsc_faqs. See also: Timothy J. Healy, Director, Terrorist Screening Center, Federal Bureau of Investigation, Statement Before the House Judiciary Committee, Washington, DC, March 24, 2010, <http://www.fbi.gov/news/testimony/sharing-and-analyzing-information-to-prevent-terrorism?searchterm=Timothy+J.+Healy>; Bellavita, “Domestic Terrorist Groups.”

⁴⁴ For the legal criteria used to designate a foreign terrorist organization, the legal ramifications of designation, and ancillary effects of designation see Department of State, “Foreign Terrorist Organizations,” January 27, 2012, <http://www.state.gov/j/ct/rls/other/des/123085.htm>. Hereinafter: Department of State, “Foreign Terrorist Organizations.”

Toward a Practical Definition: Threats Not Groups

As discussed above, DOJ and the FBI do not list domestic terrorist organizations publicly and officially. This may complicate the understanding that federal policymakers have of what exactly the government considers “domestic terrorism.” While not naming specific *groups*, DOJ and the FBI have openly delineated domestic terrorist *threats*. DOJ has identified domestic terrorism threats to include criminal activity by “animal rights extremists, eco-terrorists, anarchists, anti-government extremists such as ‘sovereign citizens’ and unauthorized militias, [b]lack separatists, [w]hite supremacists, and anti-abortion extremists.”⁴⁵

The actors who constitute each of the domestic terrorist “threats” outlined by DOJ draw upon ideologies whose expression largely involves constitutionally protected activity. The FBI safeguards against cases focused solely on constitutionally protected activities. All FBI investigations have to be conducted for an authorized national security, criminal, or foreign intelligence collection purpose.⁴⁶ The purpose of an investigation may not be to solely monitor First Amendment rights.⁴⁷

However, it is unclear how DOJ or the FBI arrive at their list of domestic terrorism threats. This poses at least two fundamental questions:

- How does a particular brand of dissent become ripe for description by DOJ and the FBI as driving a “domestic terrorism” threat?

What criteria are involved in such a process?

How many crimes or plots attributed to a specific ideology have to occur to stimulate the identification of a new extremist threat? Is the severity of the crimes linked to an ideology taken into consideration?

- At what point do ideologically driven domestic terrorism threats cease to exist?

Should there be a means for public petitioning of the government to eliminate various threats as investigative priorities?

The below discussion of domestic terrorism threats will follow the order in which DOJ listed them. This does not necessarily presume the priority of one over the other. It is also important to note that instances of animal rights extremism and eco-terrorism within the last 10 years are

⁴⁵ Department of Justice, *White Paper*, p. 59. See also: Federal Bureau of Investigation, “Domestic Terrorism.” The FBI’s domestic terrorism investigations likely cover these categories as well as lone wolves (lone offenders): extremists who commit crimes without the support of a formal organization or network. Some lone wolves are motivated by the ideologies behind the threats outlined by DOJ, but they can fashion their own ideologies as well. In the past, in the area of domestic terrorism, the FBI has distinguished between “special interest terrorism” and “traditional right-wing and left-wing terrorism: “Special interest terrorism differs from traditional right-wing and left-wing terrorism in that extremist special interest groups seek to resolve specific issues, rather than effect widespread political change. Special interest extremists continue to conduct acts of politically motivated violence to force segments of society, including the general public, to change attitudes about issues considered important to their causes. These groups occupy the extreme fringes of animal rights, pro-life, environmental, anti-nuclear, and other movements.” It is unclear whether the FBI still uses the categories of “special interest,” “left-wing,” and “right-wing” terrorism. See Jarboe, Testimony.

⁴⁶ Federal Bureau of Investigation, *Domestic Investigations and Operations Guide*, redacted, October 15, 2011, p. 4-1 through p. 4-2.

⁴⁷ Ibid.

more readily available in the public record than cases involving other types of domestic terrorism. The extensive use of such examples in this report does not imply the prominence of animal rights extremism or eco-terrorism over other domestic terrorist threats.

Animal Rights Extremists and Environmental Extremists

The term “animal rights extremism” covers criminal acts committed in the name of animal rights.⁴⁸ Environmental extremism—most often referred to as “Eco-terrorism”—includes criminal acts committed in the name of the environment.⁴⁹ These terms are not applied to groups or individuals involved with environmental movements or animal welfare protection/rights activism within the “confines of civil society and the rule of law.”⁵⁰

Many of the crimes committed by both animal rights extremists and eco-terrorists are perpetrated by independent small cells or individuals who harass and intimidate their victims.⁵¹ These cells or lone actors engage in crimes such as vandalism, theft, the destruction of property, and arson. Most animal rights and eco-extremists also eschew physical violence directly targeting people or animals. Regardless, crimes committed by eco-terrorists and animal rights extremists have caused millions of dollars in property damage, and some have involved the intimidation and harassment of victims.⁵² These two types of extremism are often discussed together, because the two broader radical *movements* from which they draw their philosophical underpinnings have similar beliefs and overlapping membership.

The two *movements*—the Animal Liberation Front (ALF) and the Earth Liberation Front (ELF)—have the greatest reach among animal rights extremists and eco-terrorists. The ALF and the ELF are too diffuse to be called groups. Neither the ALF nor the ELF maintain formal rosters or leadership structures, for example.⁵³ However, each communicates a sense of shared identity and attracts people who commit crimes in its name. They achieve this via “above-ground” wings. Largely using websites, ALF and ELF supporters publish literature highlighting movement philosophies, tactics, and accounts (press releases) of recent movement-related criminal activity. Much of this involves protected speech and occurs in the public realm. Press releases allow “underground” extremists to publicly claim responsibility for criminal activity in the name of either movement while maintaining secrecy regarding the details of their operations. The ALF and the ELF do not work alone. Members of other entities such as Stop Huntingdon Animal Cruelty (SHAC) have committed crimes in the name of animal rights, for example.

⁴⁸ Department of Homeland Security, “Domestic Terrorism and Homegrown.”

⁴⁹ For the purposes of this paper, “eco-terrorists,” “eco-extremists,” and “environmental extremists” are synonymous. These terms and “animal rights extremism” describe individuals engaged in criminal activity in the name of radical environmental ideologies or animal rights. It is unclear why environmental extremists are frequently dubbed “eco-terrorists” while animal rights extremists do not have a similar commonplace usage applied to them.

⁵⁰ See Kevin R. Grubbs, “Saving Lives or Spreading Fear: The Terroristic Nature of Eco-Extremism,” *Animal Law*, vol. 16, no. 2 (2010), p. 353-57. Hereinafter: Grubbs, “Saving Lives.”

⁵¹ See Federal Bureau of Investigation, “Putting Intel to Work Against ELF and ALF Terrorists,” June 30, 2008, http://www.fbi.gov/news/stories/2008/june/ecoterror_063008. Hereinafter: FBI, “Putting Intel.”

⁵² Ibid.

⁵³ Both the ALF and the ELF focus on criminal activity as central tenets of their philosophies or operational guidelines, and the FBI emphasizes that criminal activity is a key element in the identities of these movements. See FBI, “Putting Intel.”

Additional factors tangle our understanding of the ALF and the ELF. People can simultaneously participate in both. This may partly be true because the movements are so amorphous. The two movements also share similar agendas, and in 1993 they declared solidarity.⁵⁴ All of this can play out confusingly in the real world. For example, an individual can commit a crime and claim responsibility for it online in the name of *both* the ALF and the ELF. One case especially highlights intersections between the ALF and the ELF.

In late 2005 and early 2006, the FBI dismantled a network that, according to DOJ, committed violent acts in the name of both the ALF and the ELF. The group included about 20 individuals and called itself “the Family.” It was reportedly responsible for at least 25 criminal incidents totaling approximately \$48 million in damages in the late 1990s and early 2000s and disbanded at some point in 2001, due to law enforcement pressure on the group. The Family was responsible for an arson attack in 1998 at the Vail Ski Resort. Eight simultaneous fires damaged radio towers, ski lift towers, restaurants, and the ski patrol office at the Colorado site and totaled over \$24 million in losses.⁵⁵

Philosophical Underpinnings

Both the ALF and the ELF rely on and borrow from a number of philosophical underpinnings to rationalize their beliefs and actions. These help forge a common identity among individuals in each movement. These ideas are also key principles professed by more mainstream animal rights or environmental activists engaged in legal protest.

The ALF: Animal Rights and Speciesism. The ALF’s moral code includes the belief that animals possess basic inalienable rights such as life, liberty, and the pursuit of happiness, and this suggests that animals cannot be owned. According to the ALF, the U.S. legal system—which describes animals as property—is corrupt, and there exists a “higher law than that created by and for the corporate-state complex, a moral law that transcends the corrupt and biased statutes of the US political system.”⁵⁶ Simply put, the rights of one species do not trump the rights of others. To suggest otherwise is to be prejudiced, according to animal rights adherents.

For the ALF and other animal rights supporters, the favoring of one species, particularly humans, over others has a name: speciesism. For the ALF, speciesism is a “discriminatory belief system as ethically flawed and philosophically unfounded as sexism or racism, but far more murderous and consequential in its implications.”⁵⁷ Thus, the movement couches the theft or illegal release of

⁵⁴ U.S. Congress, Senate Committee on Environment and Public Works, “Statement of Carson Carroll, Deputy Assistant Director, Bureau of Alcohol, Tobacco, Firearms, and Explosives,” *Eco-Terrorism Specifically Examining the Earth Liberation Front and the Animal Liberation Front*, 109th Cong., 1st sess., May 18, 2005, S. Hrg. 109-947 (Washington: GPO, 2007), p. 43. Hereinafter: Statement of Carson Carroll.

⁵⁵ Federal Bureau of Investigation, “Operation Backfire: Help Find Four Eco-Terrorists,” November 19, 2008, http://www.fbi.gov/news/stories/2008/november/backfire_11908; Department of Justice, press release, “Eleven Defendants Indicted on Domestic Terrorism Charges,” January 20, 2006, http://www.justice.gov/opa/pr/2006/January/06_crm_030.html. Hereinafter: Department of Justice, “Eleven Defendants.” See also: *United States v. Joseph Dibee et al.*, Sentencing Memorandum, CR 06-60069-AA, CR 06-60070-AA, CR 06-60071-AA, CR 06-60078-AA, CR 06-60079-AA, CR 06-60080-AA, CR 06-60120-AA, CR-06-60122-AA, CR-06-60123-AA, CR-06-60124-AA, CR-06-60125-AA, CR-60126-AA, U.S. District Court, District of Oregon, May 4, 2007, pp. 6, 8, 19, 20-21. Hereinafter: *U.S. v. Dibee et al.*

⁵⁶ North American Animal Liberation Press Office, “History of the Animal Liberation Movement,” <http://www.animalliberationpressoffice.org/Background.htm>. Hereinafter: NAALPO, “History.”

⁵⁷ Steven Best and Anthony J. Nocella, II, “Behind the Mask: Uncovering the Animal Liberation Front,” in *Terrorists* (continued...)

animals used in research or for economic gain as “liberation.” The ALF views the destruction of laboratory infrastructure or tools as the elimination of items used to enslave species who have the same rights as humans. Intimidation of scientists and employees of businesses tied to animal research or testing is rationalized as confrontation with “oppressors” or those who, in the eyes of movement adherents, abuse and murder animals.⁵⁸

The ELF: An Ideological Mélange. Eco-terrorists are motivated by a mélange of environmental philosophies. There is no single formula for what constitutes the ideological makeup of an ELF follower, but several concepts likely play key roles in the movement. These are biocentrism, deep ecology, social ecology, and green anarchism. Biocentrism argues for the equality of all organisms.⁵⁹ Deep ecology suggests that all species are part of “the larger super-organism that is nature.”⁶⁰ It criticizes industrialization and views modern human impact on the earth as negative and harkens back to small communities centered around subsistence agriculture.⁶¹ Social ecology suggests that hierarchical human society leads to social inequalities and environmental harm. Green anarchism ascribes environmental harm to civilization and domestication and embraces the notion of “rewilding,” or rejecting civilization and returning to a hunter-gatherer state to preserve one’s natural surroundings.⁶²

Anarchist Extremists

According to the FBI, anarchist extremists commit crimes in the name of anarchist ideals.⁶³ These ideals include belief that

individual autonomy and collective equality are fundamental and necessary for a functional, civilized society. [Anarchism] resists the existing hierarchical structure of society that gives some people authority and control over others. [According to anarchists] authority imbues power, and power always is used in illegitimate and self-serving ways by those who have it.⁶⁴

Anarchist extremists as well as anarchists engaging in constitutionally protected activity can oppose government, business, or social interests that they view as dangerous. As this suggests, anarchists advocate some form of revolution that realigns authority and power in the societies

(...continued)

or Freedom Fighters? Reflections on the Liberation of Animals, ed. Steven Best and Anthony J. Nocella, II (New York: Lantern Books, 2004), p. 24. Hereinafter: Best and Nocella, “Behind the Mask.” Best reportedly advises NAALPO, see <http://naalpo.posterous.com/our-task-new-essay-by-press-office-advisor-st.-p.-michael-conn-and-james-v.-parker-the-animal-research-war> (New York: Palgrave Macmillan, 2008), p. xix. Hereinafter: Conn and Parker, *The Animal*. See also: NAALPO, “History” which excerpts Best and Nocella’s work.

⁵⁸ NAALPO, “History.”

⁵⁹ Stefan H. Leader and Peter Probst, “The Earth Liberation Front and Environmental Terrorism,” *Terrorism and Political Violence*, vol. 15, no. 4 (Spring/Summer 2005), pp. 39-40. Hereinafter: Leader and Probst, “The Earth Liberation Front.”

⁶⁰ Conn and Parker, *The Animal*, xx.

⁶¹ Leader and Probst, “The Earth Liberation Front,” pp. 39-40.

⁶² Sean Parson, “Understanding the Ideology of the Earth Liberation Front,” *Green Theory and Praxis: The Journal of Ecopedagogy*, vol. 4, no. 2 (2008), pp. 54-58.

⁶³ Ibid.

⁶⁴ Randy Borum and Chuck Tilby, “Anarchist Direct Actions: A Challenge for Law Enforcement,” *Studies in Conflict and Terrorism*, vol. 28, no. 3, (2005), p. 202. Hereinafter: Borum and Tilby, “Anarchist Direct Action.”

they desire to transform. However, adherents cannot agree to a single means for attaining revolutionary change.⁶⁵

As one may assume, anarchist activity is decentralized. In fact, a basic, temporary organizational structure—the affinity group—likely plays a larger role in shaping the work of U.S. anarchists than any formal long-lasting entities or networks.⁶⁶ Affinity groups are “autonomous militant unit[s] generally made up of between five-to-twenty individuals who share a sense of the causes worth defending and the types of actions they prefer to engage in. The decision-making process is anarchist, that is to say, egalitarian, participatory, deliberative, and consensual.”⁶⁷ An affinity group often consists of a circle of friends. The friends coalesce around a specific objective and break apart when they achieve their desired ends. Individual groups can band together in “clusters” and clusters can coordinate their efforts, if need be.⁶⁸ The ends can be legal or illegal, violent or non-violent, covert or open. These structures have a long history among anarchists, but other movements use them as well.⁶⁹ Also, anarchists can engage in what they call “black bloc” tactics. These involve secretive planning for public—often criminal—activity in which participants, typically dressed in black, act en-masse.⁷⁰ Adding to the sprawling nature of the anarchist movement, some adherents also participate in the ALF and the ELF. These three movements share general philosophical tenets such as opposition to globalization and capitalism.⁷¹

The FBI has described anarchist extremists as typically being “event driven,” meaning

they show up at political conventions, economic and financial summits, environmental meetings, and the like. They usually target symbols of Western civilization that they perceive to be the root causes of all societal ills—i.e., financial corporations, government institutions, multinational companies, and law enforcement agencies. They damage and vandalize property, riot, set fires, and perpetrate small-scale bombings. Law enforcement is also concerned about anarchist extremists who may be willing to use improvised explosives devices or improvised incendiary devices.⁷²

Anarchist extremists in the United States have been involved in illegal activity during mass protests surrounding events such as the 1999 World Trade Organization Ministerial Conference in Seattle, WA.

Anarchist extremists reportedly committed crimes during the 2008 Republican National Convention in St. Paul, MN.⁷³ To coordinate their protests during the convention, some anarchists

⁶⁵ Ibid., p. 203.

⁶⁶ Ibid., p. 207.

⁶⁷ Francis Dupuis-Déri, “Anarchism and the Politics of Affinity Groups,” *Anarchist Studies*, vol. 18, no. 1 (2010), p. 41. Hereinafter: Dupuis-Déri, “Anarchism.”

⁶⁸ CrimethInc. Workers’ Collective, *Recipes for Disaster: An Anarchist Cookbook*, (Olympia, WA: CrimethInc. Workers’ Collective, 2004), pp. 28-34. Hereinafter: *Anarchist Cookbook*.

⁶⁹ Dupuis-Déri, “Anarchism,” p. 43.

⁷⁰ *Anarchist Cookbook*, pp. 127-130.

⁷¹ Borum and Tilby, “Anarchist Direct Action,” p. 208.

⁷² Federal Bureau of Investigation, “Anarchist Extremism.”

⁷³ Ibid. For information on reported anarchist criminal activity related to the 2008 Republican National Convention, see Department of Justice, press release, “Michigan Man Sentenced for Possessing Molotov Cocktails,” March 10, 2009, <http://www.fbi.gov/minneapolis/press-releases/2009/mp031009.htm>; Department of Justice, press release, “Texas Man (continued...) ”

formed what they called the “RNC Welcoming Committee” (RNCWC).⁷⁴ In September 2007, the RNCWC developed a plan to broadly organize the activities of affinity groups intending to disrupt the convention. Law enforcement infiltrated and undermined these efforts, arresting 800 people, including eight involved with the RNCWC.⁷⁵ Initially, in Minnesota state court, the eight “had been charged with felonies: first-degree damage to property and second-degree conspiracy to riot. Prosecutors added a more serious charge of conspiracy to riot in furtherance of terrorism, which was later dismissed.”⁷⁶ Five of the eight pled guilty to gross misdemeanor charges in 2010. The others had all of the charges they faced dismissed.⁷⁷

On April 30, 2012, five men who reputedly had anarchist sympathies were arrested for purportedly scheming to blow up a bridge near Cleveland, OH.⁷⁸ The plot was apparently timed to coincide with peaceful protest activity arranged by Occupy Cleveland, an offshoot of the Occupy Wall Street movement. Occupy Cleveland representatives have stated that the alleged would-be bombers “were in no way representing or acting on behalf of Occupy Cleveland.”⁷⁹ An FBI sting operation led to the quintet’s arrest.⁸⁰ Purportedly, the group relied on an undercover FBI employee to supply them with two inert bombs that the conspirators believed were functional.⁸¹

Criminal acts involving anarchist extremists do not have to be event-driven. For example, Joseph Konopka, the self-dubbed “Dr. Chaos,” allegedly led a group of boys he called “The Realm of Chaos” in a series of crimes involving vandalism to radio and cell phone towers in the late 1990s and early 2000s. In 2002, he was arrested in Chicago for storing more than a pound of deadly cyanide powder in a passageway in a Chicago Transit Authority subway tunnel.⁸² He had obtained

(...continued)

Sentenced on Firearms Charges Connected to the Republican National Convention,” May 21, 2009, <http://www.fbi.gov/minneapolis/press-releases/2009/mp052109a.htm>; Department of Justice, press release, “Austin, Texas Man Sentenced for Possessing Molotov Cocktails During the Republican National Convention,” May 14, 2009, <http://www.fbi.gov/minneapolis/press-releases/2009/mp051409.htm>. For information on a matter possibly related to the anarchist criminal activity at the 2008 convention, see James C. McKinley, Jr., “Anarchist Ties Seen in ‘08 Bombing of Texas Governor’s Mansion,” *New York Times*, February 22, 2011, <http://www.nytimes.com/2011/02/23/us/23texas.html>.

⁷⁴ For an archived version of the group’s website see <http://web.archive.org/web/20080907081250/http://www.nornc.org/>.

⁷⁵ Pat Pheifer, “Guilty Pleas Close Book on ‘08 Convention Protests,” *Minneapolis-St. Paul Star Tribune*, October 19, 2010, http://www.startribune.com/templates/Print_This_Story?sid=105311223. Hereinafter: Pheifer, “Guilty Pleas.” See also: Fred Burton and Scott Stewart, “The Lessons of St. Paul,” *STRATFOR*, September 10, 2008, http://www.stratfor.com/weekly/lessons_st_paul?ip_auth_redirect=1.

⁷⁶ Pheifer, “Guilty Pleas.”

⁷⁷ Ibid.

⁷⁸ Department of Justice, press release, “Five Men Arrested in Plot to Bomb Ohio Bridge,” May 1, 2012, <http://www.fbi.gov/cleveland/press-releases/2012/five-men-arrested-in-plot-to-bomb-ohio-bridge>. Hereinafter: Department of Justice, “Five Men.” David Ariosto, “5 Arrested in Alleged Plot to Blow Up Cleveland-Area Bridge,” *CNN*, May 1, 2012, <http://www.cnn.com/2012/05/01/justice/ohio-bridge-arrests/index.html>.

⁷⁹ Henry J. Gomez, “Bridge Bomb Plot: Suspects Were Active in Occupy Cleveland, Even As Movement Slowed to a Crawl,” *Cleveland Plain Dealer*, May 2, 2012, http://www.cleveland.com/metro/index.ssf/2012/05/bridge_bomb_plot_suspects_were.html.

⁸⁰ Department of Justice, “Five Men.”

⁸¹ Ibid.

⁸² Juliet Williams, Federal appeals Court Overturns Dr. Chaos Conviction,” *Associated Press*, May 31, 2005; Mike Robinson, “Federal Prosecutors Want ‘Dr. Chaos’ to Remain Locked Up,” *Associated Press*, March 13, 2002; Meg Jones and Jesse Garza, “‘Anarchist’ Charged Over Cache of Cyanide,” *Milwaukee Journal Sentinel*, March 12, 2002.

the material (potassium cyanide and sodium cyanide) from an abandoned warehouse.⁸³ In 2002, Konopka pled guilty in federal court to possessing chemical weapons, and in 2005 he pled guilty to 11 felonies, including conspiracy, arson, creating counterfeit software, and interfering with computers in Wisconsin.⁸⁴

White Supremacist Extremists

The term “white supremacist extremism” (WSE) describes people or groups who commit criminal acts in the name of white supremacist ideology. At its core, white supremacist ideology purports that the white race ranks above all others. WSE draws on the constitutionally protected activities of a broad swath of racist hate-oriented groups active in the United States ranging from the Ku Klux Klan to racist skinheads. Some of these groups have elaborate organizational structures, dues-paying memberships, and media wings. Additionally, many individuals espouse extremist beliefs without having formal membership in any specific organization.

A large proportion of white supremacists dualistically divide the world between whites and all other peoples who are seen as enemies.⁸⁵ Particular animus is directed toward Jews and African Americans. In fact, a common racist and revisionist historical refrain is that the civil rights movement succeeded only because Jews orchestrated it behind the scenes.⁸⁶

Scholars indicate that white supremacists believe in racial separation and that society discriminates against them. To them, whites have lost “ground to other groups and ... extreme measures are required to reverse the trend.”⁸⁷ All of this has been encapsulated in a slogan known as the “Fourteen Words”: “We must secure the existence of our race and a future for white children.” This was coined by David Lane, a member of a violent terrorist group active in the 1980s. The Fourteen Words have been described as “the most popular white supremacist slogan in the world.”⁸⁸

Neo-Nazism and its obsession with Adolph Hitler and Nazi Germany is also a prominent component of white supremacist extremism in the United States.⁸⁹ The father of American neo-Nazism, George Lincoln Rockwell, became publicly active in the late 1950s. According to one scholar, Rockwell laid down three concepts that have shaped neo-Nazism ever since. For his followers, he reconfigured the racial notion of “white,” broadening it beyond “Aryan” to include people of Southern and Eastern European descent. Additionally, Rockwell denied the Holocaust.

⁸³ “Man Pleads Guilty to Storing Cyanide,” *Associated Press*, November 21, 2002.

⁸⁴ “Judge Sentences ‘Dr. Chaos’ to Prison for Damage to Wisconsin Power Systems,” *Associated Press*, November 30, 2005.

⁸⁵ Chip Berlet and Stanislav Vysotsky, “Overview of U.S. White Supremacist Groups,” *Journal of Political and Military Sociology*, vol. 34, no. 1 (Summer 2006), p. 13. Hereinafter: Berlet and Vysotsky, “Overview.”

⁸⁶ Leonard Zeskind, *Blood and Politics: The History of the White Nationalist Movement from the Margins to the Mainstream* (New York: Farrar, Straus, and Giroux, 2009), p. 40. Hereinafter: Zeskind, *Blood and Politics*.

⁸⁷ Rory McVeigh, “Structured Ignorance and Organized Racism in the United States,” *Social Forces*, vol. 82, no. 3 (March 2004), pp. 898-899.

⁸⁸ Anti-Defamation League, *Guidebook*, p. 16. Lane died in 2007 while serving 190 years in prison for his involvement with a terrorist group named the Order. See “Founder of Terrorist Group Dies in Prison,” *Terre Haute Tribune-Star*, May 29, 2007, <http://tribstar.com/local/x1155692948/Founder-of-terrorist-group-dies-in-prison>. Among other writings, Lane also drafted an influential racist ideological tract titled *The 88 Precepts*.

⁸⁹ Anti-Defamation League, *Guidebook*, p. 15.

He also encouraged tying neo-Nazism to religion, and some of his followers took up the obscure creed of Christian Identity.⁹⁰

Conflict and Conspiracy

Aside from racial superiority, a dualistic view of the world, and neo-Nazism, at least two other broad concepts shape white supremacy in the United States. They are the inevitability of violent conflict, and a belief that conspiracies hostile to white supremacy shape the existing world.⁹¹ It can be said that WSE broadly shares these concepts with the militia movement (discussed below).

The FBI has stated that white supremacists “commonly anticipate” waging war against their opponents.⁹² For example, the inevitability of RAHOWA—an acronym for “racial holy war”—is a central tenet of the neo-Nazi Creativity Movement, which has its roots in the Church of the Creator, a racist group founded by Ben Klassen in 1973.⁹³ Klassen, who committed suicide in 1993, argued that whites had no choice but to wage war against non-whites.⁹⁴ Likewise, some white supremacists use racism to interpret apocalyptic imagery from Norse mythology embodied in Odinism.⁹⁵ Most Odinists are not racists, however.⁹⁶

Conspiracism has been defined as “the idea that most major historic events have been shaped by vast, long-term, secret conspiracies that benefit elite groups and individuals.”⁹⁷ Conspiracy theories are not the province of a particular movement or group. Regardless, conspiracy theories can particularly shape the outlooks and actions of white supremacist extremists. Media sources

⁹⁰ Fredrick J. Simonelli, “The Neo-Nazi Movement,” Southern Poverty Law Center, <http://www.splcenter.org/get-informed/intelligence-files/ideology/neo-nazi/the-neo-nazi-movement>. See also: Charles S. Clark, “An American Nazi’s Rise and Fall,” *American History*, vol. 40, no. 6 (February 2006), pp. 60-66; Simonelli, “The American Nazi Party,” *Historian*, vol. 57, no. 3 (Spring 1995), pp. 553-566. A follower assassinated Rockwell in 1967. For information on Christian Identity, see Kevin Borgeson and Robin Valeri, *Terrorism in America* (Sudbury, MA: Jones and Bartlett, 2009), pp. 47-72; Martin Durham, “Christian Identity and the Politics of Religion,” *Totalitarian Movements and Political Religions*, vol. 9, no. 1 (March 2008), pp. 79-91; Tanya Telfair Sharpe, “The Identity Christian Movement: Ideology of Domestic Terrorism,” *Journal of Black Studies*, vol. 30, no. 4 (March 2000), pp. 604-623; Anti-Defamation League, “Christian Identity,” http://www.adl.org/learn/ext_us/Christian_Identity.asp?xpicked=4&item=Christian_ID.

⁹¹ Berlet and Vysotsky, “Overview,” pp. 12-13 highlights dualism, conspiracism, and apocalypticism as key themes.

⁹² The Bureau has noted that “warfare” is reflected in beliefs drawn from Christian Identity, the Creativity Movement, neo-Nazism, and Odinism. See Federal Bureau of Investigation, *White Supremacist Recruitment of Military Personnel since 9/11*, July 7, 2008, p. 4. Hereinafter: Federal Bureau of Investigation, *White Supremacist*.

⁹³ After Klassen’s 1993 death, the Church of the Creator was revived in an altered form by Matt Hale. For more information see Southern Poverty Law Center, “Church of the Creator,” <http://www.splcenter.org/get-informed/intelligence-files/groups/creativity-movement>. See also: Dobratz, “The Role,” p. 290; and Federal Bureau of Investigation, *White Supremacist*, p. 4.

⁹⁴ Ben Klassen, “RAHOWA: The Fighting Slogan of the White Race,” *Racial Loyalty*, no. 32 (February 1986), <http://www.archive.org/details/RahowaThisPlanetIsAllOurs>.

⁹⁵ Federal Bureau of Investigation, *White Supremacist*, p. 4. Odinism has been defined as either a combination of old Norse religion and Christianity or a belief system that draws exclusively on Nordic mythology. See Jonathan White, “Political Eschatology: A Theology of Antigovernment Extremism,” *The American Behavioral Scientist*, vol. 44, no. 6, (February 2001), p. 939.

⁹⁶ Berlet and Vysotsky, “Overview,” p. 30.

⁹⁷ Berlet and Vysotsky, “Overview,” p. 12. For more on conspiracy theories and terrorism see Jamie Bartlett and Carl Miller, *The Power of Unreason: Conspiracy Theories, Extremism, and Counter-Terrorism*, Demos, London, August 29, 2010. Bartlett and Miller (p. 24.) suggest that conspiracy theories “are one of a number of factors that can lead to extremism, and can turn extremism to violence.”

have stated that Richard Poplawski—convicted of shooting and killing three Pittsburgh police officers in April 2009—believed that a Zionist conspiracy controlled government and major corporations in the United States.⁹⁸

As in Poplawski's example, anti-Semitism plays a prominent role in the racist conspiracies of many white supremacists.⁹⁹ These people—as well as anti-government extremists—believe in something they call the Zionist Occupied Government (ZOG).¹⁰⁰ ZOG refers to the federal government, which adherents contend is “controlled or manipulated by international Jewish interests.”¹⁰¹ On its website, one WSE group has sold versions of a video game titled “ZOG's Nightmare.” Gameplay involves shooting nonwhites while being chased by a police agency controlled by Jews.¹⁰² Racists explain all sorts of personal or social grievances by invoking ZOG.¹⁰³ One scholar has described ZOG as

an omnipresent and omnipotent cabal involving at its heart varying constellations of Jews, Illuminati, Freemasons, plutocrats, and multinational corporations. It operates through many social ‘front’ institutions, from the United Nations to Parent-Teacher Associations.... ZOG can be used to explain not only the existence of affirmative action, environmental pollution, and pornography but also why a certain individual made poor grades in school, lost his job, or seems unable to find a partner.¹⁰⁴

According to adherents, ZOG is said to control the media, arts, religion, science, and education.¹⁰⁵

Recent Loss of Prominent Leaders

In the 1980s and 1990s, a small number of figures dominated white supremacist circles. They were intimately linked to their own relatively cohesive organizations. By the early 2000s, these groups fragmented as they lost their leaders. This fragmented situation likely persists. In fact, one study from 2006 has described “a recent crisis of leadership in the hate movement.”¹⁰⁶

Two particularly well-known white supremacist figures died in the last decade. William Pierce, head of the National Alliance died in 2002. Richard Butler, leader of Aryan Nations, died in 2004. Both Peirce and Butler articulated clear ideologies that attracted followers and drew upon

⁹⁸ Timothy McNulty, Paula Reed Ward and Sadie Gurman, “Jury Decides Poplawski Should Die for Killing 3 Officers,” *Pittsburgh Post-Gazette*, June 28, 2011. Hereinafter: McNulty et al., “Jury Decides.” See also: Anti-Defamation League, “Richard Poplawski: The Making of a Lone Wolf,” April 8, 2009, http://www.adl.org/learn/extremism_in_the_news/White_Supremacy/poplawski%20report.htm. Hereinafter: Anti-Defamation League, “Richard Poplawski.” Sean D. Hamill, “Man Accused in Pittsburgh Killings Voiced Racist Views Online,” *New York Times*, April 7, 2009, <http://www.nytimes.com/2009/04/07/us/07pittsburgh.html>. Hereinafter: Hamill, “Man Accused.”

⁹⁹ Berlet and Vysotsky, “Overview,” p. 13.

¹⁰⁰ Also seen as “Zionist Occupation Government.”

¹⁰¹ Institute for Intergovernmental Research, *Investigating Terrorism*, p. 93; Mattias Gardell, *Gods of the Blood: The Pagan Revival and White Separatism* (Durham, NC: Duke University Press, 2003), pp. 11, 54, 68-69. Hereinafter: Gardell, *Gods*.

¹⁰² Anti-Defamation League, *The National Socialist Movement*, http://www.adl.org/Learn/Ext_US/nsm/tactics.asp?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_America&xpicked=3&item=nsm.

¹⁰³ Gardell, *Gods*, p. 68.

¹⁰⁴ Ibid.

¹⁰⁵ Ibid.

¹⁰⁶ Jack Levin, *Domestic Terrorism* (New York: Infobase Publishing, 2006), pp. 48-49.

resources such as rural headquarters/compounds to sustain their organizations.¹⁰⁷ By the early 2000s, the National Alliance even had a substantial revenue stream estimated at \$1 million annually generated from a publishing company and record labels it owned as well as dues.¹⁰⁸ The deaths of Butler and Pierce exacerbated the downfall of both organizations. The decline of these groups also resulted from a number of other forces, such as infighting among members and pressure from law enforcement and watchdog groups.¹⁰⁹

Two prominent white supremacist movements are discussed below.

National Socialist Movement (NSM)

One white supremacist organization active in the United States is the National Socialist Movement (NSM). It has benefitted from the decline of these other groups as well as new leadership in the form of Jeff Schoep.¹¹⁰ The NSM also capitalized on the expansion of the Internet in the early 2000s. The group, which emerged in 1974, is a descendant of the American Nazi Party, and until the 1990s and early 2000s “it operated only on the fringes of the neo-Nazi movement.”¹¹¹ As of 2008, the group had around 500 members and close associates throughout the United States.¹¹² The NSM is flexible about membership, allowing its members to also participate in other white supremacist organizations.¹¹³

Individuals allegedly tied to the NSM at some point in their lives have run afoul of the law.

- In Minnesota in April 2012, Joseph Benjamin Thomas was indicted on drug-related charges, and Samuel James Johnson was indicted on weapons-related charges. Purportedly the two were tied to NSM—at one point Johnson had served as its leader in Minnesota. The duo had reportedly formed their own white supremacist group, gathering weapons and ammunition and planning to attack the government and other targets.¹¹⁴
- In January 2011, William White, a onetime member of the NSM and founder of his own white supremacist organization, was convicted¹¹⁵ of soliciting violence

¹⁰⁷ Freilich, Chermak, and Caspi, “Critical Events,” 511.

¹⁰⁸ *Ibid.*, pp. 512, 513.

¹⁰⁹ *Ibid.*, p. 516.

¹¹⁰ Anti-Defamation League, *American Stormtroopers: Inside the National Socialist Movement*, (2008), p. 3. Hereinafter: Anti-Defamation League, *American Stormtroopers*.

¹¹¹ *Ibid.*

¹¹² *Ibid.*

¹¹³ Southern Poverty Law Center, “National Socialist Movement,” <http://www.splcenter.org/get-informed/intelligence-files/groups/national-socialist-movement>.

¹¹⁴ Department of Justice, press release, “Mendota Heights Man Indicted for Distributing Methamphetamine,” April 27, 2012, <http://www.fbi.gov/minneapolis/press-releases/2012/mendota-heights-man-indicted-for-distributing-methamphetamine>; Department of Justice, press release, “Austin Felon Indicted for Possessing Firearms,” April 27, 2012, <http://www.fbi.gov/minneapolis/press-releases/2012/austin-felon-indicted-for-possessing-firearms>; Amy Forliti, “Affidavit: 2 Men With Supremacist Ties Had Weapons,” *Associated Press*, April 27, 2012, <http://abcnews.go.com/US/wireStory/affidavit-men-supremacist-ties-weapons-16229960?singlePage=true#.T6LAcdVVLts>.

¹¹⁵ Department of Justice, press release, “Self-Proclaimed White Supremacist William White Convicted of Soliciting Violence Against Hale Jury Foreman,” January 5, 2011, <http://www.fbi.gov/chicago/press-releases/2011/cg010511a.htm>.

online against the jury foreman in *U.S. v. Matthew Hale*.¹¹⁶ In April 2011, a federal judge reversed White's conviction. The judge ruled that prosecutors had failed to prove that White actually intended to harm the foreman and that White's web posting regarding the foreman was protected by the First Amendment.¹¹⁷ In an unrelated case, in December 2009, White was convicted of four counts of communicating threats in interstate commerce and one count of witness intimidation. One of the convictions for communicating threats in interstate commerce was later reversed.¹¹⁸ The witness intimidation charges involved White reportedly attempting to "delay or prevent the testimony" of African Americans in a discrimination case.¹¹⁹ According to publicly available information, in 2005 and 2006 White was involved with NSM, for a time serving as its national spokesman.¹²⁰ His activity with NSM ceased after he had a falling out with Schoep.¹²¹

¹¹⁶ Matthew Hale was convicted of soliciting the murder of U.S. District Judge Joan Humphrey Lefkow. In the mid 1990s, Hale revived the Church of the Creator fortunes. He changed the organization's name to the World Church of the Creator, and according to a watchdog group, by 2002 it had more chapters in the United States than any other neo-Nazi organization. Judge Lefkow had originally ruled in favor of Hale in a trademark infringement case involving the name "World Church of the Creator." Her ruling was reversed on appeal, and as a result, she had to enforce the higher court's reversal. Via email and during a conversation, Hale discussed with his security chief the idea of killing Lefkow. Hale did not know that his security chief was an FBI informant. In 2003, Hale was arrested for soliciting the murder of Judge Lefkow, and this, as well as his subsequent conviction on charges related to the case, hastened a downturn in fortune for his World Church of the Creator. Hale is serving a 40-year prison term. After another name change, the group—currently known simply as the Creativity Movement—shows signs of revival under new leadership. See Michael, *Theology of Hate*, pp. 120-133, 173-188; Southern Poverty Law Center, "Creativity"; Chris Dettro, "Follow-Up File: White Supremacist Finds Quiet Life in Prison," *The State Journal-Register*, Springfield, IL, October 25, 2010; Larry Keller, "From the Ashes," *Intelligence Report*, Southern Poverty Law Center, no. 140 (winter 2010), pp. 12-14; Federal Bureau of Investigation, "A Different Breed of Terrorist," June 6, 2004, <http://www.fbi.gov/news/stories/2004/june/hale060904>.

¹¹⁷ Laurence Hammack, "Judge Tosses William A. White Verdict," *The Roanoke Times*, April 20, 2011, <http://www.roanoke.com/news/roanoke/wb/283883>.

¹¹⁸ Department of Justice, press release, "Roanoke, Virginia Neo-Nazi Sentenced for Threats, Witness Intimidation," April 14, 2010, <http://www.justice.gov/opa/pr/2010/April/10-crt-410.html>.

¹¹⁹ Ibid.

¹²⁰ Laurence Hammack, "White's Life on Fringe Puts Him at Center of Storm," *The Roanoke Times*, July 26, 2009, <http://www.roanoke.com/news/roanoke/wb/213109>.

¹²¹ Ibid; Southern Poverty Law Center, "Bill White," 2011, <http://www.splcenter.org/get-informed/intelligence-files/profiles/bill-white>. For other cases involving individuals allegedly tied to NSM, see Department of Justice, press release, "Valley Man Enters Guilty Plea for Possession and Transport of an Improvised Explosive Device," September 27, 2011, http://www.fbi.gov/phoenix/press-releases/2011/valley-man-enters-guilty-plea-for-possession-and-transport-of-an-improvised-explosive-device?utm_campaign=email-Immediate&utm_medium=email&utm_source=phoenix-press-releases&utm_content=34188; Department of Justice, press release, "Valley Man Indicted for Possessing and Transporting Improvised Explosive Devices," January 26, 2011, <http://phoenix.fbi.gov/dojpressrel/pressrel11/px012611.htm>; Rudabeh Shahbazi, "Documents Show Apache Junction Man Planned To Take IEDs to the Border," *ABC 15*, http://www.abc15.com/dpp/news/region_southeast_valley/apache_junction/documents-show-apache-junction-man-planned-to-take-ieds-to-the-border; Federal Bureau of Investigation, "Domestic Terrorism: Tip Leads to Sting, Prison for Plotter," November 29, 2006, http://www.fbi.gov/news/stories/2006/november/terror_112906.

Racist Skinheads

In the United States, racist skinheads have a legacy stretching back to the early 1980s.¹²² However, skinhead culture originated in the United Kingdom in the late 1960s and today has a global reach.¹²³ Since the early 2000s, the movement in the United States has been characterized by a proliferation of regional groups or crews rather than a united core organization.¹²⁴ In law enforcement circles, racist skinheads have a reputation for violence. This is “reinforced by hate-filled white power music and literature.” “[T]hey foster [their reputed toughness] through their appearance (shaved heads or close-cropped hair, white power tattoos) and dress (bomber jackets, ‘braces’ (suspenders), steel-toed boots).”¹²⁵

Skinheads emerged as a non-racist movement among British working-class youth in the late 1960s. These early skinheads rejected the hippie lifestyle and embraced elements of Jamaican culture, particularly reggae and ska music. As immigration from South Asia to the U.K. grew, some white British skinheads embraced racism and neo-Nazism. This racist skinhead variant of the subculture materialized in the U.S. Midwest and in Texas in the early 1980s.¹²⁶

In the mid-1990s, many U.S.-based racist skinhead groups allied with one another to form the Hammerskin Nation (HSN). HSN eventually developed chapters throughout the United States and in Europe. It had its own annual meeting/concert called Hammerfest, ran a record label, and had a publishing company. In the early 2000s, other groups such as the Outlaw Hammerskins, Hoosier State Hammerskins, and Ohio State Skinheads challenged HSN for preeminence. These groups saw HSN as “elitist.”¹²⁷ In 2011, by one measure, 133 skinhead groups were active in the United States.¹²⁸

In January 2010, the FBI released a bulletin that, among other things, emphasized that some racist skinheads formed the most violent segment of WSE adherents.¹²⁹ This supported the findings in a 2008 FBI assessment.¹³⁰ Between 2007 and 2009, skinheads were involved in 36 of the 53 violent incidents the FBI identified in the United States as being tied to WSE proponents.¹³¹ The Bureau has stated that “violence is an integral part of the racist skinhead subculture.”¹³² Elements within

¹²² Southern Poverty Law Center, *Skinheads in America: Racists on the Rampage*, p. 3, http://www.splcenter.org/sites/default/files/downloads/publication/Skinhead_Report.pdf. Hereinafter: Southern Poverty Law Center, *Skinheads*.

¹²³ Ibid.

¹²⁴ Ibid., p. 13; Federal Bureau of Investigation, *Rage and Racism*, p. 8.

¹²⁵ Federal Bureau of Investigation, *Rage and Racism*, pp. 5-6.

¹²⁶ Michael R. Ronczkowski, *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*, 2nd ed. (Boca Raton, FL: CRC Press, Taylor and Francis Group, 2007), pp. 40-41. Hereinafter: Ronczkowski, *Terrorism*. Southern Poverty Law Center, *Skinheads*, pp. 3-4.

¹²⁷ Southern Poverty Law Center, *Skinheads*, p. 5.

¹²⁸ See Mark Potok, “The Year in Hate and Extremism,” *Intelligence Report*, Southern Poverty Law Center, no. 145 (Spring 2012), p. 46. Hereinafter: Potok, “The Year.” Potok notes that this count of skinhead groups “understates their numbers” because “skinheads are migratory and often not affiliated with groups.”

¹²⁹ Federal Bureau of Investigation, *White Supremacist Extremist Violence Possibly Decreases But Racist Skinheads Remain the Most Violent*, January 28, 2010. Hereinafter: Federal Bureau of Investigation, *White Supremacist Extremist Violence*.

¹³⁰ Federal Bureau of Investigation, *Rage and Racism: Skinhead Violence on the Far Right*, December 10, 2008. Hereinafter: Federal Bureau of Investigation, *Rage and Racism*.

¹³¹ Federal Bureau of Investigation, *White Supremacist Extremist Violence*, p. 4.

¹³² Federal Bureau of Investigation, *Rage and Racism*, p. 5.

the fractious movement even target one another.¹³³ These criminal acts are typically unrehearsed and opportunistic, targeting nonwhites and “other religious and social minorities.”¹³⁴

An apparent recent exception involved greater levels of planning. One man was convicted and two others pled guilty in a Connecticut case that involved the illegal sale of firearms and homemade grenades. The scheme included multiple meetings between late 2008 and early 2010 to negotiate the transactions, prepare the firearms, and assemble the grenades. The trio was tied to a skinhead group known as Battalion 14 (originally called the Connecticut White Wolves). They sold the weapons to a convicted felon working as an FBI cooperating witness. The informant posed as a member of the Imperial Klans of America, a Ku Klux Klan organization. Two others in the case, including the leader of Battalion 14 and a man not tied to the group, were acquitted of charges.¹³⁵

Anti-Government Extremists

As mentioned above, DOJ considers both unauthorized militias and sovereign citizens as anti-government extremists. *Neither militia membership nor advocacy of sovereign citizen tenets makes one a terrorist or a criminal.* However, in some instances both militia members and sovereign citizens have committed crimes driven in part by their ideologies.

Militia Extremists

The militia movement emerged in the 1990s as a collection of armed, paramilitary groups formed to stave off what they perceived as intrusions of an invasive government.¹³⁶ Central to this is a fear of firearm confiscation by a federal government thought to be out of control. Some adherents also believe in anti-Semitic and racist ideologies.¹³⁷ Regardless, most militia members engage in constitutionally protected activity.

Militia groups typically coalesce around a specific leader. Groups can run training compounds where they rehearse paramilitary tactics, practice their survival skills, and receive weapons instruction and lessons in movement ideology. Some militia groups also maintain websites for recruitment and fundraising.¹³⁸ Extremists within the movement who run afoul of law

¹³³ Southern Poverty Law Center, *Skinheads*, pp. 5, 16.

¹³⁴ Federal Bureau of Investigation, *Rage and Racism*, p. 5.

¹³⁵ Department of Justice, press release, “Milford Man Sentenced to 10 Years in Prison for Making Grenades and Selling Guns Intended for White Supremacist Group,” May 5, 2011, <http://newhaven.fbi.gov/dojpressrel/pressrel11/nh050511.htm>; Michael P. Mayko, “Two Acquitted in White Wolves Conspiracy Case,” *Connecticut Post*, December 2, 2010, <http://www.ctpost.com/local/article/Two-acquitted-in-White-Wolves-conspiracy-case-850538.php>; Michael P. Mayko, “White Wolves Called ‘Home Grown Terrorists,’” *Connecticut Post*, November 16, 2010, <http://www.ctpost.com/news/article/White-Wolves-called-home-grown-terrorists-812091.php>; Anti-Defamation League, “Connecticut White Supremacists Indicted on Firearms and Explosives Charges,” March 24, 2010; http://www.adl.org/learn/extremism_in_the_news/White_Supremacy/ct_arrets_batallian_14.htm?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_the_News.

¹³⁶ Institute for Intergovernmental Research, *Investigating Terrorism and Criminal Extremism: Terms and Concepts*, Version 1.0, (Tallahassee, Florida: Institute for Intergovernmental Research, 2005), p. 49; Hereinafter: Institute for Intergovernmental Research, *Investigating Terrorism*.

¹³⁷ Arizona Counter-Terrorism Information Center, “Sovereign Citizens and Militia Information,” August 19, 2008, p. 1.

¹³⁸ Lane Crothers, “The Cultural Foundations of the Modern Militia Movement,” *New Political Science*, vol. 24, no. 2 (continued...)

enforcement “tend to stockpile illegal weapons and ammunition, trying illegally to get their hands on fully automatic firearms or attempting to convert weapons to fully automatic. They also try to buy or manufacture improvised explosive devices.”¹³⁹

Segments of the militia movement believe that the U.S. government is either run by some hidden conspiracy or is an overreaching sham. Some see a “New World Order” controlling U.S. institutions such as the media and the federal government. They contend that this is partly fostered by international organizations such as the United Nations. From this perspective, these organizations sap American sovereignty. Some militia supporters believe that agents of an unauthentic “Shadow Government” are interested in seizing lawfully owned firearms as part of a plan to undermine democracy.¹⁴⁰ Importantly, others in the militia movement hold that the federal government has overstepped its constitutional bounds.¹⁴¹ One scholar has noted that some militia members assert that they have “the right to organize, purchase and use firearms, and enforce the law against agents of the government who behave unconstitutionally.”¹⁴²

A small minority of Americans who held anti-government fears formed militias largely in response to two incidents in the early 1990s. These were confrontations between federal law enforcement and private citizens at Ruby Ridge, ID, and at a site near Waco, TX.¹⁴³ Both involved warrants related to firearms violations.

- In August 1992, Randy Weaver and his family were engaged in an 11-day standoff with federal law enforcement agents. Randy Weaver had failed to appear in court on firearms-related charges in 1991. Subsequently, an unsuccessful operation to arrest Weaver led to the death of his 14-year-old son and a U.S. Marshal. It also precipitated the standoff. During the standoff, Weaver and a friend were shot and wounded. An FBI sniper also shot and killed Weaver’s wife, Vicki.¹⁴⁴ Weaver was eventually found guilty of failing to appear in court on the gun charges that played a role in the standoff. In October 1993, he was sentenced to 18 months in jail and a \$10,000 fine. In 1995, Weaver received a \$3.1 million settlement in a wrongful death suit filed against the U.S. government.¹⁴⁵ The

(...continued)

(2002), p. 231. Hereinafter: Crothers, “The Cultural.”

¹³⁹ Federal Bureau of Investigation, “Domestic Terrorism: Focus on Militia Extremism,” September 22, 2011, http://www.fbi.gov/news/stories/2011/september/militia_092211/militia_092211.

¹⁴⁰ Lane Crothers, *Rage on the Right: The American Militia Movement from Ruby Ridge to Homeland Security* (Lanham, MD: Rowman and Littlefield, 2003), p. 57. Hereinafter: Crothers, *Rage on the Right*.

¹⁴¹ Crothers, “The Cultural,” pp. 226-228.

¹⁴² *Ibid.*, p. 228.

¹⁴³ *Ibid.*, pp. 230-231. See also: Michael Barkun, “Appropriated Martyrs: The Branch Davidians and the Radical Right,” *Terrorism and Political Violence*, vol. 19, no. 1 (2007), p. 120. Hereinafter: Barkun, “Appropriated Martyrs.” See also: Steven M. Chermak, *Searching for a Demon: The Media Construction of the Militia Movement*, (Boston: Northeastern University Press, 2002).

¹⁴⁴ Stuart A. Wright, *Patriots, Politics, and the Oklahoma City Bombing* (New York: Cambridge University Press, 2007), pp. 142-148. Hereinafter: Wright, *Patriots*. Weaver has been described as a survivalist who believed in the Christian Identity religion. See Barkun “Appropriated Martyrs,” p. 118. He has also been described as holding white supremacist beliefs and was not a militia member. See Crothers, *Rage on the Right*, pp. 78-79.

¹⁴⁵ Crothers, *Rage on the Right*, p. 90.

events at Ruby Ridge helped precipitate the militia movement, whose members tend to view Randy Weaver as a hero and demonize the federal government.¹⁴⁶

- The militia movement also emerged because of the 51-day standoff between federal law enforcement and a religious sect named the Branch Davidians near Waco.¹⁴⁷ On February 28, 1993, an unsuccessful attempt by ATF agents to arrest the sect's leader, David Koresh, initiated the events near Waco. He was wanted on suspicion of federal firearms and explosives violations.¹⁴⁸ Four ATF agents and six Branch Davidians died in a gunfight during the operation.¹⁴⁹ Protracted discussions followed between federal negotiators and Koresh. These failed. On April 19, federal agents assaulted the Davidian compound, which caught on fire. At least 75 Branch Davidians perished in the assault.¹⁵⁰

If the incidents involving the Weavers and the Branch Davidians helped form the militia movement, Timothy McVeigh's bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, helped usher in a temporary decline.¹⁵¹ In the bombing's aftermath, militia groups received greater law enforcement scrutiny.¹⁵² The bombing claimed 168 lives, and until 9/11 was the largest single act of terrorism on U.S. soil. The militia movement included 441 groups in 1995. By 2000, this number was reportedly down to 72.¹⁵³ Although McVeigh's bombing cannot fully account for a dip in militia activity, it impacted the movement by causing some groups to temper their rhetoric while others grew more extreme, and militias became more marginalized.¹⁵⁴

The militia movement has experienced a recent resurgence. One watchdog group has attributed this partly to a rise in anti-government anger since 2008.¹⁵⁵ According to another organization, the number of militias in the United States jumped from 42 in 2008 to 334 in 2011 (see **Figure 1**). The recent resurgence may exhibit a key difference from its precursor. Social networking websites have encouraged looser organization of smaller, largely web-based cells.¹⁵⁶

Several examples highlight how some militia adherents have allegedly engaged in criminal activity since 9/11.

¹⁴⁶ Wright, *Patriots*, pp. 149-152; Crothers, *Rage on the Right*, pp. 92-97; Barkun, "Appropriated Martyrs," pp. 120-121.

¹⁴⁷ Crothers, *Rage on the Right*, p. 104.

¹⁴⁸ Department of Justice, *Report to the Deputy Attorney General on the Events at Waco, Texas*, October 8, 1993, <http://www.justice.gov/publications/waco/wacoexec.html>. The Branch Davidian sect emerged from the Seventh-Day Adventist Church and was formed in 1929. The two severed official ties with one another in 1934. David Koresh was not a militia member. See Crothers, *Rage on the Right*, pp. 100-101.

¹⁴⁹ Crothers, *Rage on the Right*, p. 105.

¹⁵⁰ Crothers, *Rage on the Right*, p. 110.

¹⁵¹ McVeigh was not a militia member, but he interacted with others who were.

¹⁵² Devlin Barrett and Eileen Sullivan, "FBI Sees Little Chance of Copycat Militia Plots," *Associated Press*, March 31, 2010.

¹⁵³ Potok, "The Year," p. 42.

¹⁵⁴ Crothers, *Rage on the Right*, p. 138, 147.

¹⁵⁵ Anti-Defamation League, *Rage Grows in America: Anti-Government Conspiracies, the Resurgence of the Militia Movement*, November 16, 2009, http://www.adl.org/special_reports/rage-grows-in-America/militia-movement.asp.

¹⁵⁶ *Ibid.*

- In November 2011, the FBI arrested four retirees, Samuel J. Crump, Ray H. Adams, Dan Roberts, and Frederick W. Thomas, who allegedly formed a fringe militia group and planned violent attacks on government officials. The group, based in northern Georgia, purportedly had ties to an unnamed militia organization. According to DOJ, the quartet “discussed multiple criminal activities, ranging from murder; theft; manufacturing and using toxic agents; and assassinations in an effort to undermine federal and state government and to advance their interests.”¹⁵⁷ Between June and November 2011, Roberts and Thomas met with an FBI undercover agent to negotiate the purchase of matériel for the plot: “a silencer for a rifle and conversion parts to make a fully automatic rifle, as well as explosives.”¹⁵⁸ In October, plotters reportedly discussed making ricin, a deadly poison derived from castor beans.¹⁵⁹ In April 2012, Roberts and Thomas pled guilty to conspiring to obtain an unregistered explosive device and silencer.¹⁶⁰
- In March 2011 and January 2012, four individuals were indicted in Anchorage, AK, on federal conspiracy and firearms charges.¹⁶¹ They were members of the Alaska Peacemaker’s Militia based in Fairbanks and also held sovereign citizen beliefs (described elsewhere in this report). The purported leader of the group, Francis “Schaeffer” Cox, and his followers allegedly plotted “a potential retaliatory response to any attempt by law enforcement to arrest Cox, who had an outstanding bench warrant for not attending a trial over a misdemeanor weapons charge.”¹⁶² The plotters supposedly codenamed their plan “241 (two for one),” because they reputedly intended to kill two government officials for every militia member killed in the operation.¹⁶³ DOJ has indicated that two of the indicted militia members also plotted to murder a federal district judge and an Internal

¹⁵⁷ Department of Justice, press release, “North Georgia Men Arrested, Charged in Plots to Purchase Explosives, Silencer and to Manufacture a Biological Toxin,” November 1, 2011, <http://www.fbi.gov/atlanta/press-releases/2011/north-georgia-men-arrested-charged-in-plots-to-purchase-explosives-silencer-and-to-manufacture-a-biological-toxin>.

¹⁵⁸ Ibid.

¹⁵⁹ Craig Schneider, “Documents: Men with Castor Beans, Guns Worried about Getting Caught,” *Atlanta Journal-Constitution*, November 6, 2011, <http://www.ajc.com/news/documents-men-with-castor-1218644.html>.

¹⁶⁰ Department of Justice, press release, “North Georgia Men Plead Guilty to Plot to Purchase Explosives and a Silencer,” April 10, 2012, http://www.fbi.gov/atlanta/press-releases/2012/north-georgia-men-plead-guilty-to-plot-to-purchase-explosives-and-a-silencer?utm_campaign=email-Immediate&utm_medium=email&utm_source=atlanta-press-releases&utm_content=86514.

¹⁶¹ Department of Justice, press release, “Superseding Indictment Returned by Federal Grand Jury Against Fairbanks-Area Men for Conspiracy to Kill Federal Officers,” January 23, 2011, <http://www.fbi.gov/anchorage/press-releases/2012/superseding-indictment-returned-by-federal-grand-jury-against-fairbanks-area-men-for-conspiracy-to-kill-federal-officers>; Department of Justice, press release, “Couple Charged with Conspiracy to Murder Judge and Federal Firearms Crimes, Two Others Indicted for Conspiracy to Possess Destructive Devices and Illegal Weapons,” March 17, 2011, <http://www.fbi.gov/anchorage/press-releases/2011/couple-charged-for-conspiracy-to-murder-judge-and-federal-firearms-crimes>. Hereinafter: Department of Justice, “Couple Charged.”

¹⁶² Sam Friedman, “Details Emerge in Alleged Plot to Kill Alaska State Troopers, Judge,” *Fairbanks Daily News-Miner*, March 3, 2011, http://www.newsminer.com/view/full_story/12322747/article-Details-emerge-in-alleged-plot-to-kill-Alaska-State-Troopers—judge?instance=home_news_window_left_top_2. Hereinafter: Friedman, “Details Emerge.” Cox has also been described as a sovereign citizen (discussed below). See Sam Friedman, “The Schaeffer Cox File: The Trail of a Young Man,” *Fairbanks Daily News-Miner*, April 10, 2011, http://www.newsminer.com/view/full_story/12739189/article-The-Schaeffer-Cox-File—The-trail-of-a-young-man?instance=home_most_popular2.

¹⁶³ Ibid.

Revenue Service (IRS) employee.¹⁶⁴ A fifth individual has been arrested in connection with the plot.¹⁶⁵

The above alleged activities are not necessarily indicative of trends toward violence in the larger militia movement, and in one prominent case, DOJ failed to convince the presiding judge of serious charges revolving around a purported violent plot. In March 2012, a federal judge acquitted members of a Michigan Militia group known as the Hutaree on charges of seditious conspiracy or rebellion against the United States and conspiring to use weapons of mass destruction. The judge also cleared the accused Hutaree members of weapons crimes related to the conspiracies.¹⁶⁶

The case garnered headlines in March 2010, when nine Hutaree members were indicted for allegedly preparing to violently confront U.S. law enforcement.¹⁶⁷ Their supposed plotting included the murder of a local law enforcement officer and an attack on fellow officers who gathered in Michigan for the funeral procession. According to DOJ, the Hutaree discussed the use of explosives against the funeral procession.¹⁶⁸ Audio recordings by an undercover FBI agent of reputed Hutaree leader David Brian Stone capture him discussing the New World Order and how, “it’s time to strike and take our nation back so we will be free of tyranny.... The war will come whether we are ready or not.”¹⁶⁹ According to DOJ, the group had a hit list that included federal judges, among others.¹⁷⁰ However, during the trial an Assistant U.S. Attorney acknowledged that the Hutaree had not formed a “specific plan” to attack government targets.¹⁷¹ U.S. District Judge Victoria Roberts stated that, “The court is aware that protected speech and mere words can be

¹⁶⁴ Department of Justice, “Couple Charged.”

¹⁶⁵ Friedman, “Details Emerge.” For examples of other militia adherents involved in crime, see Meghann M. Cuniff, “Health Problems Reduce Militia Leader’s Sentence,” *The Spokesman-Review*, August 11, 2011, <http://www.spokesman.com/stories/2011/aug/11/health-problems-reduce-militia-leaders-sentence/>; Bill Morlin, “Idaho Militia Leader Sentenced for Weapons, Bombs,” *Hatewatch*, Southern Poverty Law Center, August 9, 2011, <http://www.splcenter.org/blog/2011/08/09/idaho-militia-leader-sentenced-for-weapons-bombs/?ondntsrc=MBQ110870HTW&newsletter=HW081111>; David Cole, “Militia Member Sentenced on Federal Firearms and Explosives Charges,” *Coeur d’Alene Press*, August 9, 2011, http://www.cdapress.com/news/local_news/article_0cb55774-c2dc-11e0-9136-001cc4c03286.html; Federal Bureau of Investigation, “Preventing Terrorist Attacks on U.S. Soil: The Case of the Wrong Package Falling into the Right Hands,” April 9, 2004, <http://www.fbi.gov/news/stories/2004/april/krar040904>; Scott Gold, Case Yields Chilling Signs of Domestic Terror Plot,” *Los Angeles Times*, January 7, 2004.

¹⁶⁶ Ed White, “Michigan Militia Members Cleared of Conspiracy,” *Associated Press*, March 27, 2012, http://abcnews.go.com/US/wireStory/critical-charges-dropped-michigan-militia-16013255?singlePage=true#T3MB5kd_lLc. Hereinafter: White, “Michigan Militia.”

¹⁶⁷ Department of Justice, press release, “Nine Members of a Militia Group Charged with Seditious Conspiracy and Related Charges,” March 29, 2010, <http://www.fbi.gov/detroit/press-releases/2010/de032910.htm>.

¹⁶⁸ Ibid.

¹⁶⁹ Corey Williams and Jeff Karoub, “Prosecutor: Undercover FBI Agent Infiltrated Militia,” *Associated Press*, March 31, 2010.

¹⁷⁰ Dan Harris, Emily Friedman, and Tahman Bradley, “Undercover Agent Key Witness Against Hutaree Militia Members,” *ABC News*, April 1, 2010, <http://abcnews.go.com/GMA/undercover-agent-credited-hutaree-militia-bust/story?id=10257584>.

¹⁷¹ Robert Snell and Christine Ferretti, “Key Charges Dropped Against Hutaree Militia,” *Detroit News*, March 28, 2011, <http://www.detroitnews.com/article/20120328/METRO/203280376/Key-charges-dropped-against-Hutaree-militia?odyssey=mod|newswell|text|FRONTPAGE|s>.

sufficient to show a conspiracy. In this case, however, they do not rise to that level.”¹⁷² Three Hutaree members pled guilty to firearms charges.¹⁷³

Sovereign Citizen Movement

The FBI defines the sovereign citizen movement as “anti-government extremists who believe that even though they physically reside in this country, they are separate or ‘sovereign’ from the United States. As a result, they do not accept any government authority, including courts, taxing entities, motor vehicle departments, or law enforcement.”¹⁷⁴ However, simply holding these views is not a criminal act, and numerous movement adherents solely exercise their beliefs via constitutionally protected activities.

The ideas behind the movement originated during the 1970s with a group known as the Posse Comitatus and enjoyed some popularity in extremist circles during the 1980s and 1990s.¹⁷⁵ Early on, the movement featured white supremacist elements, but this has not kept some African Americans from subscribing to its ideals in recent years.¹⁷⁶ In the 1990s, the movement attracted 250,000 followers and was marked by the FBI’s standoff with a group known as the Montana Freeman that lasted 81 days.¹⁷⁷ Current estimates suggest a membership of 300,000.¹⁷⁸

For the most part, the sovereign citizen movement is diffuse and includes few organized groups.¹⁷⁹ The FBI suggests that sovereigns “operate as individuals without established leadership

¹⁷² White, “Michigan Militia.”

¹⁷³ See Department of Justice, Press Release, “Members of the Hutaree Militia Plead Guilty to Weapons Charges,” March 29, 2012, http://www.fbi.gov/detroit/press-releases/2012/members-of-the-hutaree-militia-plead-guilty-to-weapons-charges?utm_campaign=email-Immediate&utm_medium=email&utm_source=detroit-press-releases&utm_content=83489; Matthew Dolan, “Defendant in Michigan Militia Case Changes Plea to Guilty,” December 6, 2011, http://online.wsj.com/article/SB10001424052970204083204577080630555077796.html?mod=googlenews_wsj. When the Hutaree suspects were arrested in the case, some militia members in Michigan did not support the group’s alleged scheming. For example, a member of another militia group in Michigan provided information to authorities regarding the whereabouts of a fugitive Hutaree militia member. See Kirk Johnson, “Militia Draws Distinctions Between Groups,” *New York Times*, March 31, 2010, <http://www.nytimes.com/2010/04/01/us/01michigan.html>. Also, a militia leader from Michigan has said that the Hutaree case, “caused a rift in the militia movement about whether this is the sort of group we want to rally behind or if what they were doing was outside the scope of what’s acceptable.” See Robert Snell, “Militias Split over Defending Hutaree,” *Detroit News*, March 31, 2011.

¹⁷⁴ Federal Bureau of Investigation, “Domestic Terrorism: The Sovereign Citizen Movement,” April 13, 2010, http://www.fbi.gov/news/stories/2010/april/sovereigncitizens_041310. Hereinafter: Federal Bureau of Investigation, “Sovereign Citizen.”

¹⁷⁵ Anti-Defamation League, “Sovereign Citizen Movement,” http://www.adl.org/learn/ext_us/scm.asp?xpicked=4; Casey Sanchez, “Return of the Sovereigns,” *Intelligence Report*, Southern Poverty Law Center, no. 133 (spring 2009), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2009/spring/return-of-the-sovereigns>.

¹⁷⁶ Sarah Netter, “Anti-Government Sovereign Citizens Taking Foreclosed Homes Using Phony Deeds, Authorities Say,” *ABC News*, August 23, 2010, <http://abcnews.go.com/US/georgia-battling-sovereign-citizens-squatting-foreclosed-homes/story?id=11445382>. See Leah Nelson, “Sovereigns in Black,” *Intelligence Report*, Southern Poverty Law Center, no. 143 (Fall 2011), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2011/fall/-sovereigns-in-black>.

¹⁷⁷ Patrik Jonsson, “‘Sovereign citizens’: Is Jared Loughner a sign of revived extremist threat?” *Christian Science Monitor*, March 9, 2011, <http://www.csmonitor.com/USA/2011/0309/Sovereign-citizens-Is-Jared-Loughner-a-sign-of-revived-extremist-threat>.

¹⁷⁸ *Ibid.*

¹⁷⁹ One sovereign citizens group is the “Republic for the united States of America” (RuSA) which is based in Alabama. RuSA is a successor to a group known as the Guardians of the Free Republics (GFR), which in 2010 mailed letters to the governors of all 50 U.S. states urging them to leave office. See Southern Poverty Law Center, “Sovereign (continued...)”

and only come together in loosely affiliated groups to train, help each other with paperwork [critical to some of their schemes], or socialize and talk about their ideology.”¹⁸⁰ The movement involves leaders described as “gurus” who proselytize online, in print publications, or via in-person seminars. These gurus rouse followers into believing a conspiracy theory in which the legitimate federal government has been replaced by a government designed to take away the rights of ordinary citizens.¹⁸¹ This shares the same broad interplay between concepts of legitimate and illegitimate rule seen in the New World Order and WSE theories about ZOG. Gurus can also promote illegal techniques that individuals can use to supposedly cut their ties to the federal government or avoid its reach, particularly when it comes to taxation.¹⁸²

Sovereign citizens reject the legitimacy of much of the U.S. legal system.¹⁸³ Many believe that the 14th Amendment “shifted the nation from its original common-law roots with states’ rights to a federal corporation that legally enslaved everyone.”¹⁸⁴ According to movement members, the amendment ushered in an illegitimate federal government by supposedly abrogating individual rights and replacing them with a system that “grant[ed] privileges through contracts such as marriage and driver’s licenses, gun permits, and property codes.”¹⁸⁵

By ignoring all sorts of laws, avoiding taxes, disregarding permit requirements, and destroying government-issued identification documents, some sovereign citizens have tried to cut formal ties with what they perceive as an illegitimate regime.¹⁸⁶ Sovereigns have filed court documents stating that they are not U.S. citizens.¹⁸⁷ They have also created bogus financial documents to harass or defraud their enemies. (For more information, see the “Paper Terrorism”: Liens, Frivolous Lawsuits, and Tax Schemes” section in this report).

Sovereign citizens have in some instances created fictitious entities and used fake currency, passports, license plates, and driver licenses. In 2009, a federal jury found three men guilty of conspiring to use and sell fraudulent diplomatic credentials and license plates that they believed allowed “their customers [to] enjoy diplomatic immunity and [to] no longer ... pay taxes or be

(...continued)

President,” *Intelligence Report*, Southern Poverty Law Center, no. 143 (Fall 2011), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2011/fall/-sovereign-president>.

¹⁸⁰ Federal Bureau of Investigation, Counterterrorism Analysis Section, “Sovereign Citizens: A Growing Domestic Threat to Law Enforcement,” *FBI Law Enforcement Bulletin*, (September 2011), <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2011>. Hereinafter: FBI Counterterrorism Analysis Section, “Sovereign Citizens.”

¹⁸¹ Anti-Defamation League, *The Lawless Ones: The Resurgence of the Sovereign Citizen Movement*, August 9, 2010, pp. 2-6, http://www.adl.org/learn/sovereign_movement/sovereign_citizens_movement_report.pdf. Hereinafter: Anti-Defamation League, *The Lawless*.

¹⁸² *Ibid.*, p. 6.

¹⁸³ However, this reportedly does not keep some sovereign citizen extremists from cashing government paychecks. See J.J. McNabb, “Working for the Man: Anti-Government Extremists Who Cash Government Paychecks,” *Forbes*, March 5, 2012, <http://www.forbes.com/sites/jjmacnab/2012/03/05/working-for-the-man-anti-government-extremists-who-cash-government-paychecks/2/>.

¹⁸⁴ Tom Morton, “Sovereign Citizens Renounce First Sentence of 14th Amendment,” *Casper Star-Tribune*, April 17, 2011, http://trib.com/news/local/casper/article_a5d0f966-7ed0-549f-a066-b1b2c91f9489.html.

¹⁸⁵ *Ibid.*

¹⁸⁶ Anti-Defamation League, *The Lawless*, pp. 4-5.

¹⁸⁷ Lance Griffin, “Sovereigns’ Gain Attention of Law Enforcement,” *Dothan Eagle*, May 21, 2011, <http://www2.dothanegale.com/news/2011/may/21/3/sovereigns-gain-attention-law-enforcement-ar-1872889/>.

subject to being stopped, detained, or arrested by law enforcement personnel.”¹⁸⁸ In 2003, Ronald K. Delorme developed the Pembina Nation Little Shell Band of North America¹⁸⁹ into a sovereign citizen group.¹⁹⁰ It is a sham Native American tribe that anyone can join to try and avoid taxes and government-imposed costs, such as auto registration fees. For example, news reports indicate that in June 2010, a sheriff’s deputy in Florida pulled over John McCombs when the law enforcement official noticed a Pembina Nation Little Shell license plate on the motorcycle McCombs was driving. According to publicly available sources, McCombs presented a fraudulent letter of diplomatic immunity and an invalid Pembina Nation Little Shell vehicle registration.¹⁹¹

Some sovereign citizen fraud appears to be motivated by economic opportunism rather than ideology.¹⁹² This includes “pyramid schemes, other investment schemes, bogus trust scams, real estate fraud, and various types of tax frauds [as well as] more esoteric scams ... ranging from immigration fraud to malpractice insurance fraud.”¹⁹³ In November 2011, husband and wife Monty and Patricia Ervin were convicted in federal court of conspiring to defraud the United States as well as three counts of tax evasion. In addition, the federal jury convicted Patricia of structuring transactions to avoid bank reporting requirements.¹⁹⁴ The couple allegedly had not filed federal income tax returns between 2000 and 2008, denied their U.S. citizenship, and dubbed themselves “sovereign” when the IRS investigated.¹⁹⁵ The Ervins earned more than \$9 million from investment properties they owned.¹⁹⁶ A group of self-proclaimed sovereign citizens in North Georgia was indicted in March 2011 for using sovereign schemes to allegedly steal millions of dollars worth of real estate.¹⁹⁷

In a few recent cases, avowed sovereign citizens have been involved in violent altercations with law enforcement officers. According to a September 2011 FBI publication, since 2000 “lone-offender sovereign-citizen extremists have killed six law enforcement officers,” and the Bureau sees sovereign citizens as a growing threat to U.S. law enforcement.¹⁹⁸

- Perhaps the most publicized example of alleged sovereign violence directed at police occurred in 2010. In May of that year, two self-professed sovereign

¹⁸⁸ Department of Justice, press release, “Jury Convicts Three Men of Conspiracy To Use Fake Diplomatic Identification,” August 31, 2009, <http://www.state.gov/m/ds/rls/128533.htm>.

¹⁸⁹ The group is not a federally recognized tribe.

¹⁹⁰ Anti-Defamation League, *The Lawless*; Chris Gerbasi, “Tribal Claims Causing Charlotte Controversy,” *Sarasota Herald Tribune*, July 25, 2010; “Punta Gorda Man Arrested for Driving with Pembina Nation Plate,” *WINK News*, June 1, 2010, <http://www.winknews.com/Local-Florida/2010-06-01/Punta-Gorda-man-arrested-for-driving-with-Pembina-Nation-plate>.

¹⁹¹ *Ibid.*

¹⁹² For a discussion of redemption as a scam, see Federal Bureau of Investigation, *Common Fraud Schemes*, <http://www.fbi.gov/scams-safety/fraud>.

¹⁹³ Anti-Defamation League, *The Lawless*, p. 24.

¹⁹⁴ Department of Justice, press release, “Self-Proclaimed ‘Governor’ of Alabama and Wife Convicted of Tax Fraud,” November 4, 2011, <http://www.justice.gov/opa/pr/2011/November/11-tax-1459.html>. Hereinafter: Department of Justice, “Self-Proclaimed.”

¹⁹⁵ *Ibid.*; *United States v. Patricia Ervin and Monty Ervin*, Superseding Indictment, 1:11-CR-07-MHT, District Court, Middle District of Alabama, February 17, 2011.

¹⁹⁶ Department of Justice, “Self-Proclaimed.”

¹⁹⁷ Megan Matteucci, “12 ‘sovereign citizens’ indicted,” *Atlanta Journal-Constitution*, March 15, 2011, <http://www.ajc.com/news/dekalb/12-sovereign-citizens-indicted-873458.html>.

¹⁹⁸ FBI Counterterrorism Analysis Section, “Sovereign Citizens.”

citizens were involved in a violent confrontation with West Memphis, TN, police officers. During a traffic stop, Joe Kane fired an AK-47 assault rifle and killed two officers. Kane and his father Jerry fled the scene. Law enforcement sighted their vehicle in a nearby parking lot 90 minutes later. The duo died in the ensuing shootout, which also wounded two more officers.¹⁹⁹ The FBI had investigated Jerry Kane five years before the murders because he was allegedly traversing the United States peddling what the FBI termed a “debt elimination scheme.”²⁰⁰

Other cases have garnered attention. For example, in July 2011 James M. Tesi allegedly shot at a local police officer trying to arrest him near Fort Worth, TX. Tesi was reportedly wounded in the altercation. Outstanding “arrest warrants for speeding, driving without a license in possession, and failure to appear” prompted the attempted apprehension.²⁰¹ Court documents described in news reporting note that Tesi linked himself to a sovereign citizen group.²⁰² In February 2012, Tesi was found “guilty of aggravated assault on a public servant with a deadly weapon.”²⁰³ In June 2011, a police officer in Page, AZ, shot and killed William Foust while responding to a domestic violence 911 call. The shooting reportedly occurred during a physical struggle in which Foust attempted to “gain control of” the police officer’s Taser.²⁰⁴ According to a press account, Foust had declared his sovereign citizen status in court proceedings in Kenab, UT (about 75 miles from Page), related to a speeding ticket.²⁰⁵

Black Separatist Extremists

DOJ includes black separatism in its list of movements that potentially spawn domestic terrorists.²⁰⁶ However, most black separatists solely engage in constitutionally protected behavior. Since 9/11, there has been little public discussion of federal investigations involving black separatist extremists. One group exhibiting what can be described as black separatist views, the New Black Panther Party for Self Defense (NBPP), received national scrutiny over voter intimidation allegations involving members of its Philadelphia chapter during the 2008 federal general election.

¹⁹⁹ Cindy Wolff, “West Memphis Police Sued by Widow of Man Killed in Shootout,” *The Commercial Appeal*, April 21, 2011, <http://www.commercialappeal.com/news/2011/apr/21/west-memphis-police-sued-by-kanes-widow/>; Kristina Goetz, Cindy Wolff, “Grieving West Memphis Chief Raises National Curtain on Sovereign Citizens,” *The Commercial Appeal*, April 17, 2011, <http://www.commercialappeal.com/news/2011/apr/17/west-memphis-police-chief-sovereign-citizens/>.

²⁰⁰ Scott Knoll, “The Warning That Never Came: What the FBI Knew About Jerry Kane,” *WREG*, March 2, 2011, <http://www.wreg.com/wreg-fbi-file-reveals-feds-investigated-kane-story,0,4377626.story>.

²⁰¹ Domingo Ramirez Jr., “Man in ‘Sovereign Citizen’ Group is Wounded in Shootout,” July 22, 2011, <http://www.star-telegram.com/2011/07/21/3238352/man-in-sovereign-citizen-group.html>.

²⁰² *Ibid.*

²⁰³ Steve Norder, “‘Sovereign Citizen’ Gets 35 Years for Assault on Officer,” *Fort Worth Star-Telegram*, February 1, 2012, <http://www.star-telegram.com/2012/01/31/3702338/sovereign-citizen-found-guilty.html>.

²⁰⁴ Todd Glasenapp and Larry Hendricks, “Page Officer Kills Man in DV Incident,” *Arizona Daily Sun*, June 21, 2011, http://azdailysun.com/news/local/crime-and-courts/article_61e27d9d-6d47-5655-8a71-d28b846d8e3e.html.

²⁰⁵ *Ibid.*

²⁰⁶ Department of Justice, *White Paper*, p. 59.

The NBPP emerged in the early 1990s, and it is not tied to the Black Panthers from the 1960s.²⁰⁷ Watchdog groups have described the NBPP as “a virulently racist and anti-Semitic organization whose leaders have encouraged violence against whites, Jews, and law enforcement officers,”²⁰⁸ as well as “the largest organized anti-Semitic and racist black militant group in America.”²⁰⁹ The NBPP, which denies that it is a hate group, engages in “high-profile” rhetoric at rallies or demonstrations intended to encourage confrontation with authorities. The group’s actions occur “on behalf of the poor or disadvantaged, involving the ready display of firearms.”²¹⁰ As an example of the rhetoric the group uses, an NBPP representative characterized the March 2011 shooting death of a drug suspect in Jacksonville, FL, as “a violent act of terrorism” committed by police.²¹¹ Soon after the shooting, the Jacksonville Sheriff’s Office said that the confrontation involved undercover officers serving a search warrant at an apartment. Officers claimed that inside the apartment, the victim—an alleged drug dealer with a criminal record—was holding a firearm.²¹²

In 2008, the Philadelphia, PA, chapter of the NBPP was involved in a case that generated public controversy. A 2009 civil suit filed by DOJ claimed that two NBPP members wearing the group’s paramilitary uniforms loitered around the entrance to a 2008 federal general election polling station in Philadelphia. One of the NBPP members allegedly carried a nightstick. According to DOJ, some poll watchers feared for their safety because of this activity. Philadelphia police officers responding to claims of voter intimidation removed the nightstick-wielding NBPP member and allowed the other to remain (the latter was a certified poll watcher). Police asked people at the polling station whether they had been threatened by the two individuals. All those questioned replied that they had not. However, at least one individual claimed that the presence of the two NBPP members had been intimidating.²¹³ The NBPP disavowed the actions of its two members.²¹⁴ In May 2009, DOJ voluntarily dismissed claims against defendants in the case, and a July 2009 letter from 10 members of Congress to DOJ’s Inspector General questioned the decision to do so. DOJ’s Office of Professional Responsibility (OPR) investigated, and in March 2011, OPR issued a report which argued that DOJ officials did not act inappropriately regarding the matter.²¹⁵

²⁰⁷ D.J. Mulloy, “New Panthers, Old Panthers, and the Politics of Black Nationalism in the United States,” *Patterns of Prejudice*, vol. 44, no. 3 (2010), pp. 217, 219, 229-236. Hereinafter: Mulloy: “New Panthers.”

²⁰⁸ Southern Poverty Law Center, “New Black Panther Party,” <http://www.splcenter.org/get-informed/intelligence-files/new-black-panther-party>.

²⁰⁹ Anti-Defamation League, “New Black Panther Party for Self Defense,” June 1, 2011, http://www.adl.org/main_Extremism/new_black_panther_party.htm.

²¹⁰ Mulloy: “New Panthers,” p. 223, 233.

²¹¹ “Black Panthers Protest Police Shooting,” October 14, 2011, <http://www.news4jax.com/news/Black-Panthers-Protest-Police-Shooting/-/475880/1962744/-/qs5j0xz/-/index.html>; “Black Panthers Protest Police Shooting,” *First Coast News*, March 19, 2011, <http://www.firstcoastnews.com/rss/article/197113/3/Black-Panthers-Protest-Police-Shooting>.

²¹² Ibid.

²¹³ Department of Justice, Office of Professional Responsibility, Report, *Investigation of Dismissal of Defendants in United States v. New Black Panther Party for Self-Defense, Inc. et al.*, March 17, 2011, pp. 6-8. Hereinafter: DOJ, OPR, *Investigation of Dismissal*.

²¹⁴ Mulloy: “New Panthers,” p. 217-218.

²¹⁵ DOJ, OPR, *Investigation of Dismissal*, pp. 1-3.

Anti-Abortion Extremists

The vast majority of anti-abortion activists engage in constitutionally protected activity. However, anti-abortion extremism involves crime committed in the name of the anti-abortion movement. Sixty-six instances of “extreme violence” targeting abortion providers and clinics occurred in the United States from 1997 through 2010, according to one group that supports abortion rights and tracks criminal activity intended to limit access to abortion services.²¹⁶ These cases involved shootings, bombings, arson incidents, and acid attacks.²¹⁷ Since 1993, eight clinic workers have been murdered by anti-abortion extremists in the United States.²¹⁸ Because of a wave of violence focused on abortion providers in the 1980s and early 1990s, Congress passed and President Clinton signed into law the Freedom of Access to Clinic Entrances Act (FACE Act) (18 U.S.C. §248) in 1994.²¹⁹ As with other types of domestic terrorism investigations, it is unclear exactly which incidents of violence perpetrated against abortion providers the FBI considers terrorist acts.

The 2009 murder of George Tiller, an abortion provider, received sizeable public attention. On January 29, 2010, Scott Roeder was convicted of first-degree murder and two counts of aggravated assault for killing Tiller. Roeder shot Tiller while the latter was at church on May 31, 2009. Roeder was sentenced to “life in prison with no possibility of parole for 50 years.”²²⁰

A number of other unrelated schemes targeting abortion clinics have been uncovered since Roeder’s arrest. These incidents appear to involve individuals largely operating alone.

- In January 2012, Bobby Joe Rogers was charged in the firebombing of a Pensacola, FL, abortion clinic on New Year’s Day 2012. The bombing destroyed the clinic, which had been targeted in the past.²²¹ In February 2012, a federal grand jury indicted him on two counts—arson and damaging a reproductive health facility.²²²

²¹⁶ National Abortion Federation, “Clinic Violence,” http://www.prochoice.org/about_abortion/violence/history_extreme.asp. See also: “NAF Violence and Disruption Statistics,” http://www.prochoice.org/pubs_research/publications/downloads/about_abortion/stats_table2010.pdf.

²¹⁷ Ibid.

²¹⁸ NARAL Pro-Choice America Foundation, press release, “Anti-Choice Violence and Intimidation,” January 1, 2011, <http://www.naral.org/media/fact-sheets/abortion-anti-choice-violence.pdf>.

²¹⁹ This is not a terrorism-related statute. In fact, DOJ’s Civil Rights Division, prosecutes both criminal and civil cases involving the FACE Act. See <http://www.justice.gov/crt/about/crm/overview.php>; <http://www.justice.gov/crt/about/spl/face.php>. The FACE Act (18 U.S.C. §248), “protects the exercise of free choice in obtaining reproductive health services, and the exercise of First Amendment religious freedoms. Section 248 makes it unlawful for a person to use force, threat of force, or physical obstruction to intentionally injure or intimidate a person because he/she is or has been obtaining or providing reproductive health services. Section 248 also makes it unlawful for a person to use force, threat of force, or physical obstruction to intentionally injure or intimidate a person because he/she is lawfully exercising the right of religious freedom at a place of worship. Finally, Section 248 makes it unlawful for a person to intentionally damage or destroy the property of a facility because it provides reproductive health services, or because it is a place of worship. Section 248 also prohibits anyone from attempting to commit any of the above.”

²²⁰ Ron Sylvester, “Scott Roeder Gets Hard 50 in Murder of Abortion Provider George Tiller,” *Wichita Eagle*, April 1, 2010, <http://www.kansas.com/2010/04/01/1249310/roeder-to-be-sentenced-thursday.html>. Hereinafter: Sylvester, “Scott Roeder.” Roeder reportedly also adhered to anti-government beliefs beginning in the 1990s. See Ron Sylvester, Abortion Issue Front and Center in Roeder Murder Trial,” January 10, 2010, *Wichita Eagle*, <http://www.kansas.com/2010/01/10/1130385/abortion-issue-front-and-center.html#storylink=cpy>.

²²¹ “Man Indicted for Abortion Clinic Firebombing,” *Associated Press*, February 23, 2012.

²²² Department of Justice, press release, “Arson Indictment Returned Regarding American Family Planning Clinic,” February 23, 2012, [http://www.fbi.gov/jacksonville/press-releases/2012/arson-indictment-returned-regarding-american-\(continued...\)](http://www.fbi.gov/jacksonville/press-releases/2012/arson-indictment-returned-regarding-american-(continued...))

- In May 2011, Ralph Lang was arrested after allegedly accidentally firing his handgun through the door of the hotel room in Madison, WI. He was reportedly planning to kill abortion providers in the area.²²³

One underground network that supports attacks on abortion clinics is the Army of God (AOG).²²⁴ The loosely structured organization openly promotes anti-abortion violence.²²⁵ However, its members deny that they are terrorists. They also deny that attacks against clinics and abortion providers constitute violent activity, because they see it as “Godly work.”²²⁶ AOG first made headlines with the 1982 kidnapping of a doctor and his wife, both of whom ran an abortion clinic in Illinois. Three individuals who claimed membership in AOG were responsible.²²⁷ The group disseminates a manual that “is a ‘how to’ for abortion clinic violence. It details methods for blockading entrances, attacking with butyric acid, arson, bomb making, and other illegal activities. The manual contains anti-abortion language as well as anti-government and anti-gay/lesbian language. The manual begins with a declaration of war on the abortion industry.”²²⁸ Eric Rudolph, who in the late 1990s bombed an abortion clinic near Atlanta, GA, and one in Birmingham, AL, “published his writings on the Army of God website.”²²⁹

(...continued)

family-planning-clinic.

²²³ Kevin Murphy, *Feds Mull Felony Charge for Suspect Ralph Lang of Marshfield in Abortion Clinic Shooting Plot*, “*Marshfield News*, May 28, 2011; Department of Justice, press release, “Wisconsin Man Charged with FACE Act Violations,” May 26, 2011, <http://www.justice.gov/opa/pr/2011/May/11-crt-695.html>. For other examples of individuals involved in abortion-related violence, see Department of Justice, press release, “Man Pleads Guilty to Civil Rights Violation in Connection with Arson at Planned Parenthood and Vandalism of Mosque in Madera, California,” October 7, 2011, <http://www.justice.gov/opa/pr/2011/October/11-crt-1336.html>. Mower also threw a brick at a mosque in Madera. Ryan Seals, “Update: Concord Man Charged in Plot to Bomb Abortion Clinic,” *Greensboro News and Record*, September 9, 2010, http://www.news-record.com/content/2010/09/09/article/concord_man_charged_with_plotting_to_bomb_abortion_clinic; “Man Guilty of Bombing Plot Gets 30 Months,” *Salisbury Post*, March 2, 2011, <http://www.salisburypost.com/news/030211-moose-sentencing-today-qcd>.

²²⁴ National Consortium for the Study of Terrorism and Responses to Terrorism (START), “Terrorist Organization Profile: Army of God,” http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=28. Hereinafter: START, “Army of God.”

²²⁵ Mireille Jacobson and Heather Royer, “Aftershocks: The Impact of Clinic Violence on Abortion Services,” National Bureau of Economic Research, Working Paper No. 16603, (January 7, 2010), p. 6.

²²⁶ Jennifer Jefferis, *Armed for Life: The Army of God and Anti-Abortion Terror in the United States* (Santa Barbara, CA: Praeger, 2011), p. xvi. Hereinafter: Jefferis, *Armed for Life*.

²²⁷ *Ibid.*, p. 23. The victims were released unharmed after eight days of captivity. See; “Abortion Opposition Stressed in Kidnapping Trial in Illinois,” *New York Times*, January 26, 1983.

²²⁸ START, “Army of God.”

²²⁹ Beau Seegmiller, “Radicalized Margins: Eric Rudolph and Religious Violence,” *Terrorism and Political Violence*, vol. 19, no. 4 (October 2007), p. 524. The 1998 bombing in Birmingham killed a police officer and injured a nurse. On May 31, 2003, Rudolph was arrested and charged with the clinic bombings, bombing the Centennial Olympic Park during the 1996 summer Olympic games in Atlanta (claiming one life), and attacking a gay club—Atlanta’s Otherside Lounge—in 1997. Rudolph admitted to the bombing spree in April 2005. He claimed that the 1996 attack at Centennial Olympic Park was intended to shame the U.S. government for what Rudolph saw as its support of abortion rights. See “Rudolph Pleads Guilty in Series of Bombings,” *Associated Press* at *MSNBC*, April 13, 2005, http://www.msnbc.msn.com/id/7486021/ns/us_news-crime_and_courts/t/rudolph-pleads-guilty-series-bombings/#.TwN9CUdO3y0; “Rudolph Agrees to Plea Agreement,” *CNN*, April 12, 2005, http://articles.cnn.com/2005-04-08/justice/rudolph.plea_1_emily-lyons-eric-robert-rudolph-atlanta-attacks?_s=PM:LAW.

Protected Activities vs. Terrorism—Divergent Perceptions of the ALF

The boundary between constitutionally protected legitimate protest and terrorist activity has received much attention in public discussions of domestic terrorism. As an example of this, the next several sections of this report explore such considerations regarding the ALF.

A Serious Domestic Concern or “Green Scare?”

U.S. law enforcement, some business groups, and some scientists—among others—have stressed that animal rights extremists (and eco-terrorists) are a security and law enforcement concern. In 2008, the FBI stated that animal rights extremists and eco-terrorists together posed a serious domestic terrorism threat for several reasons, including the number of crimes attributed to animal rights extremists and eco-terrorists (between 1,800 and 2,000 incidents accounting for more than \$110 million²³⁰ in damages from 1979 to early 2009), the broad pool of victims (such as large pharmaceutical corporations, scientific laboratories, ski resorts, automobile dealerships, individual researchers, and lumber companies), and the movement’s rhetoric and destructive tactics.²³¹ In March 2012, the FBI suggested that the threat from eco-terrorists may be declining in recent years.²³²

As articulated by some scientific researchers, the monetary toll on legitimate businesses and laboratories in the United States exacted by animal rights and eco extremists is compounded by less tangible issues. For example, animal rights extremists and eco-terrorists have impacted the work of scientists. In some cases, special equipment and research materials have been destroyed in attacks. The consequences of criminal activity in the name of movements such as the ALF can also be more personal. Two advocates of animal research conducted strictly according to federal regulations have noted that the actions of animal rights extremists have pushed some scientists to quit lab work involving animals. Often, this work relates to products and procedures that some maintain cannot feasibly be marketed without animal testing.²³³ In 2006, a UCLA professor of behavioral neuroscience declared he was stopping his research on monkeys because of what he

²³⁰ ELF claims that it has caused over \$150 million in damages, although the geographic range and timeframe for this figure are unknown. Earth Liberation Front.org, “What Is the Earth Liberation Front?” <http://www.earthliberationfront.org/elffaq.html>. Hereinafter: ELF, “What Is the Earth?” See also: <http://www.animalliberationfront.com/ALFront/ELF/ELFPRESSOFFICE.htm>.

²³¹ There is some imprecision in the FBI’s public statements regarding the number of crimes committed by animal rights extremists and eco-terrorists. In April 2009, the FBI estimated that “to date [animal rights and eco-] extremists have been responsible for more than 1,800 criminal acts.” Ten months earlier, in June 2008, the FBI placed the number of criminal acts at “over 2,000 since 1979.” See Michael J. Heimbach, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, press conference, April 21, 2009, <http://www.fbi.gov/news/speeches/new-most-wanted-terrorist-announced>. Hereinafter: Heimbach, press conference. See also: FBI, “Putting Intel.” The \$110 million figure remained the same in both publicly released documents.

²³² Juliet Eilperin, “As Eco Terrorism Threat Wanes, Governments Keep Eyes on Activists,” *Washington Post*, March 11, 2012, http://www.washingtonpost.com/national/health-science/as-eco-terrorism-wanes-governments-still-target-activist-groups-seen-as-threat/2012/02/28/gIQA4Ay3R_story.html. Hereinafter: Eilperin, “As Eco Terrorism.”

²³³ Conn and Parker, *The Animal*, pp. xii, xvi. See also: 21 C.F.R. §314.610 (regarding approval based on evidence of effectiveness from studies in animals).

described as harassment by animal rights groups.²³⁴ Additionally, animal rights extremists are said to be driving out students from research programs.²³⁵

Critics of U.S. efforts to fight animal rights extremism and eco-terrorism have suggested that the threat is overblown by law enforcement and that the government's pursuit of purported extremists perpetuates a "green scare," chilling the exercise of protected speech by protesters.²³⁶ Some say that the government conflates property crime with terrorism.²³⁷ Others add that people engaged in what the government describes as animal rights extremism or eco-terrorism do not deserve the terrorist label.

Animal Enterprise Terrorism Act (P.L. 109-374)

The Animal Enterprise Terrorism Act (P.L. 109-374; AETA) expanded the federal government's legal authority to combat animal rights extremists who engage in criminal activity. Signed into law in November 2006, it amended the 1992 Animal Enterprise Protection Act (P.L. 102-346; AEPA). Namely, the AETA

Amends the federal criminal code to revise criminal prohibitions against damaging or interfering with the operations of an animal enterprise to include intentional damage or loss to any real or personal property and intentional threats of death or serious bodily injury against individuals (or their family members, spouses, or intimate partners) who are involved with animal enterprises.²³⁸

The AETA expanded the AEPA to include both successful and attempted conspiracies. It also prohibits intentionally placing a person in "reasonable fear" of death or serious bodily injury while damaging or interfering in the operations of an animal enterprise. The AETA revised and increased monetary and criminal penalties. It also stipulates that it does not prohibit First Amendment-protected activity.

DOJ successfully prosecuted individuals on charges relating to animal enterprise terrorism for the first time under the AEPA in 2006 (the case had been built before the AETA had been signed into law).²³⁹ Six individuals were convicted for what DOJ described as "their roles in a campaign to terrorize officers, employees, and shareholders of HLS [Huntingdon Life Sciences, a research

²³⁴ Samantha Henig, "UCLA Professor Halts Monkey Research," *Chronicle of Higher Education*, vol. 53, no. 2 (September 1, 2006), p. 21.

²³⁵ Michael Conn and James Parker, "Winners and Losers in the Animal Research Wars," *American Scientist*, vol. 96, no. 3 (May-June 2008), p. 184.

²³⁶ See Will Potter, *Green Is the New Red: An Insider's Account of a Social Movement Under Siege*, (San Francisco: City Lights Books, 2011), p. 61.

²³⁷ Coalition to Abolish the AETA, "AETA v. AEPA: A Side-by-Side Comparison," October 16, 2008, <http://abolishtheaeta.org/web/aeta-v-aepa-a-side-by-side-comparison/>; Center for Constitutional Rights, factsheet, "The Animal Enterprise Terrorism Act (AETA)," [http://ccrjustice.org/learn-more/faqs/factsheet%3A-animal-enterprise-terrorism-act-\(aeta\)](http://ccrjustice.org/learn-more/faqs/factsheet%3A-animal-enterprise-terrorism-act-(aeta)).

²³⁸ P.L. 109-374, CRS summary. Instead of damage and interference, the AEPA focused on the "physical disruption to the functioning of an animal enterprise." According to AETA, "animal enterprise" means: "(A) a commercial or academic enterprise that uses or sells animals or animal products for profit, food or fiber production, agriculture, education, research, or testing; (B) a zoo, aquarium, animal shelter, pet store, breeder, furrier, circus, or rodeo, or other lawful competitive animal event; or (C) any fair or similar event intended to advance agricultural arts or sciences."

²³⁹ Department of Justice, press release, "Three Militant Animal Rights Activists Sentenced to Between Four and Six Years in Prison," September 21, 2006.

corporation that performs animal research and has U.K. and U.S. facilities].”²⁴⁰ These individuals belonged to an animal rights campaign named Stop Huntingdon Animal Cruelty (SHAC)²⁴¹ and the entity SHAC USA, Inc. SHAC involves both legal protests and criminal activity against HLS.

Reportedly, the six incited threats, harassment, and vandalism and on this basis were convicted of violating the AEPA.²⁴² DOJ has noted that SHAC’s stated mission was to work “outside the confines of the legal system.”²⁴³ DOJ proved in court that the group managed websites that encouraged others “to direct their intimidation, harassment, and violence against HLS and its targeted employees, as well as secondary targets—companies and employees who did business with HLS.”²⁴⁴

DOJ has also successfully applied the AETA. For example, on February 14, 2011, Scott DeMuth was sentenced to six months in prison on one count of misdemeanor conspiracy to commit animal enterprise terrorism. He was involved in a raid that released about 200 ferrets at a Minnesota farm in 2006. Activists had claimed the action in the name of the ALF.²⁴⁵ In another case, William James Viehl and Alex Hall were sentenced to 24 months and 21 months in prison, respectively, under AETA. The duo had released 650 minks, destroyed breeding records, and vandalized structures at the McMullin Ranch in South Jordan, UT, in 2008.²⁴⁶

DOJ has experienced at least one setback in its application of the AETA. In February 2009, the FBI announced the arrests of what it described as “four animal rights extremists.” The four (two women, two men, all in their 20s) allegedly violated the AETA by using “force, violence, or

²⁴⁰ Ibid. See also: “The SHAC 7,” <http://www.shac7.com/case.htm>.

²⁴¹ An undercover British television report on the treatment of animals at a British company, Huntingdon Life Sciences (HLS), sparked the creation of Stop Huntingdon Animal Cruelty (SHAC) in the United Kingdom in 1999. Active in a number of countries around the world, including the United States, the campaign has tried to compel business and financial firms to cut ties to HLS. It has involved both legal protests and crime. John P. Martin, “Animal Rights and Wrongs,” *Newark Star-Ledger*, November 28, 2004; Anti-Defamation League, *Ecoterrorism*. For more on SHAC from a movement perspective, see “History of the Animal Liberation Front,” http://www.animalliberationfront.com/ALFront/Premise_History/ALF_History.htm. The SHAC campaign made its way to the United States in 2000. See Heimbach, press conference.

²⁴² Four of the six were guilty of other charges related to the case as well. Department of Justice, “Militant Animal Rights Group, Six Members Convicted in Campaign to Terrorize Company, Employees, and Others,” March 2, 2006, http://www.justice.gov/usao/nj/press/files/shac0302_r.htm. Hereinafter: Department of Justice, “Militant Animal Rights.” Anti-Defamation League, “Animal Rights Group Sentenced for Inciting Violence and Stalking,” September 22, 2006, <http://www.adl.org/NR/exeres/7FBDB1FE-9176-4802-8704-54F8EAC3C215,18AA02A5-13A1-44F3-B4D4-6176E1ECC36C.frameless.htm>. Hereinafter: Anti-Defamation League, “Animal Rights Group.”

²⁴³ Department of Justice, *White Paper*, p. 60.

²⁴⁴ Ibid. The convictions in the case were upheld by a federal appeals court in 2009. See Lisa Coryell, “Convictions of Animal Rights Activists Upheld,” *Times of Trenton*, October 14, 2009, http://www.nj.com/mercer/index.ssf/2009/10/convictions_of_animal_rights_a.html. Subsequently, the U.S. Supreme Court refused to review the case. See Center for Constitutional Rights, “U.S. v. SHAC 7,” <http://ccrjustice.org/us-v-SHAC7>; Will Potter, “Supreme Court Will Not Hear SHAC 7 Case,” March 7, 2011, <http://www.greenisthenewred.com/blog/shac-7-supreme-court/4447/>.

²⁴⁵ Ryan J. Foley, “Minn. Man Gets 6 Months for Raid on Ferret Farm,” *Associated Press*, February 14, 2011. Jennifer Kotila, “Minneapolis Man To Be Sentenced for Releasing HL Ferrets He Thought Were Mink,” *Delano Herald Journal*, (Minnesota) December 20, 2010, <http://www.herald-journal.com/archives/2010/stories/latzig-ferrets-scott-demuth.html>.

²⁴⁶ Dennis Romboy, “Man Who Raided South Jordan Mink Farm Sentenced,” *Deseret News*, July 1, 2010, <http://www.deseretnews.com/article/700044577/Man-who-raided-South-Jordan-mink-farm-sentenced.html>; Department of Justice, press release, “Viehl Pleads Guilty to Damaging, Interfering with Animal Enterprise in Connection with McMullin Mink Farm Incident,” September 3, 2009, <http://www.justice.gov/usao/ut/press/releases/viehl%20cop.pdf>.

threats to interfere with the operation of the University of California.”²⁴⁷ The incidents leading to the indictment included protests at the houses of researchers from the University of California, Berkeley and University of California, Santa Cruz. According to the FBI’s press release, in one instance, three of the indicted individuals tried to forcibly enter the home of a researcher, whose husband was hit by an object while confronting the protesters.²⁴⁸ In July 2010, a federal judge dismissed the indictment against the four. According to the ruling, the indictment failed to specifically describe crimes allegedly committed by the defendants.²⁴⁹ Opponents of the prosecution stress that the case involved over-broad application of AETA to First Amendment-protected behaviors.²⁵⁰

Criticisms of federal government efforts to counter animal rights extremists have focused on the AETA itself and First Amendment-related issues. Opponents of the AETA suggest that it expanded the AEPA too much by making it easier to prosecute individuals who wage protest campaigns against secondary or tertiary targets—companies or people (such as insurers) indirectly tied to an animal enterprise.²⁵¹ Opponents also take issue with the inclusion of “reasonable fear” in the AETA, suggesting that protected speech or activities may possibly be interpreted as provoking “reasonable fear” in some instances. Echoing critiques of the AETA, one observer emphasizes that while activities linked to U.S.-based animal rights extremists have caused significant property damage, none of these criminal acts has physically harmed people. This critic suggests that describing vandalism or arson as *terrorism* and not ordinary *crime* dampens constitutionally protected protest activity by people who support animal rights or radical environmentalism but do not engage in criminal activity.²⁵² In essence, this position argues that the U.S. government is encouraging a “green scare” by labeling the activity of movements such as the ALF and the ELF as terrorism or extremism.²⁵³ After serving 40 months in prison for her involvement with SHAC USA, Lauren Gazzola argued that she was not a terrorist, claiming, “I hadn’t hurt anyone or vandalized any property. In fact, the indictment didn’t allege that I’d committed any independent crime at all, only that I’d ‘conspired’ to publish a website that advocated and reported on protest activity against a notorious animal testing lab in New Jersey.”²⁵⁴

The U.S. Code’s definition of “domestic terrorism” has been seen by some as potentially chilling to legitimate animal rights and environmental protest activities.²⁵⁵ As mentioned, the current

²⁴⁷ Federal Bureau of Investigation, press release, “Four Extremists Arrested for Threats and Violence Against UC Researchers,” February 20, 2009, <http://sanfrancisco.fbi.gov/pressrel/pressrel09/sf022009.htm>.

²⁴⁸ Ibid.

²⁴⁹ “S.C. Animal Activists Won’t Face Charges,” *The Monterey County Herald*, July 14, 2010.

²⁵⁰ Will Potter, “Breaking: AETA 4 Case Dismissed, But Re-Indictment Possible,” *GreenIsTheNewRed.com*, July 12, 2010, <http://www.greenisthenewred.com/blog/aeta-4-case-thrown-out-dismissed/3015/>; Bill Quigley and Rachel Meeropol, “Victory for Animal Rights Dissent,” *Huffington Post*, July 16, 2010, http://www.huffingtonpost.com/bill-quigley/victory-for-animal-rights_b_648852.html. Hereinafter: Quigley and Meeropol, “Victory for Animal.”

²⁵¹ The AETA makes it illegal to damage or interfere with the operations of an animal enterprise. Presumably this covers tertiary targets.

²⁵² Will Potter, “The Green Scare,” *Vermont Law Review*, vol. 33, no. 4 (June 2009), pp. 672-673.

²⁵³ Ibid; Quigley and Meeropol, “Victory for Animal.”

²⁵⁴ Lauren Gazzola, “Animal Rights Activists Like Me Aren’t Terrorists,” *EGP News*, January 12, 2012, <http://egpnews.com/?p=33714>.

²⁵⁵ American Civil Liberties Union, “How the USA PATRIOT Act Redefines “Domestic Terrorism,” December 6, 2002, <http://www.aclu.org/national-security/how-usa-patriot-act-redefines-domestic-terrorism>. For an additional view suggesting that the activities of movements such as the ALF and the ELF should not be treated as terrorism, see (continued...)

delineation of domestic terrorism in the U.S. Code includes criminal acts “dangerous to human life” that appear to intend to intimidate or coerce a civilian population or influence governmental policy via intimidation or coercion. This line of reasoning suggests that the crimes committed by animal rights extremists and eco-terrorists cannot be compared to clearly violent attacks by groups such as Al Qaeda. An opposing commentary stresses that such discussion is irrelevant and

miss[es] the mark. The ALF ideology encourages members to instill fear in those who engage in the activities that the ALF opposes: fear of harm to themselves and their families, and fear of personal and professional economic loss. Additionally, these arguments assume that “true terrorism” is fundamentally different from animal rights terrorism. While it is true that animal rights terrorism, as a whole, does not engage in the same scale of violence as other extremist groups, those working in academia, research, agriculture, and food service industries are no less fearful when their homes and workplaces are firebombed; violent tactics can instill fear even when they are used infrequently.²⁵⁶

Assessing Domestic Terrorism’s Significance

Domestic terrorist attacks have come nowhere near the devastation of 9/11. However, it is worth noting that (as mentioned above) Timothy McVeigh’s bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, claimed 168 lives and injured more than 500 others. It ranks as the second-deadliest terrorist attack on U.S. soil, behind only the devastation wrought by Al Qaeda on 9/11. Domestic terrorists feature prominently among the concerns of some law enforcement officers. For example, Los Angeles Deputy Police Chief Michael P. Downing recently described violent Islamists such as Al Qaeda, Hezbollah, and Hamas as Los Angeles’s main terrorist threats “along with three other terrorist categories: black separatists, white supremacist/sovereign citizen extremists, and animal rights terrorists.”²⁵⁷ In one 2008 study, state police agencies “overwhelmingly reported” dangerous domestic extremist groups present in their jurisdictions.²⁵⁸ Of course, as one expert reminds us, most followers of extremist viewpoints pose no threat: “Most of them are not going to do anything but bore their relatives and friends with ridiculous papers and treatises.”²⁵⁹

Five themes speak to the possible threat posed by domestic terrorists. First, domestic terrorists likely have been responsible for more than two dozen incidents since 9/11, and there appears to be a growth in anti-government extremist activity as measured by watchdog groups in the last several years. Second, a large number of those labeled as domestic terrorists do not necessarily use major terrorist tactics such as bombings or airplane hijackings. Third, domestic terrorists—much like their violent jihadist analogues—are often Internet savvy and use the medium as a resource for their operations. Fourth, domestic terrorism can be seen as a somewhat decentralized threat often involving lone wolves and movements operating under the model of leaderless

(...continued)

DeMond Shondell Miller, Jason David Rivera, and Joel C. Yelin, “Civil Liberties: The Line Dividing Environmental Protest and Ecoterrorists,” *Journal for the Study of Radicalism*, vol. 2, no. 1 (2008), pp. 109-123.

²⁵⁶ Grubbs, “Saving Lives,” pp. 364-365.

²⁵⁷ Bill Gertz, “L.A. Police Use Intel Networks Against Terror,” *Washington Times*, April 11, 2011, <http://www.washingtontimes.com/news/2011/apr/11/la-police-use-intel-networks-against-terror/?page=all#pagebreak>.

²⁵⁸ “Far Right Domestic Terrorism on Par with Foreign Threat, Experts Say,” CNN, July 25, 2011, <http://www.cnn.com/2011/US/07/25/domestic.extremism/>.

²⁵⁹ Ibid.

resistance. Finally, prison has been highlighted as an arena in which terrorist radicalization can occur, and WSE plays a role in the activities of several U.S. prison gangs. Sovereign citizen theories have also taken root in U.S. prisons.

Counting Incidents

Animal rights extremists, eco-terrorists, anarchist extremists, sovereign citizen extremists, militia extremists, black separatist extremists, white supremacist extremists, and anti-abortion extremists target American citizens, businesses, and institutions. The National Counterterrorism Center's Worldwide Incidents Tracking System (WITS) publicly lists 35 terrorist incidents²⁶⁰ involving *all types* of terrorists as occurring in the United States between the beginning of 2004 and the end of September 2011.²⁶¹ Twenty-five of these can be linked to domestic terrorists. Of the 25, the vast majority, 22, can be attributed to environmental or animal rights extremists.²⁶² Even so, the FBI has publicly noted a decline in eco-terrorism especially after a wave of successful prosecutions in 2007. The Bureau also reportedly attributes the perceived dip to activists possibly viewing "a Democratic administration as more sympathetic to their goals and [thus] be less inclined to take radical steps."²⁶³ This latter factor fails to explain high levels of activity in the 1990s. Five of the 35 incidents documented in WITS can be associated with violent jihadists either operating in the United States or attacking the homeland from abroad. For five other incidents, the ideological backgrounds of those involved were unknown.²⁶⁴

These numbers may be too low to make any useful generalizations about the violent threats to the homeland posed by either violent jihadists or domestic terrorists. Other sources—not necessarily databases—indicate that the number of domestic terrorist incidents may be even higher. These sources do not necessarily focus on the same period covered by the WITS. Also, some center on specific categories of domestic terrorist activity. Examples of such sources include the following:

- A September 2011 study by the New America Foundation and Syracuse University's Maxwell School of Public Policy found 114 individuals involved in non-jihadist terrorist acts in the 10 years following 9/11. However, the study did not limit its findings to animal rights extremists, eco-terrorists, anarchist extremists, sovereign citizens, unauthorized militias, black separatists, white supremacists, and anti-abortion extremists. It included incidents by what it described as left-wing and right-wing terrorists.²⁶⁵

²⁶⁰ The WITS methodology describes "incidents" as when "subnational or clandestine groups or individuals deliberately or recklessly attacked civilians or noncombatants (including military personnel and assets outside war zones and war-like settings)." For the WITS methodology, see http://www.nctc.gov/witsbanner/wits_subpage_criteria.html.

²⁶¹ This is based on CRS analysis of information drawn from the WITS on February 1, 2012. The search used for this report drew from the entire time period covered in WITS as of February 1, 2012. The search results included only incidents described in the database as having occurred in the United States.

²⁶² The three remaining domestic terrorism incidents break down thusly: two likely involved anti-abortion extremists. One involved a WSE adherent.

²⁶³ Eilperin, "As Eco Terrorism."

²⁶⁴ Some of the WITS entries include information regarding the terrorist groups involved in committing the incidents. Where possible, publicly-available reporting was used to corroborate this information. For incidents where the WITS did not provide terrorist identifying information, public sources were used to ascertain the possible ideologies of those involved. In five cases this was not possible. These five instances are described as the "unknown" incidents above.

²⁶⁵ Peter Bergen et al. *Right- and Left-Wing Terrorism Since 9/11*, New America Foundation, September 10, 2011, (continued...)

- An unclassified 2008 DHS report includes a table that lists *selected* criminal acts perpetrated by people involved in the animal rights extremist and eco-terrorist movements. This list counts 74 criminal acts between 9/11 and March 2008.²⁶⁶
- As noted above, the FBI estimated that animal rights extremist and eco-terrorists together committed between 1,800 and 2,000 criminal incidents accounting for more than \$110 million in damages from 1979 to early 2009.²⁶⁷
- An unclassified FBI intelligence bulletin estimates that 53 acts of violence were committed by what it calls “white supremacist extremists” between 2007 and 2009 in the United States. Victims included other white supremacists, African Americans, and Latinos. Most of the incidents involved assaults. The bulletin bases these findings on law enforcement and media reporting.²⁶⁸

In the WITS dataset, domestic terrorist incidents may outrank violent jihadist incidents by a factor of four to one. However, within the 35 terrorist incidents, the ones perpetrated by violent jihadists appear more lethal. Overall, 16 people died and 58 were injured in all terrorist incidents described by WITS. Most of the fatalities came from a single homegrown jihadist attack—Army Major Nidal Hasan’s alleged mass shooting at Fort Hood, TX, in November 2009. It claimed 13 of the deaths.²⁶⁹ Forty-three people were injured in this attack as well. One other death was tied to a homegrown violent jihadist, Abdulhakim Muhammad. In June 2009, he shot to death a soldier at the U.S. Army-Navy Career Center in Little Rock, AR.²⁷⁰ Muhammad was charged in state court with capital murder, attempted capital murder, and 10 counts of unlawful discharge of a firearm.²⁷¹ In July 2011, he pled guilty to these charges.²⁷²

The last two deaths associated with the WITS incidents came at the hands of apparent domestic terrorists:

(...continued)

<http://homegrown.newamerica.net/overview>. Hereinafter: Bergen et al. *Right- and Left-Wing*.

²⁶⁶ Department of Homeland Security, *Ecoterrorism: Environmental and Animal-Rights Militants in the United States*, Universal Adversary Dynamic Threat Assessment, May 7, 2008. Table 1 from the report is a “compilation of material from ALF and ELF communiqués and publications, media reports, and law enforcement” listing *selected* criminal acts perpetrated by the ALF and the ELF from 1984 to March 2008. Table 1 from the DHS report is not a comprehensive list of crimes tied to the ALF and the ELF. Hereinafter: Department of Homeland Security, *Ecoterrorism*.

²⁶⁷ Heimbach, press conference; Federal Bureau of Investigation, “Putting Intel.”

²⁶⁸ Federal Bureau of Investigation, *White Supremacist Extremist Violence*, pp. 1-2. The FBI bulletin defines “acts of violence” to include “arson; assaults and murders; and acts designed to threaten or intimidate due to a person’s ethnicity, religious beliefs, or lifestyle.” See Federal Bureau of Investigation, *Rage and Racism* p. 5.

²⁶⁹ For more information on Hasan, see Senator Joseph Lieberman and Senator Susan Collins, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government’s Failure to Prevent the Fort Hood Attack*, Senate Committee on Homeland Security and Governmental Affairs, February 2011, http://hsgac.senate.gov/public/_files/Fort_Hood/FortHoodReport.pdf; and CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*, by Jerome P. Bjelopera. Hereinafter: CRS Report R41416.

²⁷⁰ For more information on Muhammad, see CRS Report R41416, pp. 91-93.

²⁷¹ James Dao, “Man Claims Terror Ties in Little Rock Shooting,” *New York Times*, January 22, 2010, <http://www.nytimes.com/2010/01/22/us/22littlerock.html>. Hereinafter: Dao, January 22, 2010.

²⁷² “Man Pleads Guilty to Recruiting Center Killing, Gets Life,” *CNN.com*, July 25, 2011, http://articles.cnn.com/2011-07-25/justice/arkansas.recruiter.shooting_1_capital-murder-quinton-ezeagwula-carlos-bledsoe?_s=PM:CRIME.

- On January 29, 2010, Scott Roeder was convicted of first-degree murder and two counts of aggravated assault for killing abortion provider George Tiller.²⁷³
- Described as a neo-Nazi and white supremacist, James von Brunn reportedly shot and killed a security guard at the U.S. Holocaust Memorial Museum in Washington, DC, in June 2009. In January 2010, the 89-year-old von Brunn died in federal prison, before he could be tried.²⁷⁴

Caution regarding these incident counts and the related fatalities is suggested by other factors. For example, it is unclear why the aforementioned incidents involving Richard Poplawski as well as Jerry and Joe Kane are not counted in WITS. If they were counted in WITS, these incidents would raise the number of fatalities attributed to domestic terrorists by five. Additional caution regarding the number of fatalities attributed to domestic terrorists is suggested in the aforementioned study by the New America Foundation and Syracuse University's Maxwell School of Public Policy. It counted "[a]t least 14 people ... killed in right- and left-wing terrorism-related incidents [in the 10 years since 9/11]."²⁷⁵ The reader is also reminded that within a relatively small pool of incidents, Hasan's purported shooting was far more violent than any other incident—jihadist inspired or not.

Additionally, most of the 35 incidents—as underscored above—have been linked to either animal rights extremists or eco-terrorists. This further complicates any comparative discussion of levels of violence. As highlighted elsewhere in this report, many animal rights extremists and eco-terrorists claim to avoid violent acts that directly target people. The attacks by these individuals can often be described as property crimes involving arson or vandalism.

Growth in Hate Groups and Anti-Government Extremism

Beyond counting terrorist incidents, the Southern Poverty Law Center (SPLC)²⁷⁶ has noted both a steady rise in the number of hate groups from 2000-2011 and a marked expansion in the militia movement (discussed elsewhere in this report) over the same period. Between 2009 and 2011, militia groups resurged to levels not seen since the 1990s.²⁷⁷ The SPLC's figures likely capture a range of activity broader than that described by DOJ and the FBI as domestic terrorism. Regardless, the SPLC argues that the rise is "driven by resentment over the changing racial demographics of the country, frustration over the government's handling of the economy, and the mainstreaming of conspiracy theories and other demonizing propaganda aimed at various

²⁷³ Sylvester, "Scott Roeder."

²⁷⁴ Anti-Defamation League, "James von Brunn: An ADL Backgrounder," http://www.adl.org/main_Extremism/von_brunn_background.htm.

²⁷⁵ Bergen et al. *Right- and Left-Wing*.

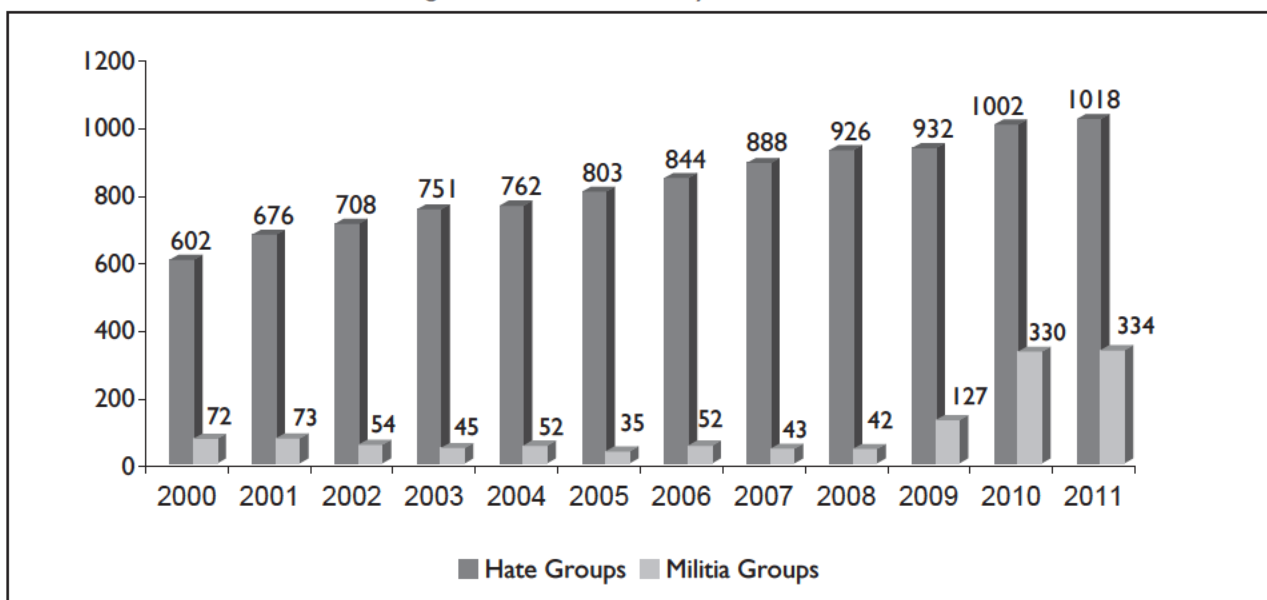
²⁷⁶ The Southern Poverty Law Center has been criticized regarding its labeling of the Family Research Council, as a hate group for its opposition to gay rights. See Family Research Council, press release, "FRC, Members of Congress, Governors, and Conservative Leaders Release Open Letter Calling for Civil Debate, End to Character Assassination," December 15, 2010, <http://www.frc.org/get.cfm?i=PR10L07&f=RF07B02>; Mark Potok, "SPLC Responds to Attack by FRC, Conservative Republicans," December 15, 2010, <http://www.splcenter.org/blog/2010/12/15/splc-responds-to-attack-by-frc-conservative-republicans/>; Sean Lengell, *Washington Times*, "Family Research Council Labeled a 'Hate Group,'" November 24, 2010, <http://www.washingtontimes.com/news/2010/nov/24/frc-labeled-a-hate-group/>.

²⁷⁷ *Ibid.*, p. 42.

minorities.²⁷⁸ SPLC also assesses that 2010 was the first year ever that the number of hate groups topped 1,000 (Figure 1).

Figure 1. Hate Groups and Militia Groups, 2000-2010

According to the Southern Poverty Law Center



Source: Mark Potok, "The Year in Hate and Extremism," Southern Poverty Law Center, *Intelligence Report*, no. 145 (Spring 2012).

Notes: The Southern Poverty Law Center includes Ku Klux Klan, neo-Nazi, white nationalist, racist skinhead, Christian Identity, neo-Confederate, black separatist, and general hate groups in its hate group category. The organization goes on to elaborate that "Christian Identity describes a religion that is fundamentally racist and anti-Semitic. Black Separatist groups are organizations whose ideologies include tenets of racially based hatred. Neo-Confederate groups seek to revive many of the racist principles of the antebellum South. White Nationalist groups espouse white supremacy or white separatism but generally avoid anti-Semitism. General Hate groups espouse ideologies of hatred and include the sub-categories of Anti-Gay groups, Anti-Immigrant groups, Holocaust Denial groups, Racist Music labels, [and] Radical Traditionalist Catholic groups (which reject core Catholic teachings and espouse anti-Semitism)." The SPLC describes patriot groups and militias as anti-government, "engaging in groundless conspiracy theorizing or advocat[ing] or adher[ing] to extreme anti-government doctrines." The patriot or militia organizations counted by Southern Poverty Law Center do not necessarily "advocate or engage in violence or other criminal activities." Neither are they necessarily racist.

"Non-Violent" Strategies

While some domestic terrorism suspects engage in violent plotting, others commit much different crimes that do not physically harm people. This latter group differs from their homegrown violent jihadist counterparts, who are often bent on killing or harming people. Two types of activities that avoid visiting violence upon people but are commonly associated with subjects of domestic terrorism investigations stand out. First, many animal rights extremists, eco-terrorists, and anarchist extremists believe in "direct action." This typically involves what movement members would characterize as *non-violent but criminal* protest or resistance activities furthering the

²⁷⁸ Potok, "The Year," p. 41.

movement's ideology. While direct action has a long legacy among anarchists, in recent years the ALF and the ELF have played a large role in articulating its meaning. Second, "paper terrorism" is a term used to describe some of the *non-violent* criminal activity committed by sovereign citizens involving the filing of fraudulent documents in the hopes of harassing enemies or bilking state or federal tax authorities.

Direct Action

Anarchist extremists, animal liberation extremists, and environmental extremists refer to much of their operational activity as "direct action." This term has a long history, and it can be used to describe legitimate protest such as letter writing campaigns or work stoppages. However, this report uses "direct action" to describe criminal activities such as sabotage and arson.²⁷⁹

ALF and ELF members understand that criminality and direct action are one and the same. *The Animal Liberation Primer*, a movement resource, highlights criminality in the actions of supporters: "anyone working in the ALF is a criminal. You have to begin to think like a criminal." ALF and ELF members also generally view direct action as nonviolent and heroic. Using politically charged language, the ALF allegedly styles itself along the lines of the Underground Railroad, freedom fighters in Nazi Germany, anti-Apartheid protestors, U.S. civil rights activists, and Palestinian groups opposing Israel.²⁸⁰ The ELF views constitutionally protected protest as "state sanctioned" and eschews such activity. The ELF, much like the ALF, also wraps itself in the mantle of reformers and describes itself as inheriting the spirit of Luddites, abolitionists, suffragists, and even the American revolutionary-era Boston Tea Party.²⁸¹

The ALF: "Live Liberations" and "Economic Sabotage"

The ALF's version of direct action is framed as what it considers to be "economic sabotage" or "ethical vandalism." The ALF supports the destruction of property and intimidation of individuals and businesses considered by the movement to be involved in the exploitation of animals. Cells and individuals linked to the ALF also engage in trespassing and theft, or what they perceive as "live liberations" or "rescuing" animals from "the horrors of exploitation"²⁸² and human use²⁸³ by stealing them from places such as legitimate research facilities or farms. Economic sabotage can be virtual. The North American Animal Liberation Press Office (NAALPO) has carried claims of cyber hacking incidents in the name of animal rights.²⁸⁴ NAALPO is one of the web-based

²⁷⁹ According to the DOJ's Office of the Inspector General, the FBI "generally" defines "direct action" as, "criminal activity designed to cause economic loss or to destroy property or operations." See Department of Justice, Office of the Inspector General, Oversight and Review Division, *A Review of the FBI's Investigations of Certain Domestic Advocacy Groups*, (September 2010), p. 97, <http://www.justice.gov/oig/special/s1009r.pdf>; Darren Thurston, *The ALF Primer*, n.d. p. 4. DOJ believes Thurston authored the *Primer*, although he is not attributed as an author in the document. Hereinafter: Thurston, *The ALF Primer*. See also: *Guide to Direct Action*, 2010, http://www.animalliberationfront.com/ALFront/Activist%20Tips/Direct_Action-Guide.htm; Earth Liberation Front.org, "Earth Liberation Front Frequently Asked Questions," Hereinafter: ELF, "FAQs." See also: http://www.animalliberationfront.com/ALFront/ELF/elf_faq.pdf.

²⁸⁰ NAALPO, "History."

²⁸¹ ELF, "FAQs."

²⁸² NAALPO, "History." A section of *The ALF Primer* describes both economic sabotage and live liberation as legitimate strategies. See Thurston, *The ALF Primer*, p. 2.

²⁸³ Conn and Parker, *The Animal*, p. xvii.

²⁸⁴ Communiqué, July 13, 2007, [http://www.animalliberationpressoffice.org/communiques/2007/2007-07-\(continued...\)](http://www.animalliberationpressoffice.org/communiques/2007/2007-07-(continued...))

vehicles used by ALF supporters to publicize criminal activities claimed on behalf of the movement.

The ELF: “Monkeywrenching”

Like the ALF, the ELF’s discussions of direct action also revolve around economic sabotage. The ELF rejects legal protest tactics partly for what it views as pragmatic reasons—“because they have been proven not to work, especially on their own.”²⁸⁵ Economic sabotage in the name of environmentalism has a long history, perhaps stretching back to the 1950s,²⁸⁶ and has been called “monkeywrenching,” a term taken from a 1975 novel, *The Monkey Wrench Gang* by Edward Abbey. The book depicts such activity.²⁸⁷ A guidebook that describes monkeywrenching offers what can be interpreted as a call to arms for would-be extremists:

It is time for women and men, individually and in small groups to act heroically in the defense of the wild, to put a monkeywrench into the gears of the machine that is destroying natural diversity. Though illegal, this strategic monkeywrenching can be safe, easy, and—most important—effective.²⁸⁸

The guidebook also defines monkeywrenching as nonviolent by stressing that it should never target people or “other forms of life.”²⁸⁹

Arson and Explosive Devices

Federal officials are especially concerned about the use of incendiary devices and explosives by animal rights extremists and eco-terrorists. In congressional testimony from 2005, then-ATF Deputy Assistant Director Carson Carroll stated that the “most worrisome” trend regarding animal rights extremists and eco-terrorists was their “willingness to resort to incendiary and explosive devices.”²⁹⁰

This pronouncement came on the heels of two related incidents that occurred near San Francisco, CA, and involved explosive devices. An entity called the Revolutionary Cells of the Animal Liberation Brigade claimed responsibility for both attacks, which the FBI has also linked to a man named Daniel San Diego. In August 2003, two ammonium nitrate pipe bombs exploded at the campus of the biotechnology firm Chiron but caused little damage and no injuries. In October 2003, a reputed 10-pound ammonium nitrate bomb damaged the offices of Shaklee, a health, beauty, and household product company. No one was injured. The perpetrator(s) believed that both companies did business with Huntingdon Life Sciences (the same firm targeted by SHAC

(...continued)

13_lagrange_hls.htm.

²⁸⁵ ELF, “FAQs.”

²⁸⁶ Bron Taylor, “The Tributaries of Radical Environmentalism,” *Journal for the Study of Radicalism*, vol. 2, no. 1 (2008), p. 45.

²⁸⁷ Edward Abbey, *The Monkey Wrench Gang*, 3rd ed. (Salt Lake City, UT: Dream Garden Press, 1985).

²⁸⁸ Dave Foreman, “Strategic Monkeywrenching,” in *Ecodefense: A Field Guide to Monkeywrenching*, ed. Dave Foreman and Bill Haywood, 3rd ed. (Chico, CA: Abzug Press, 1993), p. 8. Hereinafter: Foreman, “Strategic Monkeywrenching.” Foreman was a founder of Earth First! See Anti-Defamation League, *Ecoterrorism*.

²⁸⁹ Dave Foreman, “Strategic Monkeywrenching,” p. 9.

²⁹⁰ Statement of Carson Carroll, p. 43.

and discussed above). A related communiqué stressed that, “all customers and their families are considered legitimate targets.”²⁹¹

One commentator has suggested that the combination of “fire” as a tactic and instilling “fear” as a goal ensures eco-terrorists will continue to warrant the terrorist label.²⁹² Both animal rights extremists and eco-terrorists have histories of using incendiary devices to damage or destroy property—the Vail, CO, fire (mentioned elsewhere in this report) setting a prominent example for extremists. In fact, one of the hallmark publications circulated in extremist circles is a handbook on how to fashion incendiary devices titled *Arson Around with Auntie ALF*.²⁹³ A recent example underscores this focus on arson.

- In January 2012, NAALPO issued a communiqué in which “unnamed activists” claimed responsibility for setting fires that damaged 14 tractor trailer rigs at the Harris Ranch, a cattle feedlot in Coalinga, CA. The perpetrators used containers of accelerant, kerosene-soaked rope, and digital timers to set the blazes. According to the communiqué, the fires apparently embodied a reaction to “the horrors and injustices of factory farming.”²⁹⁴

Some ELF adherents have focused on targets they perceive as emblematic of urban sprawl²⁹⁵ or the excesses of industrialized society. Since 2000, a number of ELF actions have involved the torching of housing projects as well as activities such as the damaging and destruction of sports utility vehicles and other emblems of industrialized society and urban sprawl.²⁹⁶ Between August

²⁹¹ Stacy Finz, “Militants Say They Planted Shaklee Bomb,” *San Francisco Chronicle*, October 1, 2003, http://articles.sfgate.com/2003-10-01/bay-area/17512148_1_pipe-bombs-shaklee-chiron; Stacy Finz, Bernadette Tansey, “2 Bombs Shatter Biotech Firm’s Windows,” August 29, 2003, <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/08/29/MN173487.DTL&type=printable>. The FBI assessed that the devices may have been intended to harm people. The second Chiron bomb was timed to explode after the first, “an apparent strike at first responders,” while the Shaklee bomb was wrapped in nails, “to significantly increase its lethality to anyone in the area at the time of the detonation.” See U.S. Congress, Senate Committee on Environment and Public Works, “Statement of John E. Lewis, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation,” *Eco-Terrorism Specifically Examining Stop Huntingdon Animal Cruelty (“SHAC”)*, 109th Cong., 1st sess., October 26, 2005, 109-1005 (Washington: GPO, 2008), p. 7. In April 2009, the FBI placed Daniel San Diego on its Most Wanted Terrorists List for his involvement in the bombings. See Heimbach, press conference. The Bureau also tied him to SHAC. He had slipped away from FBI surveillance in October 2003. See Federal Bureau of Investigation, “New Most Wanted Terrorist,” April 21, 2009, http://www.fbi.gov/wanted/wanted_terrorists/daniel-andreas-san-diego. Hereinafter: FBI, “New Most Wanted”; “Daniel Andreas San Diego,” *America’s Most Wanted*, <http://www.amw.com/fugitives/case.cfm?id=25800>.

²⁹² Grubbs, “Saving Lives,” p. 370.

²⁹³ Auntie ALF, Uncle ELF, and the Anti-Copyright Gang, *Arson-Around with Auntie ALF: Your Guide for Putting the Heat on Animal Abusers Everywhere*, 2001. Hereinafter: *Arson-Around*.

²⁹⁴ See http://www.animal liberationpressoffice.org/communiques/2012/2012-01-10_harrisranch.htm; Henry K. Lee, “14 Cattle Trucks Burned in Arson at Harris Ranch,” *San Francisco Chronicle*, January 11, 2012; <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/01/10/BABM1MN8BU.DTL>. For other examples, see Peter Young, “Fire and Explosions Rock Oregon Mink Farm,” July 28, 2010, http://www.animal liberationpressoffice.org/press_releases/2010/pr_2010_07_27_astoriafurfarm.htm; J.M. Brown, “A Year after Firebombings, No Arrests, Though Awareness Remains among Scientists,” *Santa Cruz Sentinel*, August 2, 2009; John Coté, “Firebombings Suggest New Tactic for Animal Activists,” *San Francisco Chronicle*, August 5, 2008; Shanna McCord, “FBI to Take Over Santa Cruz Firebombs Case,” *Monterey County Herald*, August 4, 2008; Anti-Defamation League, “‘Justice Department’ Claims Responsibility for Threats against UCLA Animal Researcher,” December 3, 2010, http://www.adl.org/learn/extremism_in_america_updates/movements/ecoterrorism/justice_department_ucla.htm. Hereinafter: Anti-Defamation League, “Justice Department.”

²⁹⁵ Brad Knickerbocker, “Firebrands of ‘Ecoterrorism’ Set Sights on Urban Sprawl,” *Christian Science Monitor*, August 6, 2003, <http://www.csmonitor.com/2003/0806/p01s02-ussc.html>. Hereinafter: Knickerbocker, “Firebrands.”

²⁹⁶ Anti-Defamation League, “Radical Environmentalist Group Suspected in San Diego Arson,” August 8, 2003, (continued...)

and October 2002, three individuals tied to the ELF damaged construction vehicles and sports utility vehicles, and vandalized fast food restaurants in Virginia. In one incident, these individuals vandalized two homes under construction, spray painting “sprawl” on one of the structures. In November 2005, the ELF claimed responsibility for fires set in five townhomes under construction in Hagerstown, MD.²⁹⁷ Similar activity has occurred on the West Coast.²⁹⁸

Guidelines

Both the ALF and the ELF have established guidelines and posted them on the Web for cells or lone wolves to follow. The guidelines are straightforward and short for both movements (see **Figure 2**). A key point in the guidelines for both the ALF and the ELF is to avoid harming any animal, human and non-human.²⁹⁹ The ALF’s guidelines also stipulate that individuals professing affiliation with the movement must be vegetarians or vegans.

Interestingly, the ALF employs a number of caveats in its understanding of violence. On the one hand, it supports intimidation as a tactic. On the other, the movement does not see intimidation as potentially involving violence.³⁰⁰ The ALF also views arson as “violence against property,” not people.³⁰¹ Beyond this, ALF does not greatly elaborate on its notion of violence.

(...continued)

http://www.adl.org/learn/news/San_Diego_Arson.asp; Knickerbocker, “Firebrands”; Chris Dixon, “Arrest in Vandalism of S.U.V.s,” *New York Times*, <http://www.nytimes.com/2004/03/10/us/national-briefing-west-california-arrest-in-vandalism-of-suv-s.html?ref=earthliberationfront>.

²⁹⁷ Federal Bureau of Investigation, *Terrorism 2002-2005*, http://209.235.0.153/publications/terrorism/terrorism2002_2005.htm.

²⁹⁸ “Activists Topple Towers, Claim Dangers of AM Radio Waves,” *CNN.com*, September 4, 2009, http://articles.cnn.com/2009-09-04/justice/washington.towers.terrorism_1_elf-radio-station-radio-waves?_s=PM:CRIME; “Officials: No Explosive Devices Found at Scene of Seattle-Area House Fires,” *Fox News*, March 4, 2008, <http://www.foxnews.com/story/0,2933,334875,00.html>; Debera Carlton Harrell, Aubrey Cohen, and Paul Shukovsky, “‘Street of Dreams’ Houses Torched; Eco-Terrorists Suspected,” *Seattle Post-Intelligencer*, March 4, 2008; “Camano Island Mansion Fire Ruled Ecoterrorist Arson,” *KOMO News.Com*, January 20, 2006, <http://www.komonews.com/news/archive/4175026.html>.

²⁹⁹ For ALF guidelines, see <http://www.animalliberationpressoffice.org/Background.htm>. For ELF guidelines, see http://www.animalliberationfront.com/ALFront/ELF/elf_faq.pdf.

³⁰⁰ *Ibid.*

³⁰¹ See North American Animal Liberation Front, “Frequently Asked Questions About the North American Animal Liberation Press Office,” <http://www.animalliberationpressoffice.org/faq.htm#7>.

Figure 2. ALF and ELF Guidelines

Animal Liberation Front	Environmental Liberation Front
<p>To Liberate animals from places of abuse, i.e. laboratories, factory farms, fur farms, etc., and place them in good homes where they may live out their natural lives, free from suffering.</p> <p>To inflict economic damage to those who profit from the misery and exploitation of animals.</p> <p>To reveal the horror and atrocities committed against animals behind locked doors, by performing direct actions and liberations.</p> <p>To take all necessary precautions against harming any animal, human and non-human.</p> <p>Any group of people who are vegetarians or vegans and who carry out actions according to these guidelines have the right to regard themselves as part of the Animal Liberation Front.</p>	<p>To cause as much economic damage as possible to a given entity that is profiting off the destruction of the natural environment and life for selfish greed and profit,</p> <p>To educate the public on the atrocities committed against the environment and life,</p> <p>To take all necessary precautions against harming life.</p>

Source: CRS graphic based on ALF and ELF guidelines.

Notes: For ALF guidelines, see <http://www.animalliberationpressoffice.org/Background.htm>. For ELF guidelines, see http://www.animalliberationfront.com/ALFront/ELF/elf_faq.pdf

Exceptions

Some animal rights extremists support violence. For example, in February 2012 Meredith Lowell was arrested for allegedly using a Facebook page she created (under an assumed name) to solicit a hit man to kill “someone who is wearing fur.”³⁰² In the investigation, the FBI used an undercover employee to pose as a hit man and communicate with Lowell online. She was arrested before anyone could be harmed.³⁰³

An animal rights extremist entity named the “Justice Department” believes in the efficacy of violence against humans.³⁰⁴ Founded in the United Kingdom in 1993, the “Justice Department” has been described as an offshoot of the ALF.³⁰⁵ In 1999, the first incident claimed in its name on U.S. soil involved the mailing of more than 80 envelopes containing razor blades allegedly positioned to cut recipients. Some of the razors may have been covered in rat poison. The letters were received by animal researchers, hunting guides, and others in the United States and Canada.³⁰⁶ In November 2010, individuals asserting ties to the “Justice Department” mailed two communiqués to NAALPO. The missives claimed that “Justice Department” extremists had

³⁰² James Ewinger, “Cleveland Heights Woman Charged with Using Facebook to Hire Killer,” *Cleveland Plain Dealer*, February 21, 2012, http://blog.cleveland.com/metro/2012/02/heights_woman_charged_with_usi.html.

³⁰³ Ibid.

³⁰⁴ North American Animal Liberation Press Office, press release, “Liberationist Group ‘Justice Department’ Increasingly Vocal on Animal Abuse,” November 23, 2010, http://www.animalliberationpressoffice.org/press_releases/2010/pr_2010_11_23_jd.htm. Hereinafter: NAALPO, “Liberationist Group.”

³⁰⁵ Anti-Defamation League, “Justice Department.”

³⁰⁶ Ibid.; Southern Poverty Law Center, “Eco-Violence: The Record,” *Intelligence Report*, Southern Poverty Law Center, no. 107 (Fall 2002), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2002/fall/from-push-to-shove/eco-violence-the-rec>.

mailed AIDS-tainted razors to two scientists at the University of California, Los Angeles.³⁰⁷ One of the communiqués read:

We are the past generation of animal liberationists, but we will now be the future, striking at the heart of the vivisection industry, and if we have to go back to egg timers and incense [sic] sticks then we will. Mark our words, we will destroy all who fall into our focus.³⁰⁸

Presumably, allusion to egg timers and incense sticks suggests timing devices and fuses for explosive or incendiary devices.³⁰⁹

“Paper Terrorism”: Liens, Frivolous Lawsuits, and Tax Schemes

Sovereign citizens have committed non-violent crimes based on their ideological underpinnings.³¹⁰ These are often bundled under the concept of “paper terrorism.”³¹¹ This concept can include forging documents (fake money orders and bad personal checks, for example), failing to pay taxes, phony tax filings, and presenting sham legal arguments in court. Sovereign citizens have filed fraudulent property liens against their foes.³¹² Some sovereigns hold illegal courts and target officials with fake criminal indictments. They can also “issue warrants for judges and police officers.”³¹³

Retaliatory Filings

While these acts may not be violent, they are frequently “designed to intimidate or defraud targeted individuals, private institutions, or government entities.”³¹⁴ Thus, some sovereigns saddle their opponents with time-consuming legal efforts to wipe out sham retaliatory court filings. As a

³⁰⁷ NAALPO, “Liberationist Group.”

³⁰⁸ Ibid.

³⁰⁹ *Arson-Around*, pp. 16-17 describes assembly of an incendiary device incorporating incense sticks as a fuse. Incense sticks have been used as fuses for incendiary devices by ELF and ALF activists. See Federal Bureau of Investigation, *Terrorism 2000-2001*, 2004, p. 4, <http://www.fbi.gov/stats-services/publications/terror/terrorism-2000-2001> for an example of an ELF incident. For additional examples involving the cell known as “The Family” active with both the ALF and the ELF, see *U.S. v. Dibee et al.* Kitchen timers are discussed in William Rodgers and Stanislas Meyerhoff, *Setting Fires with Electrical Timers: An Earth Liberation Front Guide*, May 2001, pp. 15-17. Although the document lists no authors, DOJ believes that Rodgers and Meyerhoff wrote it. They were members of “The Family” which also used kitchen timers in its incendiary devices. See *United States v. Joseph Dibee et. al*, Indictment, CR 06-60011-AA, District Court, District of Oregon, January 19, 2006.

³¹⁰ Department of Homeland Security and the Federal Bureau of Investigation, *Sovereign Citizen Group Calls for Removal of U.S. Governors*, March 29, 2010, p. 2. Hereinafter: “*Sovereign Citizen Group Calls*.”

³¹¹ For an example of the use of this oft-used term, see Department of Justice, press release, “Member of Anti-Government Movement Pleads Guilty to Laundering Money for FBI Undercover Agents,” March 25, 2011, <http://www.fbi.gov/lasvegas/press-releases/2011/lv032511.htm>.

³¹² One source has defined a lien as “a claim encumbrance or charge on property for payment of a debt or obligation.” Liens can be consensual or nonconsensual. They can be statutory or derive from common law. An example of a nonconsensual common law lien is “when a mechanic refuses to return a car until repairs are paid for.” See Robert Chamberlain and Donald P. Haider-Markel, “‘Lien on Me’: State Policy Innovation in Response to Paper Terrorism,” *Political Research Quarterly*, vol. 58, no. 3 (September 2005), p. 450.

³¹³ Ibid.; Federal Bureau of Investigation, “Sovereign Citizen.” See also: Christopher A. Young, “Minnesota Has New Weapons in the Fight Against ‘Paper Terrorism,’” *Hennepin Lawyer*, August 28, 2007, <http://hennepin.timberlakepublishing.com/article.asp?article=1148>.

³¹⁴ “*Sovereign Citizen Group Calls*,” p. 2.

result, sovereign foes incur court fees and their credit ratings potentially suffer. In some cases, these proceedings arise from what most citizens might consider fairly mundane run-ins with law enforcement authorities. Some sovereigns do not necessarily see violations like parking tickets and trespassing arrests as run-of-the-mill. They can react to such encounters with police by challenging the very authority and jurisdiction of U.S. law enforcement and by harassing officials with dubious liens, for example.

- In November 2011, Kenneth W. Leaming, from Spanaway, WA, was arrested for allegedly issuing billions of dollars in frivolous liens to intimidate public officials enforcing laws against sovereign citizens. Reportedly, he has been tied to other sovereign citizen adherents and groups. Also, he purportedly planned to harass the children of U.S. Supreme Court Chief Justice John Roberts.³¹⁵

Redemption

Sovereign citizen guru Roger Elvick is the reputed founder of “redemption,”³¹⁶ a concept that blurs the line between sovereign citizen ideology and pure scam. Redemption suggests that when the United States left the gold standard during the Great Depression, the nation found a way to monetize people. According to the theory, each child who is born in the United States and has a birth certificate also has a U.S. Treasury account “valued from \$630,000 to more than \$3 million”³¹⁷ viewed as collateral against the nation’s debts. Redemption supporters hold that by filing certain forms with state or federal authorities, people can draw money from these accounts. To do so, they occasionally attempt to pass bogus checks.³¹⁸

On a broad level, redemption can be viewed as an ideologically driven tactic meant to illegally wrangle money from the U.S. government via the IRS. According to DOJ, in some instances this involves the filing of “a series of false IRS forms, including tax returns, amended returns, and

³¹⁵ Levi Pulkkinen, “FBI: Spanaway ‘Sovereign Citizen’ Planned to Track Down Justice’s Children,” *Seattle Post-Intelligencer*, November 28, 2011, <http://www.seattlepi.com/local/article/FBI-Spanaway-sovereign-citizen-planned-to-2299295.php>; Anti-Defamation League, “Little Shell Pembina Band,” http://www.adl.org/learn/ext_us/little_shell.asp?learn_cat=extremism&learn_subcat=extremism_in_america&xpicked=3&item=little_shell. For other examples, see Rick Montgomery, “Sovereign Citizens: Crackpots, Crooks, or Defenders of Liberty?” *Kansas City Star*, November 26, 2011, <http://www.kansascity.com/2011/11/26/3288115/sovereign-citizens-bulldogs-guarding.html>.

³¹⁵ Marnie Eisenstadt, “Fringe Group Terrorizes Small-Town Officials with False Liens,” *The Post Standard*, May 23, 2011; Rick Montgomery, “Sovereign Citizens: Crackpots, Crooks, or Defenders of Liberty?” *Kansas City Star*, November 26, 2011, <http://www.kansascity.com/2011/11/26/3288115/sovereign-citizens-bulldogs-guarding.html>; Marnie Eisenstadt, “Fringe Group Terrorizes Small-Town Officials with False Liens,” *The Post Standard*, May 23, 2011; “Two Admit Scheme to Defraud Public Employees,” *Daily Freeman*, January 14, 2011, <http://www.dailyfreeman.com/articles/2011/01/14/blotter/doc4d2fb54d3189f270459164.txt>; Michael Virtanen, “NY Man’s Sentencing Put Off in Liens Case,” *Associated Press*, July 12, 2011.

³¹⁶ “His ‘Straw Man’ Free, a Scammer Finds the Rest of Him Isn’t,” *Intelligence Report*, Southern Poverty Law Center, Issue 118, (Summer 2005), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2005/summer/patriots-for-profit>. Hereinafter: Southern Poverty Law Center, “His Straw Man Free.”

³¹⁷ FBI Counterterrorism Analysis Section, “Sovereign Citizens.”

³¹⁸ Elvick promoted his ideas in the 1980s, and was jailed for much of the 1990s as well as in the next decade because of passing bad checks, forgery, extortion, and corruption. See *Ibid.*; Southern Poverty Law Center, “His Straw Man Free”; For a description of redemption, see Institute for Intergovernmental Research, *Investigating Terrorism*, pp. 70-71.

Forms 1099 (including Form 1099-OID) or Forms W-2, to request fraudulent tax refunds based on phony claims of large income tax withholding.”³¹⁹

In addition, DOJ describes some redemption adherents as scammers who dupe customers into filing false IRS forms to redeem money via the purported secret accounts the government holds for its citizens.³²⁰ One guru recently pled guilty to money laundering charges.³²¹ In another case, in December 2009 Audie Watson received a 14-year prison sentence for his involvement in an immigration benefit fraud scheme that sold membership in the Pembina Nation Little Shell Band to illegal aliens. Watson and co-conspirators charged individuals \$1,500 and couples \$2,000. They conned clients into believing that membership could be used to avoid removal from the United States.³²²

- In March 2011, DOJ announced that the U.S. District Court for the Western District of Missouri had permanently barred Gerald A Poynter “from preparing tax returns for others and from promoting” a redemption scam.³²³ Poynter informed his customers that he could obtain tax refunds for them, charged them for his services, and then produced fraudulent IRS forms claiming \$64 million in refunds for 165 customers.³²⁴

The Internet and Domestic Terrorists

In the counterterrorism world, there has been much concern regarding violent jihadist use of the Internet.³²⁵ However, domestic terrorists also are computer savvy and active online. One count suggested that 657 U.S.-based hate websites existed in 2010.³²⁶ A Web presence may help extremist groups—sometimes relatively small, with rosters in the 100s or fewer—educate their

³¹⁹ Department of Justice, press release, “Government Files Seven Lawsuits Nationwide to Block Alleged Scheme Involving Fraudulent Tax-Refund Claims,” October 28, 2009, <http://www.justice.gov/opa/pr/2009/October/09-tax-1161.html>.

³²⁰ Ibid.

³²¹ Carri Greer Thevenot, “Idaho Man Pleads Guilty to Money Laundering,” *Las Vegas Review-Journal*, March 25, 2011, <http://www.lvrj.com/news/sovereign-movement-leader-pleads-guilty-to-money-laundering-118685369.html>.

³²² Immigration and Customs Enforcement, press release, “South Florida Man Sentenced to 14 Years in Prison for Immigration Fraud,” December 8, 2009, <http://www.ice.gov/news/releases/0912/091208miami.htm>.

³²³ Department of Justice, press release, “Federal Court Shuts Down Missouri Tax Preparer Who Promoted Tax Scam,” March 28, 2011, <http://www.justice.gov/tax/txdv11382.htm>. For the injunction, see http://www.justice.gov/tax/Poynter_Injunction.pdf.

³²⁴ Ibid.

³²⁵ For example, see Edna Erez, Gabriel Weimann, and A. Aaron Weisburd, “Jihad, Crime, and the Internet: Content Analysis of Jihadist Forum Discussions,” October 31, 2011, Report submitted to the National Institute of Justice in fulfillment of requirements for Award Number 2006-IJ-CX-0038; Akil N. Awan, “The Virtual Jihad: An Increasingly Legitimate Form of Warfare,” *CTC Sentinel*, vol. 3, no. 5 (May 2010), p. 11, <http://www.ctc.usma.edu/sentinel/CTCSentinel-Vol3Iss5.pdf>; Gilbert Ramsay, “Relocating the Virtual War,” *Defence Against Terrorism Review*, vol. 2, no. 1 (Spring 2009), p. 34, http://www.tmmm.tsk.tr/publications/datr3/03_Gilbert%20Ramsay.pdf; Tim Stevens, “Regulating the ‘Dark Web’: How a Two-Fold Approach Can Tackle Peer-to-Peer Radicalisation,” *The RUSI Journal*, vol. 154, no. 2 (Apr. 2009), p. 29; Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenge* (Washington, DC: United States Institute of Peace Press, 2006); Maura Conway, “Terrorism and Mass Communication: Nitro to the Net,” *The World Today*, vol. 60, no. 8/9 (Aug/Sep 2004), pp. 19-22, http://doras.dcu.ie/513/1/nitro_to_net_2004.pdf.

³²⁶ Potok, “The Year,” p. 50. This count included web pages “from Ku Klux Klan, Neo-Nazi, White Nationalist, Racist Skinhead, Christian Identity, Neo-Confederate, Black Separatist, and General Hate groups.”

existing membership and forge a group identity. Also, in many instances they can use websites to focus on outsiders to propagandize, socialize, and recruit new adherents.³²⁷ A few domestic terrorists also have exploited the Web to harm their targets.

White supremacists have long been using computer technology to communicate and interact. As one study has suggested, white supremacists “were among the very early users of the electronic communication network that eventually evolved into the Internet.”³²⁸ Among a variety of findings, the study indicated that white supremacist extremist websites were possibly an effective recruiting tool that the groups exploited. Membership forms are available on some sites. Others exhibit multimedia material, and some actually retail items such as music and video games.³²⁹ The Internet allows individuals and groups to connect with one another and to disseminate ideology.³³⁰ It also enables groups to manage how others perceive them. Many white supremacist sites claim that their sponsoring groups are non-violent and not even racist.³³¹

Some white supremacists may be unwilling to affirm their views in public spaces such as work, school, or in street demonstrations. To them, the virtual realm is an important antidote. As one study has suggested, “free spaces” in both the real and virtual worlds—where conflict with non-believers will be minimized—are important for adherents. In them they can “meet, articulate, and support their views.”³³² Supremacists can turn to virtual free spaces to receive indoctrination into movement culture, key narratives outlining movement grievances, adopt ideologies, and “talk of violence against ‘racial enemies.’”³³³

Much of this online ideological activity involves constitutionally protected speech. A number of examples stand out.

- The ALF and the ELF have their long-established guidelines posted on the Web for independent groups or individuals to follow.³³⁴ Movement websites virtually connect like-minded individuals. As mentioned elsewhere in this report, key ideological texts are also made available online.³³⁵ The websites of animal rights extremists and eco-terrorists also post press releases publicizing crimes perpetrated on behalf of the movements.³³⁶

³²⁷ Jeffrey Kaplan, Leonard Weinberg, and Ted Oleson, “Dreams and Realities in Cyberspace: White Aryan Resistance and the World Church of the Creator,” *Patterns of Prejudice*, vol. 37, no. 2 (2003), pp. 149-150.

³²⁸ Phyllis B. Gerstenfeld, Diana R. Grant, Chau-Pu Chiang, “Hate Online: A Content Analysis of Extremist Internet Sites,” *Analysis of Social Issues and Public Policy*, vol. 3, no. 1, (2003), p. 29. Hereinafter: Gerstenfeld et. al., “Hate Online.”

³²⁹ Ibid.

³³⁰ See Josh Adams and Vincent J. Roscigno, “White Supremacists, Oppositional Culture, and the World Wide Web,” *Social Forces*, vol. 84, no. 2 (December 2005), pp 759-778.

³³¹ Gerstenfeld et. al., “Hate Online,” pp. 33-41.

³³² Pete Simi, Robert Futrell, “Cyberculture and the Endurance of White Power Activism,” *Journal of Political and Military Sociology*, vol. 34, no. 1 (Summer 2006), p. 117. Hereinafter: Simi and Futrell, “Endurance.”

³³³ Ibid., 122-126, 131. Some free spaces exist in the real world. Examples include the privacy of the home, supremacist events such as conferences, isolated compounds or communities, and ideologically-focused musical concerts.

³³⁴ See <http://www.animalliberationpressoffice.org/Background.htm>; ELF, “What Is the Earth?”

³³⁵ Anti-Defamation League, *Ecoterrorism: Extremism in the Animal Rights and Environmentalist Movements*, http://www.adl.org/learn/ext_us/ecoterrorism.asp. Hereinafter: Anti-Defamation League, *Ecoterrorism*.

³³⁶ See <http://www.animalliberationfront.com/>; <http://www.animalliberationpressoffice.org/>; and (continued...)

- Reverend Donald Spitz administers the Army of God's website.³³⁷ Among other things, the site includes lists of people who support "violent opposition to abortion" as well as listing people incarcerated because of anti-abortion crimes they committed.³³⁸
- The National Socialist Movement sponsors its own social networking site, the "New Saxon Social Network."³³⁹

Some domestic terrorists also engage in cyber attacks. According to DOJ, an animal rights extremist cell (SHAC USA, Inc.) active between 2001 and 2004 listed online the personal information—names, addresses, phone numbers—of workers at a firm it was targeting. (The business uses animals in its research.) The extremist cell likely devised the list to help focus the activities of the group's online followers. In some cases, the published information included the names of spouses and children of employees, license plate numbers, churches attended by the employees, as well as the schools their children attended. The websites used by the extremist cell also posted suggestions for action by supporters—including what it described as the "top 20 terror tactics."³⁴⁰ Supporters across the United States vandalized victims' homes and automobiles and engaged in cyber attacks against the research firms and other companies tied to it, among other activities.³⁴¹

In January 2009, in an unclassified assessment available on the Internet, DHS stated that "leftwing" extremists were likely to increasingly use cyber attacks. The assessment noted that animal rights extremists engaged in cyber attacks such as "deletion of user accounts, flooding a company's server with e-mails, and other types of e-mail assaults intended to force businesses to exhaust resources."³⁴²

A Decentralized Threat

Domestic terrorism can be described as a decentralized threat. As this report has already suggested, domestic terrorism suspects generally operate on their own or in small, independent

(...continued)

<http://www.earthliberationfront.org/>.

³³⁷ Jefferis, *Armed for Life*, p. 53.

³³⁸ Ibid., p. 77.

³³⁹ See <http://newsaxon.org/>.

³⁴⁰ Department of Justice, *White Paper*, p. 60; *United States v. Stop Huntingdon Animal Cruelty USA, Inc., et. al*, Superseding Indictment, CR 04-373, District Court, District of New Jersey, n.d. <http://www.justice.gov/usao/nj/press/files/pdf/shacind2.pdf>. Hereinafter: Department of Justice, *United States v. Stop Huntingdon*. The "top 20 terror tactics" included activity such as: "demonstrations at one's [a target's] home using a loudspeaker; abusive graffiti, posters and stickers on one's car and house; invading offices and, damaging property and stealing documents; chaining gates shut, and blocking gates; physical assault including spraying cleaning fluid into one's eyes; smashing the windows of one's house while the individual's family was at home; flooding one's home while the individual was away; vandalizing one's car; firebombing one's car; bomb hoaxes; threatening telephone calls and letters including threats to kill or injure one's partner or children; e-mail bombs in an attempt to crash computers; sending continuous black faxes causing fax machines to burn out; telephone blockades by repeated dialing to prevent the use of the telephone; and arranging for an undertaker to call to collect one's body."

³⁴¹ According to the superseding indictment in the case, the cell also placed reports of intimidation and vandalism on its websites to encourage its followers. See Department of Justice, *United States v. Stop Huntingdon*.

³⁴² Department of Homeland Security, *Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade*, January 26, 2009.

cells. In other words, they do not necessarily belong to organizations with cohesive, well-articulated leadership structures or cadres.

However, independently acting domestic terrorism suspects are not necessarily isolated, adrift, and cut off from any outside contact or influence. Some take ideological cues from broader movements or groups espousing extremist ideas. These groups or movements publicly disavow violent criminal behavior and engage in constitutionally protected activities. This dynamic—the interplay between above-ground groups or movements proffering extremist dogma or ideology (protected speech) that is then consumed and acted upon by independent underground groups or cells who commit crimes—is a critical feature of domestic terrorism.

Leaderless Resistance

Within the domestic terrorism realm, the notions of decentralized activity received attention in the 1980s and early 1990s when white supremacist Louis Beam circulated his theories of “leaderless resistance.”³⁴³ He saw leaderless resistance as a means to transform the white supremacy movement. Beam described it as a means of avoiding law enforcement infiltration of white supremacist groups, and he suggested *two levels* of leaderless movement activity. First, on an operational level, militant, underground, ideologically motivated cells or individuals (lone wolves) engage in movement-related illegal activity without any centralized direction or control from an organization that maintains traditional leadership positions and membership rosters. Second, on another level, the above-ground public face (the “political wing”) of the movement propagandizes and disseminates ideology—engaging in protected speech. In this system, underground cells or lone wolves would be responsible for their own actions, and the public face of the movement would not be held accountable.³⁴⁴

Online comments from the leadership of the neo-Nazi National Socialist Movement (NSM) offer a specific example of an above-ground movement avoiding violence and the terrorist label. The NSM’s leader has posted the following statement on the group’s website:

I want it made perfectly clear to all of our members, supporters, prospective members, readers, etc. that the National Socialist Movement condemns illegal actions and in such we do not endorse any acts of violence or terrorism. The NSM is a White Civil Rights Movement that adheres to Political activism, and a legal means to restore America to its former glory. Acts of violence or terrorism against America, or its Citizens is unacceptable, and not tolerated within the ranks of the National Socialist Movement.³⁴⁵

³⁴³ He was a Ku Klux Klan (KKK) and Aryan Nations activist.

³⁴⁴ Paul Jooose, “Leaderless Resistance and Ideological Inclusion: The Case of the Earth Liberation Front,” *Terrorism and Political Violence*, vol. 19, no. 3 (September 2007), pp 351-368. Hereinafter: Jooose, “Leaderless Resistance.” Fred Burton, “The Challenge of the Lone Wolf,” *STRATFOR*, May 30, 2007, http://www.stratfor.com/challenge_lone_wolf; Hereinafter: Burton, “The Challenge.” Southern Poverty Law Center, “Louis Beam,” <http://www.splcenter.org/get-informed/intelligence-files/profiles/louis-beam>; Anti Defamation League, “Louis Beam,” http://www.adl.org/learn/ext_us/beam.asp?xpicked=2&item=beam. Beam secretly discussed leaderless resistance among white supremacists and anti-government extremists as early as 1983. See Wright, *Patriots*, p. 87. Forms of leaderless resistance likely have a long history. For example, late-nineteenth-century anarchists can be seen as having engaged in a type of leaderless resistance in their rejection of organized authority. See Jean-Marc Flükiger, “The Radical Animal Liberation Movement: Some Reflections on Its Future,” *Journal for the Study of Radicalism*, vol. 2, no. 2 (2009), pp. 112. Hereinafter: Flükiger, “The Radical.” See also: Ramón Spaaij, “The Enigma of Lone Wolf Terrorism: An Assessment,” *Studies in Conflict and Terrorism*, vol. 33, no. 9 (2010), p. 859. Hereinafter: Spaaij, “The Enigma.”

³⁴⁵ Jeff Schoep, “CDR Jeff Schoep Denounces Violence & Domestic Terrorism,” <http://www.nsm88.org/> (continued...)

“The Turner Diaries”

One of the key texts read by neo-Nazis and anti-government extremists is *The Turner Diaries*, a 1978 novel by William Pierce, the deceased founder of the neo-Nazi group National Alliance.³⁴⁶ This book can be seen as an above-ground product that motivates underground cells or individuals to commit crimes. The book has partly inspired a number of violent acts by white supremacist extremists and anti-government extremists.

The Turner Diaries predates the widespread acceptance of the “leaderless resistance” concept. However, its lasting place in the neo-Nazi and anti-government extremist movements highlights how leaderless resistance works. Peirce’s book has been described as “the most widely read book among far-right extremists.”³⁴⁷ The novel reflects the author’s own racist religious philosophies.³⁴⁸ Perhaps 500,000 copies of the book have been sold.³⁴⁹ In it, Pierce emphasized that the current racial order of things had to be cataclysmically destroyed and reborn in accordance with white supremacist ideals.³⁵⁰ To convey this message, he devised his book as the edited diaries of neo-Nazi character Earl Turner. As such, Turner’s story is annotated by a fictionalized editor, one Andrew Macdonald. The novel describes Turner leading a terrorist group whose actions trigger a race war that results in the overthrow of the government—controlled by Jews in Pierce’s construction. Turner also initiates a nuclear war that wipes out earth’s non-white human inhabitants. The atomic apocalypse allows for the rebirth of a revitalized white race.³⁵¹

The book has informed the activities of domestic terrorists. In September 1983, white supremacist Robert Mathews formed a small underground group known as The Order. Its inspiration came from passages in *The Turner Diaries*. The group planned for and engaged in what it viewed as a revolution.³⁵² Over the next 15 months, The Order went on a violent crime spree. Among other crimes, it robbed banks, armored cars, electronic stores, a truck stop, and a video store, and allegedly gave some of the spoils to Richard Butler, who was at the time the leader of the WSE group Aryan Nations. The Order also bombed a synagogue and murdered a Jewish talk show host, Alan Berg, before it was dismantled by federal law enforcement.³⁵³

(...continued)

commandersdesk/.

³⁴⁶ Renee Brodie, “The Aryan New Era: Apocalyptic Realizations in *The Turner Diaries*,” *Journal of American Culture*, vol. 21, no. 3, (fall 1998), pp. 13-22.

³⁴⁷ Anti-Defamation League, “*The Turner Diaries*,” 2005, http://www.adl.org/learn/Ext_US/turner_diaries.asp.

³⁴⁸ See Brad Whitsel, “*The Turner Diaries* and Cosmotheism: William Pierce’s Theology,” *Nova Religio: The Journal of Alternative and Emergent Religions*, vol. 1, no. 2 (April 1998), pp. 183-197. Hereinafter: Whitsel, “*The Turner Diaries*.”

³⁴⁹ Freilich, Chermak, and Caspi, “Critical Events,” p. 505. Another estimate dating back to 2001 places the number sold at 300,000. See Rob McAlear, “Hate, Narrative, and Propaganda in *The Turner Diaries*,” *The Journal of American Culture*, vol. 32, no. 3 (September 2009), p. 192. Hereinafter: McAlear, “Hate, Narrative.”

³⁵⁰ George Michael, “The Revolutionary Model of Dr. William L. Pierce,” *Terrorism and Political Violence*, vol. 15, no. 3 (Autumn 2003), p. 75.

³⁵¹ Whitsel, “*The Turner Diaries*,” p. 185; Terence Ball and Richard Dagger, “*The Turner Diaries*: Neo-Nazi Scripture,” *PS: Political Science and Politics*, vol. 30, no. 4, (December 1997), pp. 717-718. McAlear, “Hate, Narrative,” p. 196.

³⁵² Wright, *Patriots*, pp. 87-88; Anti-Defamation League, “Richard Scutari,” http://www.adl.org/learn/ext_us/scutari.asp?xpicked=2&item=scutari. Hereinafter: Anti-Defamation League, “Scutari.” Zeskind, *Blood and Politics*, pp. 96-100.

³⁵³ Balch, “The Rise and Fall,” 87, 109; Wright, *Patriots*, p. 86-89.

Anti-government extremist Timothy McVeigh, an avid reader of the book, had passages from the *Turner Diaries* with him when he was arrested. The 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City mimicked one described in the novel and involved a small cell of underground conspirators.³⁵⁴ Sales of the book allegedly rose after the bombing.³⁵⁵

The ALF, the ELF

The concept of leaderless resistance has been mirrored by other extremist movements in the United States. Both the ALF and the ELF have rejected recognizable leadership structures or hierarchies and follow a leaderless resistance model instead, making their activities more difficult for law enforcement to investigate.³⁵⁶ According to the model, above-ground elements in the movements provide guidelines and an ideological platform that underground individuals—lone wolves—or independent cells can draw upon to motivate their own criminal actions. Exercising First-Amendment rights, the above-ground components of the ALF and the ELF lawfully communicate shared identities largely via websites. As one scholar has suggested for the ELF, this possibly creates a broad consensus focused on a very specific cause and avoids internecine conflicts over ideological fine points.³⁵⁷ Much like the NSM, the above-ground elements of the ALF take pains to distinguish themselves from criminal activity. For example, NAALPO states:

Disclaimer: The Animal Liberation Press Officers do not engage in illegal activities, nor do they know any individuals who do. Rather, the Press Office receives and posts communiqués from anonymous parties and provides comment to the media.³⁵⁸

Additionally, the above-ground literature of both the ALF and the ELF suggests that independent cells avoid communication with one another.³⁵⁹ This leaderless format is followed to avoid law enforcement infiltration and is based on models used by other domestic terrorists. As one scholar has suggested, this parallels franchising in the business world.³⁶⁰

Lone Wolves

Some domestic terrorists are “lone wolves.” This can be seen as a form of leaderless resistance. One scholar has offered a succinct conceptualization:

Lone wolf terrorism involves terrorist attacks carried out by persons who (a) operate individually, (b) do not belong to an organized terrorist group or network, and (c) whose *modi operandi* are conceived and directed by the individual without any direct outside command hierarchy.³⁶¹

³⁵⁴ McAlear, “Hate, Narrative,” p. 192; Wright, *Patriots*, pp. 6, 10.

³⁵⁵ Freilich, Chermak, and Caspi, “Critical Events,” p. 505.

³⁵⁶ Ackerman, “Beyond Arson,” p. 151.

³⁵⁷ Joosse, “Leaderless Resistance,” p. 352, 354.

³⁵⁸ NAALPO, “History.”

³⁵⁹ Thurston, *The ALF Primer*, p. 1. See also: *United States v. Joseph Dibee et. al*, Indictment, CR 06-60011-AA, District Court, District of Oregon, January 19, 2006; Leader and Probst, “The Earth Liberation Front,” pp. 37-58.

³⁶⁰ Flükiger, “The Radical,” pp. 111-119.

³⁶¹ *Ibid.*, p. 856.

Lone wolves have committed crimes in the names of a number of domestic terrorism movements. For example, according to the FBI, when it comes to violence attributed to white supremacist extremism, lone wolves play a prominent role. Lone wolves filter in and out of WSE groups. They can either get dismissed from these groups because of their “violent tendencies” or voluntarily leave because they find the organizations too passive.³⁶² There is little research on the lone wolf phenomenon and no universally accepted definition of the term.³⁶³

The above definition stresses how lone wolves operate. Just as critical is what they believe. Lone wolves can hew to broader ideological causes and use them to justify their actions.³⁶⁴ This suggests that lone wolves potentially adopt the ideas of broader terrorist movements while not claiming formal membership in them. Divining exactly what “formal membership” constitutes leads to debate regarding whether or not some individuals acted as lone wolves or part of larger movements. For example:

- On January 29, 2010, Scott Roeder was convicted of first-degree murder and two counts of aggravated assault for killing abortion provider George Tiller.³⁶⁵ Roeder allegedly had “connections with militant abortion foes but few formal ties with known groups.”³⁶⁶ Some supporters of abortion rights consider his contacts among anti-abortion adherents as evidence of possible conspiracy.³⁶⁷ Meanwhile, some anti-abortion activists have stressed that Roeder was a lone wolf.³⁶⁸ He remains the only person convicted of Tiller’s murder.

Because lone wolves are not plugged into terrorist organizations, distinguishing them from individuals who commit hate crimes can also be difficult.³⁶⁹ In these cases, as mentioned above, the FBI likely attempts to determine whether the motives involved were personal (hate crime) and not focused on broader ideologies (domestic terrorism).

The Law Enforcement Challenges Posed by Lone Wolves

Lone wolves present particular challenges to law enforcement. Because lone wolves, by definition, operate alone, it can be difficult for law enforcement to assess exactly which radicalized individuals intend to turn their beliefs into action and pursue terrorist activity. One former FBI counterterrorism official has said:

The lone wolf is arguably one of the biggest challenges to American law enforcement. How do you get into the mind of a terrorist? The FBI does not have the capability to know when a

³⁶² Federal Bureau of Investigation, *Rage and Racism*, p. 8.

³⁶³ Spaaij, “The Enigma,” pp. 855-856.

³⁶⁴ Ibid.

³⁶⁵ Sylvester, “Scott Roeder.”

³⁶⁶ Judy L. Thomas, “Was Suspect in Tiller Case a Lone Wolf?” *The Kansas City Star*, June 14, 2009. Hereinafter: Thomas, “Was Suspect?”

³⁶⁷ Amanda Robb, “Not a Lone Wolf,” *Ms. Magazine*, vol. 20, no. 2 (Spring 2010), pp. 26-31.

³⁶⁸ Thomas, “Was Suspect?”

³⁶⁹ Eric Boehlert, “Terrorism or Hate Crime?” *Salon.com*, April 17, 2003, http://dir.salon.com/story/news/feature/2003/04/17/terrorist_act/index.html.

person gets up in middle America and decides: ‘I’m taking my protest poster to Washington or I’m taking my gun.’³⁷⁰

Aside from intent, it is also hard to assess the operational capability of potential lone wolf terrorists—knowledge of explosives, familiarity with firearms, or experience in surveillance, for example.³⁷¹ Lone wolves do not participate in terrorist networks or training camps that can be infiltrated or whose communications can be traced. They do not rehearse their schemes or practice their criminal skills with conspirators who can potentially act as cooperating witnesses. To attempt to overcome these issues, the FBI asserted in 2009 that it was “beginning an extensive study on identified lone offenders to come up with indicators and behavior predictors that investigators can use to assess suspects.”³⁷²

Not all of the news for law enforcement regarding lone wolves is necessarily dire. They have weaknesses. Their lack of tradecraft may make it harder for lone wolves to engage in large-scale attacks. Likewise, lone wolves do not necessarily experience the reinforcement of a closely knit terrorist social network. They cannot rely on others to assist them in any type of complicated plot.³⁷³

Regardless, lone wolf attacks can be lethal. For example, according to one scholarly examination, between 1990 and April 2009, “far-rightists” have been responsible for the deaths of 42 law enforcement officers—most from state and local agencies in the United States. Most of the incidents involved firearms, *and most of the assailants acted alone*.³⁷⁴ Other instances of fatalities have been documented as well. Aside from the 2010 actions of Scott Roeder and the 2009 shooting involving James von Brunn (discussed elsewhere), suspected lone wolves were involved in at least two fatal shooting incidents in 2009, according to media sources and watchdog groups. The individuals involved in these incidents held white supremacist beliefs.

- Richard Poplawski shot and killed three Pittsburgh police officers in April 2009. He has been described as a “white supremacist” lone wolf.³⁷⁵ He had posted anti-government messages on racist websites.³⁷⁶
- On January 21, 2009, Keith Luke allegedly shot and killed two Cape Verdean immigrants and raped and shot a third. Police arrested him before he could attack

³⁷⁰ Gary Fields and Evan Perez, “FBI Seeks to Target Lone Extremists,” *Wall Street Journal*, June 15, 2009, <http://online.wsj.com/article/SB124501849215613523.html>.

³⁷¹ Scott Stewart and Fred Burton, *Lone Wolf Lessons*, STRATFOR, June 3, 2009, http://www.stratfor.com/weekly/20090603_lone_wolf_lessons?ip_auth_redirect=1. Hereinafter: Stewart and Burton, *Lone Wolf*. See also: Steven M. Chermak, Joshua D. Freilich & Joseph Simone Jr., “Surveying American State Police Agencies About Lone Wolves, Far-Right Criminality, and Far-Right and Islamic Jihadist Criminal Collaboration,” *Studies in Conflict and Terrorism*, vol. 33 no. 11 (2010).

³⁷² Federal Bureau of Investigation, “Domestic Terrorism.”

³⁷³ Stewart and Burton, *Lone Wolf*.

³⁷⁴ START, press release, “Background Information: Far-Right Attacks on U.S. Law Enforcement,” April 2009, http://www.start.umd.edu/start/media/Far-Right_Attacks_on_US_Law_Enforcement_PressRelease.pdf. The scholars who developed the information in the press release defined “far-right ideology” as “principles such as fierce nationalism, anti-globalization, suspicions of centralized Federal authority, support for conspiracy theories, and reverence for individual liberties (including gun ownership).”

³⁷⁵ McNulty et al., “Jury Decides.” See also: Anti-Defamation League, “Richard Poplawski.”

³⁷⁶ Hamill, “Man Accused.”

a synagogue, as he planned.³⁷⁷ Luke purportedly informed police that he had decided to go on his spree after reading about “the demise of the white race” on a neo-Nazi website.³⁷⁸ He reputedly said that he was “fighting for a dying race” and that he had been planning the attack for six months.³⁷⁹

The shootings perpetrated by Roeder and von Brunn have been described by the federal government as terrorist acts.³⁸⁰ It is unclear whether the Poplawski and Luke cases are considered as such.

Lone wolves do not necessarily have to focus on gun-related crimes. Kevin Harpham’s case illustrates as much. On March 9, 2011, law enforcement officers arrested Kevin Harpham (discussed elsewhere) and charged him in connection to a bomb concealed in a backpack and placed along the route of a Martin Luther King, Jr. Day March in Spokane, WA. In September 2011, Harpham pled guilty to committing a federal hate crime and attempting to use a weapon of mass destruction.³⁸¹ Media reports and watchdog groups have indicated that Harpham had ties to white supremacists. Allegedly, he was a member of the neo-Nazi National Alliance in 2004. The group denied that he was still a member. Harpham had also been in contact with Paul Mullet, leader of a white supremacist group active in Athol, ID. Mullet said that he and Harpham spoke many times but that the latter never joined Mullet’s group.³⁸² Harpham reportedly made postings on white supremacist websites and read *The Turner Diaries*.³⁸³

Also, lone wolf activity is not solely the domain of purported white supremacists. Another case illustrates the kind of attack a domestic lone wolf animal rights extremist can commit:

³⁷⁷ John Ellement, “DA Says Racism Drove Brockton Killings, Rape,” *Boston Globe*, January 23, 2009, http://www.boston.com/news/local/massachusetts/articles/2009/01/23/da_says_racism_drove_brockton_killings_rape/?page=1.

³⁷⁸ Phillip Martin, “Man Will Face Charges After Police Standoff,” *WGBH*, April 4, 2011, <http://www.wgbh.org/articles/-2503>.

³⁷⁹ Maureen Boyle, “Prosecutor: Suspect in double slaying in Brockton hatched an ‘Evil Plan of Mass Murder and Rape,’” *Brockton Enterprise*, January 22, 2009, updated June 9, 2010, <http://www.enterpriseneews.com/archive/x1898857767/Shots-fired-at-Brockton-police-cruiser#ixzz1K05tOtW6>.

³⁸⁰ Both von Brunn and Roeder are included in the National Counterterrorism Center’s Worldwide Incidents Tracking System (WITS) database that compiles worldwide terrorist incidents. Poplawski is not.

³⁸¹ Department of Justice, press release, “Attempted Bomber Pleads Guilty to Federal Hate Crime and Weapons Charge,” September 7, 2011, http://www.justice.gov/usao/wae/news/2011/2011_09_07_Harpham_Plea.html; Department of Justice, press release, “Attempted Bomber Arrested,” March 9, 2011, <http://seattle.fbi.gov/dojpressrel/pressrel11/se030911.htm>.

³⁸² See Southern Poverty Law Center, “Spokane Bombing Arrest Details Emerge,” March 9, 2011, <http://www.splcenter.org/blog/2011/03/09/update-spokane-bombing-arrest-details-emerge/>. Hereinafter: Southern Poverty Law Center, “Spokane Bombing.” Thomas Clouse and Meghann M. Cuniff, “White Supremacist Arrested in MLK Bomb Plot,” *Spokesman-Review*, March 10, 2011, <http://www.spokesman.com/stories/2011/mar/10/arrest-in-bomb-plot/>; Hereinafter: Clouse and Cuniff, “White Supremacist”; Joel Millman and Evan Perez, “Suspect Is Arrested in Spokane Bomb Case,” *Wall Street Journal*, March 10, 2011, <http://online.wsj.com/article/SB10001424052748704132204576190820122057388.html>. Hereinafter: Millman and Perez, “Suspect Is Arrested.”

³⁸³ Federal Bureau of Investigation, press release, “MLK Parade Bomber,” January 13, 2012, http://www.fbi.gov/news/stories/2012/january/hatecrime_011312/hatecrime_011312?utm_campaign=email-Immediate&utm_medium=email&utm_source=seattle-top-stories&utm_content=62754; Jessica Robinson, “Court Documents Reveal Evolution Of MLK Day Bomber’s Racist Beliefs,” *Northwest News Network*, December 1, 2011, <http://kuow.org/northwestnews.php?storyID=143023416>; Department of Justice, press release, “Colville, Wash., Man Indicted for Federal Hate Crime in Attempted Bombing of the MLK Unity March,” April 21, 2011, <http://www.justice.gov/opa/pr/2011/April/11-crt-509.html>; “FBI: Bomb Found on MLK March Route,” *MSNBC*, January 18, 2011, http://www.msnbc.msn.com/id/41139894/ns/us_news-crime_and_courts/.

- In November 2010, Walter Bond pled guilty to two felonies stemming from an April 2010 arson that destroyed a store known as the Sheepskin Factory in Glendale, CO.³⁸⁴ Speaking from jail, Bond condemned the business, which sold sheepskin products, as engaging in “blood trade” and drawing profits “from the death and exploitation of suffering animals.”³⁸⁵ Bond worked alone. A web posting claimed the arson “in defense and retaliation for all the innocent animals that have died cruelly at the hands of human oppressors.”³⁸⁶ Apparently, Bond strongly identified with the notion of being a lone wolf. The ATF, working with a confidential informant, recorded Bond discussing the fire and the fact that he actually used the nickname “Lone Wolf.”³⁸⁷ In a jailhouse letter, Bond stated, “I used the name ‘ALF Lone Wolf’ in the media to convey to my ALF brothers and sisters worldwide (whoever they are) the power of acting alone.”³⁸⁸

Prison Radicalization

As some experts have pointed out, prison offers an environment in which individuals can potentially radicalize³⁸⁹ on the way to becoming terrorists. This issue has loomed large among experts examining international terrorism.³⁹⁰ A scholar of the prison radicalization phenomenon in the United Kingdom notes that jail time potentially jump starts the radicalization process for individuals who are at risk of radicalizing. Prison brings together disaffected people who may be receptive to anti-social messages offering “clear, albeit intolerant, solutions to complex problems of identity and belonging.”³⁹¹ In other words, some disaffected prisoners may discover and adopt terrorist ideals as they try to find meaning behind bars, potentially establishing bonds with like-

³⁸⁴ Yesenia Robles, “Vegan Activist Pleads Guilty to Torching Sheepskin Factory,” *Denver Post*, November 19, 2010, http://www.denverpost.com/news/ci_16653821. Hereinafter: Robles, “Vegan Activist.”

³⁸⁵ “Suspect in Arson at Sheepskin Factory in Glendale Decries Animal ‘Blood Trade,’” *Denver Post*, August 6, 2010, http://www.denverpost.com/news/ci_15691097.

³⁸⁶ Robles, “Vegan Activist.”

³⁸⁷ *United States v. Walter Bond*, Criminal Complaint, MJ-01120-MJW, District Court, District of Colorado, July 23, 2010. Hereinafter: *U.S. v. Walter Bond*.

³⁸⁸ Walter Bond, “I Am the ALF ‘Lone Wolf,’” December 4, 2010, http://www.animalliberationpressoffice.org/essays/2010-12_bond_lonewolf.htm. He was also convicted for two other arsons. See “Walter Bond Sentenced to 7 years for two ALF Arsons,” <http://www.animalliberationfrontline.com/walter-bond-sentenced-to-seven-years-for-animal-liberation-front-arsons/>; Scott Stewart, Escalating Violence from the Animal Liberation Front,” STRATFOR, July 29, 2010, http://www.stratfor.com/weekly/20100728_escalating_violence_animal_liberation_front?ip_auth_redirect=1. See also: *U.S. v. Walter Bond*.

³⁸⁹ For this report, “radicalization” describes the process of acquiring and holding radical or extremist beliefs. “Terrorism” describes violent or illegal action taken on the basis of radical or extremist beliefs.

³⁹⁰ Neumann, *Prisons and Terrorism*. James Brandon, “The Danger of Prison Radicalization in the West,” *Combating Terrorism Center Sentinel*, vol. 2, no. 12 (December 2009), p. 4, <http://www.ctc.usma.edu/posts/the-danger-of-prison-radicalization-in-the-west>. Hereinafter: Brandon, “The Danger of Prison.” Greg Hannah, Lindsay Clutterbuck, and Jennifer Rubin, *Radicalization or Rehabilitation: Understanding the Challenges of Extremist and Radicalized Prisoners*, RAND Europe, Cambridge, U.K., 2008, http://www.rand.org/pubs/technical_reports/2008/RAND_TR571.pdf; U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Prison Radicalization: Are Terrorist Cells Forming in U.S. Cell Blocks?* 109th Cong., 2nd sess. September 19, 2006, S. Hrg. 109-954 (Washington: GPO, 2007), pp. 1-6, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:30597.pdf; George Washington University Homeland Security Policy Institute (HSPI) and The University of Virginia Critical Incident Analysis Group (CIAG), “Out of the Shadows: Getting Ahead of Prisoner Radicalization,” HSPI and CIAG, Washington, DC. September 2006, http://www.healthsystem.virginia.edu/internet/ciag/publications/out_of_the_shadows.pdf.

³⁹¹ James Brandon, “The Danger of Prison” p. 4.

minded people in jail. Another study of government policies on prison radicalization in 15 countries (including the United States) concludes that “[w]hether or not one believes that prisons have become Al Qaeda’s ‘universities’ or ‘finishing schools’ there can be no question that prisons matter.”³⁹² They matter because they have figured largely in the development of many previous radical movements around the globe. Prisons also unsettle prisoners who “are more likely than elsewhere to explore new beliefs and associations.”³⁹³

Some prison gangs delve into radical or extremist ideologies that also motivate domestic terrorists, and in a number of instances, these ideologies are integral to fashioning cohesive group identities within prison walls. It must be reiterated, however, that even for gangs exhibiting these ideological dimensions, criminal enterprises such as drug trafficking—not radical beliefs—largely drive their activities. The largest white supremacist prison gangs illustrate this.

Several gangs in America’s penal institutions subscribe to white supremacist beliefs, views broadly shared by some domestic extremist groups such as the National Socialist Party, the National Alliance, Aryan Nations, and racist skinheads. A national-level gang of this ilk with approximately 15,000 members in and out of prison, the Aryan Brotherhood, has factions within facilities managed by the California Department of Corrections and the Federal Bureau of Prisons.³⁹⁴ The Nazi Low Riders, a regional-level gang with a membership estimated between 800 and 1,000, exists in correctional facilities on the West Coast and in the Southwest.³⁹⁵ Another white supremacist gang with a prison and street presence, Public Enemy Number One—largely a local-level organization with between 400 and 500 members—is mostly active in California with scattered groups outside of the state.³⁹⁶

These three groups may espouse racial hatred, but they are largely guided by the profit motive, not extremism.³⁹⁷ For example, one expert has described the Aryan Brotherhood’s ideological underpinnings as “mostly just a good recruiting tool and a way to maintain structure and discipline. These guys are more about making money than starting any kind of white revolution.”³⁹⁸ As another indicator of the primacy of profit, members of all three white supremacist groups often set aside their racism and “have working relationships with Hispanic street gangs and non-white prison gangs such as the Mexican Mafia, due to a shared interest in criminal activity, particularly the drug trade.”³⁹⁹ However, members of racist gangs do commit

³⁹² Neumann, *Prisons and Terrorism*, p. 7.

³⁹³ Ibid.

³⁹⁴ Department of Justice “Prison Gangs and Photos,” <http://www.justice.gov/criminal/ocgs/gangs/prison.html>; “Member of Aryan Brotherhood Booked in Slidell,” *Associated Press State and Local Wire*, October 6, 2009; David Holthouse, “Smashing the Shamrock,” *Intelligence Report*, Southern Poverty Law Center, Issue 119, (Fall 2005), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2005/fall/smashing-the-shamrock?page=0,1>. Hereinafter: Holthouse, “Smashing.”

³⁹⁵ Ibid. For the description of the Aryan Brotherhood as a “national” prison gang, the Nazi Low Riders as a “regional” prison gang, and Public Enemy Number One as a “local” prison gang, see National Drug Intelligence Center, *Attorney General’s Report to Congress on the Growth of Violent Street Gangs in Suburban Areas*, (April 2008), Appendix B, <http://www.justice.gov/ndic/pubs27/27612/appendb.htm#start>.

³⁹⁶ Ibid. See also: Pete Simi, Lowell Smith, and Ann M. S. Reeser, “From Punk Kids to Public Enemy Number One,” *Deviant Behavior*, vol. 29, no. 8 (2008), pp. 753-774. Hereinafter: Simi et al., “From Punk.”

³⁹⁷ Freilich, Chermak, and Caspi, “Critical Events,” p. 508; Holthouse, “Smashing”; Camille Jackson, “Nazi Low Riders,” *Intelligence Report*, Southern Poverty Law Center, Issue 114, (Summer 2004), <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2004/summer/nazi-low-riders>.

³⁹⁸ Holthouse, “Smashing.”

³⁹⁹ Anti-Defamation League, *PEN1, Public Enemy Number 1: California’s Fastest Growing Racist Gang*, (2007), p. 7, (continued...)

hate crimes. For example, in 1998 “[t]wo of the three men who murdered James Byrd Jr., a black man, by tying him to their pickup truck and dragging him over three miles of road near Jasper, Texas, were ex-cons who belonged to the [Aryan] Brotherhood.”⁴⁰⁰

One study has estimated that “hundreds, possibly thousands” of sovereign citizens have been incarcerated in the United States since the 1990s, where some have continued to practice their beliefs and even pass their knowledge on to other prisoners.⁴⁰¹ An unknown number of prisoners have converted to the movement’s ideology, while others have simply used sovereign tactics.⁴⁰² The following cases suggest how this may occur.

- In September 2010, Marlon T. Moore pled guilty to one count of filing a false claim with the IRS, requesting a fraudulent refund of \$9,087,987.95.⁴⁰³ Prior to his 2010 guilty plea, he had become a sovereign citizen during a six-year stint in prison on drug-related money laundering charges.⁴⁰⁴
- In 1992, James T. McBride discovered sovereign citizen ideology while in a Michigan prison on drug-related charges. After he left prison, among other things, he became a sovereign guru and operated a business that peddled sovereign ideas.⁴⁰⁵

Policy Considerations for Congress

Congress may choose to consider issues in three areas regarding the federal role in combating domestic terrorism: (1) assessing this threat’s scope, (2) the adequacy of domestic terrorism intelligence collection efforts, and (3) how domestic terrorism fits into the Obama Administration’s efforts to counter radicalization that may lead to terrorism.

Scoping the Threat

As this report suggests, at least three factors may make it hard for policymakers to form a baseline evaluation of the domestic terrorism threat from publicly available information. First, federal agencies employ varying terminology to describe the threat. Second, the federal government lacks a public and official method for either designating specific domestic groups as terrorists or formally and openly describing particular extremist movements as threats. Finally,

(...continued)

http://www.adl.org/learn/ext_us/peni_report.pdf; Simi et al., “From Punk,” p. 765.

⁴⁰⁰ Leah Nelson, “Fugitive with ties to Aryan Brotherhood Captured,” August 20, 2010, Southern Poverty Law Center, <http://www.splcenter.org/blog/2010/08/20/fugitives-with-ties-to-aryan-brotherhood-captured/>.

⁴⁰¹ Anti-Defamation League, *The Lawless*, p. 12.

⁴⁰² Anti-Defamation League, *The Lawless*, p. 13.

⁴⁰³ Department of Justice, press release, “Miami-Dade Man Pleads Guilty to Filing a False Claim with the IRS for More Than \$9 Million,” September 10, 2009.

⁴⁰⁴ Anti-Defamation League, *The Lawless*, p. 13. See also: Tim Elfrink, “Did Fringe Movement Sovereign Citizens Trick a Miami Man into Filing a \$14 Trillion Tax Return?” *Miami New Times*, March 4, 2010.

⁴⁰⁵ Andrew Welsh-Huggins, “Sovereign Citizens—A 21st Century Counter Culture,” *Associated Press*, available from MSNBC, August 12, 2010, http://www.msnbc.msn.com/id/38668124/ns/us_news-life/t/sovereign-citizens-st-century-counter-culture/.

there is no clear sense of how many domestic terrorism plots and attacks the government has investigated in recent years.

Terminology

The federal government has used broad conceptualizations to describe domestic terrorism. DOJ discusses the issue in terms of a handful of general “threats” such as animal rights extremists, eco-terrorists, anarchists, and anti-government extremists—not specific groups. Additionally, terms such as “terrorism” and “extremism” appear to be used interchangeably. Presumably, using the term “extremist” allows lawyers, policymakers, and investigators the flexibility to discuss terrorist-like activity without actually labeling it as “terrorism” and then having to prosecute it as such. However, this may lead to inconsistencies in the development and application of the law in the domestic terrorism arena. For example, policymakers may ponder why a specific terrorism statute covers ideologically motivated attacks against businesses that involve animals,⁴⁰⁶ while there are no other domestic terrorism statutes as narrow in their purview covering a particular type of target and crime.

Designating Domestic Terrorist Groups

The federal government lacks a process for publicly designating domestic terrorist organizations. In other words, there is no official open-source roster of domestic groups that the FBI or other federal agencies target as terrorist organizations. *The lack of such a designation may spring partly from First Amendment concerns.* Such a list might discourage speech and expression related to the ideologies underpinning the activities of named groups. Regardless, this stands in stark contrast to the world of international counterterrorism, where the United States maintains a well-established—legally and procedurally proscribed—regimen regarding the identification of foreign terrorist organizations (FTOs).⁴⁰⁷

Official FTO designation benefits counterterrorism efforts in a number of ways. Most importantly, it facilitates the prosecution of those who provide material support⁴⁰⁸ to listed foreign terrorist groups. Arguably, because there is no domestic terrorism equivalent of FTO designation, it is more difficult to press material support charges against domestic terrorists. In 2010, one scholar was unable to identify any material support cases involving “a domestic terrorist group or its supporters.”⁴⁰⁹ According to the Department of State, FTO designation has other effects. It

1. Supports [U.S.] efforts to curb terrorism financing and to encourage other nations to do the same.
2. Stigmatizes and isolates designated terrorist organizations internationally.
3. Deters donations or contributions to and economic transactions with named organizations.
- 4.

⁴⁰⁶ The Animal Enterprise Terrorism Act (P.L. 109-374).

⁴⁰⁷ Department of State, “Foreign Terrorist Organizations.”

⁴⁰⁸ As described in U.S. Code, Title 18, Part I, Chapter 113B, 2339A and 2339B. For more information, see CRS Report R41333, *Terrorist Material Support: An Overview of 18 U.S.C. 2339A and 2339B*, by Charles Doyle. DOJ has used material support charges as a key component in its prosecutions against foreign terrorist organizations. See CRS Report R41416 for a discussion of a number of these cases targeting homegrown jihadists.

⁴⁰⁹ Heller, “Designating Domestic,” p. 70. It may be possible to use 18 U.S.C. 2339A to prosecute an individual engaged in domestic terrorism. This statute “restricts aid to perpetrators of terrorism in general.” See Benjamin Yaster, “Resetting Scales: An Examination of Due Process Rights in Material Support Prosecutions,” *New York University Law Review*, vol. 83, no. 4 (October, 2008), p. 1364; and *ibid*.

Heightens public awareness and knowledge of terrorist organizations. 5. Signals to other governments our concern about named organizations.⁴¹⁰

This description suggests that the absence of a designation regimen for domestic terrorist groups makes it harder for the federal government to discredit such groups and simultaneously strengthen public understanding of the domestic terrorist threat. Likewise, the lack of a list might make it more difficult for the federal government to communicate exactly what the threat is to its own agencies, let alone local or state entities.

While there is no official designation process for domestic terrorist *organizations*, as it stands, DOJ and the FBI have publicly named and discussed domestic terrorism *threats*—such as animal rights extremism or anarchist extremism—without illuminating exactly how they arrive at these categories. Federal lawmakers may opt to consider the feasibility of officially formalizing this process and/or opening it up to greater oversight. Ideally, an attempt to render this process less bureaucratically opaque would simultaneously (1) enhance federal efforts to combat domestic terrorism while (2) protecting civil rights and civil liberties. For example, such a list may potentially offer agencies outside of DOJ—including relevant players at the state and local level—formal opportunities to provide input into ranking domestic terrorism threats while enshrining mechanisms by which individuals who believe in the philosophies undergirding a designated threat could petition to have that threat “de-listed.”⁴¹¹ On the other hand, making this process more open may take away the FBI’s flexibility to rapidly adapt its domestic terrorism priorities, especially if threats quickly mutate.

A Public Accounting of Plots and Incidents

A publicly available official accounting of domestic terrorist plots and incidents may help policymakers understand the scope of the threat in lieu of a regimen designed to name domestic terrorism organizations. However, the federal government does not produce such a document. The source that comes closest to providing an official record of domestic terrorism incidents is the National Counterterrorism Center’s (NCTC) Worldwide Incidents Tracking System (WITS)—a database that includes basic information regarding numerous terrorism incidents that have occurred throughout the world. WITS also *does not include* plots foiled by law enforcement. NCTC’s public measure of terrorist incidents also may underestimate the scope of the domestic terrorist threat since 9/11.

- FBI has made specific claims regarding levels of violence among white supremacist extremists, and these are not borne out in WITS. As mentioned earlier, an unclassified FBI intelligence bulletin estimates that 53 acts of violence were committed by what it calls “white supremacist extremists” between 2007 and 2009 in the United States. Why did these cases fail to make it into WITS?
- Likewise, in February 2012 the FBI announced that sovereign citizen convictions increased from 10 in 2009 to 18 in both 2010 and 2011.⁴¹² These are not reflected in WITS. (Presumably, many were foiled plots.)

⁴¹⁰ Department of State, “Foreign Terrorist Organizations.”

⁴¹¹ The FTO designation process has such provisions. See *ibid.*

⁴¹² Patrick Temple-West, “Anti-Government Extremists Opposed to Taxes and Regulations Pose a Growing Threat to Local Law Enforcement Officers in the United States, the FBI Warned on Monday,” *Reuters*, February 6, 2012, <http://www.reuters.com/article/2012/02/07/us-usa-fbi-extremists-idUSTRE81600V20120207>.

- Additionally, an unclassified 2008 DHS report counted more than 40 criminal acts from 2004 to early March 2008 allegedly perpetrated by people involved in the animal rights extremist and eco-terrorist movements in a table of *selected* incidents.⁴¹³ Many of these did not make the cut for inclusion in WITS.

However, a fuller accounting of domestic terrorism plots and attacks may call prosecutorial flexibility into question. Such an accounting may reveal the instances in which FBI *investigated* individuals as domestic terrorists but DOJ did not *prosecute* them as such.

Better Sense of Scope May Assist Policymakers

Regardless, a better sense of domestic terrorism's scope publicly proffered by the federal government may assist policymakers. It may be of policymaking value for executive branch agencies to release annual statistics on domestic terrorism prosecutions, naming individuals and movements involved. Congress may also consider requesting an even more detailed annual public report that counts and describes the domestic terrorist plots dismantled; the number of attacks investigated; and the federal, state, and local agencies involved. Until 2005, the FBI used to regularly release a report that catalogued annual terrorist plots and incidents in the United States.⁴¹⁴ The lack of such an accounting makes it difficult for policymakers to exercise oversight by comparing the levels of domestic terrorist activity against items such as homegrown violent jihadist activity and other threats to the homeland. A regular public accounting could also help policymakers assess the effectiveness of the government's response to the domestic terrorist threat. It may also assist policymakers who wish to compare one domestic terrorist threat against another. Finally, without a clear, publicly available understanding of the domestic terrorist threat, it may be difficult to measure how much federal funding is allocated to this issue.

Intelligence

Intelligence collection efforts against foreign terrorist groups have received much scrutiny since 9/11. U.S. efforts to gather information versus domestic terrorism actors have not. Domestic terrorism does not feature in the Director of National Intelligence's National Intelligence Priorities Framework (NIPF), described as the "means to capture issues of critical interest to senior Intelligence Community (IC) customers and communicating those issues to the IC for action."⁴¹⁵ Importantly, for intelligence gathering and program prioritization purposes, "there is no ... standard across federal agencies that can be applied to [domestic terrorism] cases."⁴¹⁶ Also, there likely is no established standard for the collection of intelligence from state and local investigators.⁴¹⁷ Congress may choose to examine these issues as well as the scope of intelligence collection efforts focused on domestic terrorism.

⁴¹³ Department of Homeland Security, *Ecoterrorism*, Table 1. WITS starts its incident count in 2004.

⁴¹⁴ See <http://www.fbi.gov/stats-services/publications/terrorism-2002-2005>.

⁴¹⁵ See <http://www.dni.gov/content/AT/NIPF.pdf>; Department of Justice, *FBI FY2012 Authorization and Budget Request for Congress*, February 2011, p. 4-24, <http://www.justice.gov/jmd/2012justification/pdf/fy12-fbi-justification.pdf>. Hereinafter: Department of Justice, *FBI FY2012 Authorization*.

⁴¹⁶ Department of Justice, *FBI FY2012 Authorization*, p. 4-24.

⁴¹⁷ Aside from suspicious activity reporting. For more information on this, see CRS Report R40901, *Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress*, by Jerome P. Bjelopera.

By law, “NCTC serves as the primary organization in the United States Government ... for integrating and analyzing all intelligence pertaining to counterterrorism (except for information pertaining exclusively to domestic terrorism).”⁴¹⁸ Because of its lead status for counterterrorism investigations in the homeland, the FBI arguably serves the parallel role for the domestic terrorist threat. The development of any *interagency* regimen for the collection and analysis of domestic terrorism information might start with the Bureau’s capacities in this regard. Congress may wish to consider whether the FBI has allocated appropriate resources and expended enough effort in collection and analysis of domestic terrorism-related intelligence as well as the safeguarding of civil rights.

How Does Domestic Terrorism Fit into the U.S. Countering Violent Extremism Strategy?

In August 2011, the Obama Administration released a strategy for countering the radicalization of terrorists, also described as combating violent extremism (CVE).⁴¹⁹ This document was fleshed out to a degree by the Administration’s release in December 2011 of its “Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States.”⁴²⁰ The Administration’s CVE strategy and plan revolve around countering the radicalization of all types of potential terrorists, but the radicalization of *violent jihadists* is its key focus. Regardless, domestic terrorism falls under the strategy’s purview.

Federal CVE efforts often depend on government agencies cooperating with local groups. In fact, the Obama Administration’s national CVE strategy highlights a “community-based approach” for the federal government. To this end, the strategy states that the federal government most effectively acts as a “facilitator, convener, and source of information.”⁴²¹ As all of this may suggest, to date the bulk of federal-level CVE work has revolved around *community engagement*.⁴²² Congress may opt to ask the Administration which domestic terrorists it will focus on under the strategy and which communities it intends to engage regarding issues surrounding non-jihadist terrorism.

⁴¹⁸ See “About the National Counterterrorism Center,” http://www.nctc.gov/about_us/about_nctc.html.

⁴¹⁹ *Empowering Local Partners to Prevent Violent Extremism in the United States*, August 2011, http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf. Hereinafter: *Empowering Local Partners*.

⁴²⁰ *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*, December 2011, <http://www.whitehouse.gov/sites/default/files/sip-final.pdf>. Hereinafter: *Strategic Implementation Plan*.

⁴²¹ *Empowering Local Partners*, p. 3.

⁴²² See CRS Report R41416, for more information.

Author Contact Information

Jerome P. Bjelopera
Specialist in Organized Crime and Terrorism
jbjelopera@crs.loc.gov, 7-0622

From: [REDACTED]
To: [IA.HCTD.EXECSEC](#); (b) (6)
Subject: FW: Countering Violent Extremism Programs and Initiatives Report - Due COB 2/12/16
Date: Tuesday, February 09, 2016 8:08:04 AM
Attachments: [DHS CVE Action Plan 08 21 2015 FINAL.docx](#)
[CVE Interagency Budget Data FY16 Revised.xlsx](#)
Importance: High

Good Morning (b) (6)

We just received this tasker last evening concerning CVE. I will work this morning to provide the budgetary data, however we need your division to review the "Budget Data" file and note which areas are part of your mission with regards to CVE. I will be happy to review this with you. We need this completed today. If we could meet early this afternoon to discuss and review?

Thank you!

(b) (6)

[REDACTED]
Budget Analyst
Office of Intelligence & Analysis
Budget Office

(b) (6)

From: (b) (6)
Sent: Monday, February 08, 2016 5:09 PM
To: Budget Officers Principals [REDACTED]; DHS Budget Officers [REDACTED]

Cc: (b) (6)

Subject: Countering Violent Extremism Programs and Initiatives Report - Due COB 2/12/16
Importance: High

Budget Officers

Below and attached you will find the data call related to personnel costs and funding levels for Countering Violent Extremism Programs and Initiatives in FY 2016 mapped to the recently outlined in the DHS CVE Action Plan.

Background: In order to ensure the United States is positioned to counter homegrown violent extremism and prevent domestic radicalization, the House Report directs the Office of Community Partnerships to provide a detailed description of all DHS countering violent extremism (CVE) programs and initiatives, including associated personnel and funding levels, not later than 60 days

IA_00357

after the date of enactment of the DHS appropriation.

In the attached file, the CVE Interagency Budget Data is divided into 4 different portions:

- **CVE Program Funding Levels:** Each component should provide a brief summary of the CVE program or exercise that they funded.
- **FY16 Plan Budget:** Each component should provide an estimate of their funding of CVE programs for FY2016.
- **Salaries and Benefits:** Each component should provide the planned amount for FY 16 for salaries and benefits for CVE related work.

Attached is the DHS CVE Action Plan for your information. If you have any questions regarding this data call, please contact [REDACTED] @ (b) (6) [REDACTED]

Please provide your completed file to [REDACTED] by COB, 2/9/16. Negative replies are requested.

Thanks,

[REDACTED]

[REDACTED]

Budget Director
Office of the Chief Financial Officer
U. S. Department of Homeland Security

[REDACTED]

From: [REDACTED]
To: [Field Ops \(ALL\)](#)
Subject: FW: FYI - 1107967 - CVE letter
Date: Monday, September 28, 2015 3:12:11 PM
Attachments: [9282015_30003PM_15-3720 - S1 Signed Memo - Building Community Partnerships to Counter Violent Extremism.pdf](#)

FYSA

-----Original Message-----

From: [REDACTED]
Sent: Monday, September 28, 2015 3:09 PM
To: (b) (6)
Subject: FW: FYI - 1107967 - CVE letter

[REDACTED]
Wanted to share - I assume you will start getting questions on this since the press release went out today.
[REDACTED]

-----Original Message-----

From: IGA ExecSec2
Sent: Monday, September 28, 2015 3:06 PM
To: (b) (6)
Cc: CVE Coordinator ExecSec; IGAExecSec
Subject: FYI - 1107967 - CVE letter

(b) (6)

Sending along this FYI- also adding CVE.

-----Original Message-----

From: (b) (6)
Sent: Monday, September 28, 2015 2:21 PM
To: IGAExecSec [REDACTED]
Subject: Information Copy from Nancy Clark for ESEC Workflow # 1107967 (Contact 1107967) (Intranet Quorum IMA004809658)

All: Please provide Attachment 1 to your Leadership. Please confirm receipt. Thank you.
[REDACTED]

From: [DHS.IGA](#)
To: [DHS.IGA](#)
Subject: FACT SHEET: COUNTERING VIOLENT EXTREMISM TASK FORCE
Date: Friday, January 08, 2016 1:00:05 PM
Attachments: [@](#)

DOJ Office of Public Affairs

202.514.2007

DHS Office of Public Affairs

202.282.8010

Fact Sheet

Jan. 8, 2016

COUNTERING VIOLENT EXTREMISM TASK FORCE

Since the White House Summit on Countering Violent Extremism (CVE) last February, the United States Government has focused on strengthening our effort to prevent extremists from radicalizing and mobilizing recruits, especially here at home. Advancing this effort means working as effectively as possible across the U.S. Government, which is why we are forming the CVE Task Force.

"Countering violent extremism has become a homeland security imperative, and it is a mission to which I am personally committed," said Secretary of Homeland Security Jeh Johnson. "At the Department of Homeland Security, our Office of Community Partnerships – which I established last year to take the Department's CVE efforts to the next level – has been working to build relationships and promote

information



INFORMATION SHARING ENVIRONMENT

Sharing



ISE INFORMATION SHARING ENVIRONMENT

Annual Report to The Congress

Prepared by the
Program Manager, Information Sharing Environment

30 June 2011

IA_00361

The threats against the American people and our institutions have compelled us to accelerate responsible information sharing across every level of government. The operators, analysts, and investigators who protect our nation need access to the right information at the right time, shared in a secure manner.

Threats do not differentiate between departmental or jurisdictional borders; rather, they are dynamic, often seeking to exploit those boundaries. We must work together, to standardize how we interact, to share best practices and to provide oversight and guidance across every level of government. I am proud to report that the Information Sharing and Access Interagency Policy Committee (ISA IPC) and other governance bodies have made great strides in institutionalizing common standards and solutions. This governance, policy, and strategy structure, which includes broad leadership from across the Federal Government, as well as participation from state, local, and tribal representatives, is a key component of the ISE and has been and will continue to be a driving factor in its success.

- The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) continues to implement standardized processes and policies that provide federal, state, local, and tribal law enforcement with the capability to share timely, relevant SAR information that has a potential nexus to terrorism, while ensuring that the privacy, civil rights, and civil liberties of Americans are protected.
- The PM-ISE, in coordination with federal partners, led the first nationwide Baseline Capabilities Assessment (BCA) of the national network of fusion centers (National Network). The BCA evaluated the maturity of the fusion centers' capabilities and identified gaps in an effort to aid fusion centers in better receiving, analyzing, disseminating, and gathering threat information for state, local, tribal, and territorial agencies. The results of the BCA led our partners to develop a Critical Operational Capabilities Gap Mitigation Strategy, which now guides efforts to build and strengthen capabilities in these critical areas.
- The ISE partners have accelerated the development and adoption of common standards and shared approaches to interoperable architectures through industry engagement and sharing of best practices across all levels of government.

We detail many other areas of progress in this Report, including improving the interoperability of our nation's Sensitive But Unclassified (SBU) and Secret networks; successes by the Interagency Threat Assessment and Coordination Group to strengthen information sharing between the Intelligence Community and state, local, and tribal law enforcement; and the tireless work of the terrorist watchlisting and screening community to streamline and standardize processes for information sharing while protecting the privacy, civil rights, and civil liberties of individuals.

While we have made great progress, we still face significant challenges. The unauthorized disclosure of classified information as a result of the WikiLeaks breach illustrates some fundamental failures to protect sensitive information properly and challenges our government to renew its focus on enhancing the means for the secure and effective use of information. While we cannot eliminate every insider threat, we have taken this opportunity to reassess our posture, our progress toward our goals, and our focus on responsible information sharing and protection.

We are building our mitigation efforts, and numerous corrective actions have been instituted across the Federal Government. We are seizing the momentum of existing efforts to strengthen responsible, trusted, and secure information sharing through efforts like data tagging and managing access to classified information and systems.

We will continue to work closely with our partners to build capacity, strengthen governance, and improve performance. Our roadmap for this will be a new National Strategy for Information Sharing and Protection, which we are currently drafting in close coordination with our ISE mission partners. Our partners have called for holistic solutions, including opening the aperture to the totality of terrorism-related information, focusing on critical capabilities like data aggregation and moving to an enterprise data management approach.

Our partners in public safety organizations are facing significant challenges with fiscal constraints forcing drastic budget cuts. State, local, and tribal public safety executives acknowledge that fundamental changes are required to meet the new realities of policing, including improved operational interoperability through proactive strategies, virtual consolidation, and shared services. We are in a position to support the national public safety and law enforcement community in the development of a common, distributed, decentralized information sharing system that builds upon existing technologies, better aligns and leverages existing efforts, and reinvents the public safety model for the 21st century.

We are continuing to work together, at every level of government, to accelerate the delivery of the ISE in a strategic and focused way.



Kshemendra Paul
Program Manager,
Information Sharing Environment



Table of Contents

Foreword	iii
Table of Contents.....	v
Executive Summary	ix
Strengthening Management and Oversight	x
Improving Information Sharing Activities	xi
Establishing Standards for Responsible Information Sharing and Protection	xv
Enabling Assured Interoperability Across Networks	xvi
Enhancing Privacy, Civil Rights, and Civil Liberties Protections (P/CR/CL)	xviii
Ten Year Anniversary of 9/11.....	xix
1 Introduction	1
1.1 Purpose and Scope of the Information Sharing Environment (ISE)	1
1.2 ISE Mission Partners	5
1.3 Strengthening Information Sharing and Information Protection.....	6
1.4 Structure of this Report.....	7
2 Strengthening Management and Oversight	8
2.1 ISE Governance.....	8
2.1.1 Information Sharing and Access Interagency Policy Committee (ISA IPC)	8
2.1.2 Working with State, Local, and Tribal Partners	10
2.1.3 Interdependencies.....	11
2.1.4 Department and Agency Information Sharing Offices.....	11
2.1.5 Other Interagency Policy Coordination and Implementation Bodies.....	12
2.2 Performance and Investment Integration.....	13
2.2.1 Three-way Partnership (Agencies, OMB/NSS, and PM-ISE).....	13
2.2.2 Programmatic Guidance	13
2.2.3 Strategic Investment.....	15
2.2.4 Performance Management.....	18
2.3 Stakeholder Engagement	19
2.3.1 Refreshing of the Vision for Information Sharing	21
2.4 ISE Culture Initiatives.....	24
2.4.1 Appraisal/Information Sharing Behavior	25
2.4.2 Information Sharing Training.....	26
2.4.3 Incentives.....	28
2.4.4 Exercises	28
2.4.5 Best Practices.....	29

Building the Foundation.....	30
3 Improving Information Sharing Activities	32
3.1 Suspicious Activity Reporting	33
3.1.1 Implementation of the NSI – Building on Success	34
3.1.2 Suspicious Activity Reporting (SAR) Sub-Committee	38
3.1.3 Enhancing SAR Analysis	39
3.1.4 Building Communities of Trust (BCOT)	40
3.1.5 Leveraging the SAR Experience.....	40
3.2 National Network of Fusion Centers	41
3.2.1 Fusion Centers and the FBI	41
3.2.2 Baseline Capabilities Assessment (BCA)	42
3.2.3 Fusion Center Sub-Committee.....	44
3.2.4 Federal Resource Allocation Criteria (RAC)	45
3.2.5 Fusion Center – High Intensity Drug Trafficking Area (HIDTA) Partnership.....	46
3.2.6 Improving Information Sharing On Threats to the Southwest Border	47
3.2.7 Major City Chiefs Intelligence Unit Commanders Group.....	47
3.2.8 National Fusion Center Conference (NFCC).....	47
3.3 Interagency Threat Assessment and Coordination Group (ITACG).....	49
3.3.1 Assessment of the Detail’s Access to Information	49
3.3.2 ITACG Involvement in Intelligence Production	50
3.3.3 ITACG Performance	50
3.3.4 Intelligence Guide for First Responders, 2nd Edition	51
3.3.5 Guide for Public Safety Personnel	51
3.3.6 Federal Community Orientation Program	51
3.4 Tribal Information Sharing	52
3.4.1 Information Sharing Implications of the Tribal Law & Order Act (TLOA)	52
3.4.2 Building the Community	52
3.4.3 Providing Access to all Tribal Front Line Officers.....	53
3.4.4 Tribal Integration with NSI and Fusion Centers	53
3.4.5 FBI and Tribal Integration	54
3.5 Multimodal Information Sharing.....	54
3.5.1 Information Sharing in the Air Domain.....	55
3.5.2 Information Sharing in the Maritime Domain	55
3.6 WMD Information Sharing	57
3.6.1 Securing the Cities (STC)	58
3.6.2 West Coast Maritime Pilot.....	58
3.7 Intelligence Community (IC) Intelligence Sharing Services	58
3.7.1 NCTC CURRENT	58
3.7.2 Worldwide Incidents Tracking System (WITS)	58
3.7.3 Intelligence Today.....	59
3.7.4 Intelink.....	59
3.8 Watchlisting and Screening	60

3.9	Private-Sector Information Sharing	60
3.9.1	Collaborative Partnerships between the Private Sector and the IC	60
3.9.2	InfraGard.....	60
3.9.3	Domestic Security Alliance Council (DSAC).....	61
3.9.4	Tripwire Program.....	61
3.9.5	Critical Infrastructure Information Sharing	62
3.10	Foreign Partner Information Sharing	64
3.10.1	International Information Sharing Pacts.....	65
3.10.2	Sharing Best Practices.....	66
3.10.3	Cross-Border Sharing Empowered by the National Information Exchange Model (NIEM)	66
3.11	Law Enforcement Information Sharing	67
3.11.1	Criminal Justice Information Services (CJIS)	67
3.11.2	eGuardian Adopted by DoD.....	68
3.11.3	Technical Resource for Incident Prevention (TRIPwire)	69
3.11.4	Next Generation Identification System (NGI)	69
3.11.5	United States Visitor and Immigration Status Indicator Technology (US-VISIT).....	70
3.11.6	Law Enforcement Information Sharing Initiative (LEISI)	71
3.11.7	National Law Enforcement Telecommunications System (Nlets).....	72
3.11.8	Domestic Highway Enforcement Initiative (DHE)	72
3.11.9	INTERPOL I-24/7	73
3.12	Homeland Security Standing Information Needs.....	75
	<i>Building Beyond the Foundation</i>	<i>76</i>
4	Establishing Standards for Responsible Information Sharing and Protection.....	77
4.1	Advancing Existing Standards for Information Sharing and Protection	77
4.2	Coordination of Standards to Enable Interoperable Capabilities	78
4.2.1	Standards Governance.....	79
4.2.2	Industry Engagement.....	79
4.3	The National Information Exchange Model (NIEM)	80
4.3.1	Advancing Use of NIEM Across All Levels of Government.....	80
4.3.2	Advancing NIEM and UML Tools.....	81
4.4	Identity, Credential and Access Management (ICAM)	82
4.4.1	Implementing Federated Identity Standards into the ISE's Interoperability Efforts	82
4.4.2	Advancing Attribute Governance and Backend Attribute Exchange (BAE)	84
4.5	Security, Auditing and Cross-Domain Frameworks	85
4.5.1	Securely Sharing Classified Information with State, Local, Tribal, and Private-Sector (SLTPS) Partners	85
4.5.2	Policy and Procedural Framework for Security Reciprocity.....	86
4.5.3	Information Assurance and Auditing	88
4.5.4	Information Sharing Across Security Domains	89
4.5.5	Guiding Departments and Agencies	89

<i>Information Sharing and Protection Challenges and Opportunities</i>	<i>91</i>
5 Enabling Assured Interoperability Across Networks.....	92
5.1 Data Aggregation.....	92
5.2 Assured Secret Network Interoperability.....	94
5.3 Assured Sensitive But Unclassified (SBU) Network Interoperability	96
5.3.1 Simplified Sign On (SSO)	98
5.3.2 Measuring SBU Progress.....	98
5.3.3 Future Plans.....	99
5.3.4 Controlled Unclassified Information (CUI).....	100
5.3.5 Progress on CUI.....	101
5.3.6 The Way Ahead.....	101
<i>Senior Privacy and Civil Liberties Officers</i>	<i>102</i>
6 Enhancing Privacy, Civil Rights, and Civil Liberties Protections.....	103
6.1 Privacy, Civil Rights, and Civil Liberties Protection Policies.....	103
6.2 Privacy Training and Outreach	105
6.3 Privacy & Civil Liberties (P/CL) Sub-Committee	105
7 APPENDIX A — Performance Assessment Data	A-1
8 APPENDIX B — Acronyms	B-1



Executive Summary

This Fifth Annual Report to the Congress on the state of the Information Sharing Environment (ISE) is submitted in accordance with requirements in Section 1016(h) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, and Section 210D(c) of the Homeland Security Act of 2002, as amended. This Report builds upon the mission partner accomplishments highlighted in the 2010 Report and reflects:

- Progress on ISE implementation by the bureaus and agencies of federal, state, local, and tribal governments and our private-sector and international partners;
- Collective accomplishments of the terrorism and homeland security information sharing and access community;
- Individual agency initiatives that stand out as best practices in information sharing and help form the fabric of the ISE; and
- Successful partnerships between the PM-ISE and federal and non-federal mission partners, involving terrorism, homeland security, and weapons of mass destruction (WMD) information sharing.

The Program Manager, Information Sharing Environment (PM-ISE) facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. Consistent with the direction and policies issued by the President and the Office of Management and Budget (OMB), the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE. The ISE is realized by the investment of mission partners—the bureaus and agencies of federal, state, local, and tribal governments and our partners in the private sector and internationally—and is used by front line law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel.

This Report describes information sharing progress since July 2010. The Report is organized into five central themes:

1. Strengthening Management and Oversight
2. Improving Information Sharing Activities
3. Establishing Standards for Responsible Information Sharing and Protection
4. Enabling Assured Interoperability Across Networks
5. Enhancing Privacy, Civil Rights, and Civil Liberties Protections

Strengthening Management and Oversight

In strengthening the management and oversight of the ISE, the PM-ISE actively governs, integrates performance and investment, engages stakeholders, and encourages a culture of information sharing.

Governance: The Information Sharing and Access Interagency Policy Committee (ISA IPC) is the interagency forum for overseeing the planning and implementation of the ISE. The ISA IPC formally charters Sub-Committees to provide advice and support to the IPC on a range of related issues within their designated portfolios, and inform ISE planning and implementation. ISA IPC Sub-Committees have formed a number of Working Groups to address discrete issues or topics within the Sub-Committees portfolio.

Since January 2011, ISA IPC Sub-Committees and Working Groups have organized and managed their efforts, and are reporting their accomplishments on a quarterly basis in line with annual and longer-term objectives and goals for the ISE. In accordance with IRTPA Section 1016, several of the ISA IPC Sub-Committees and Working Groups include participation by representatives of non-federal organizations in order to ensure adequate consultation and representation from all ISE stakeholders.

More than half of the ISE departments and agencies have dedicated information sharing offices, directorates, divisions or executives. The establishment of a single office to ensure full cooperation in the development of the ISE is considered a best practice and is encouraged across the ISE.

- In October 2010, the Director of National Intelligence (DNI) strengthened the responsibilities and title of the Intelligence Community (IC) Information Sharing Executive.
- The Federal Bureau of Investigation (FBI) established an ISE and a Chief Information Sharing Officer position in 2008 to coordinate internal and external information sharing policy issues. In February 2011, the Directorate of Intelligence (DI) created a new DI Branch, the Intelligence Integration Branch (IIB), to enhance sharing and outreach efforts. The IIB is specifically charged with engaging federal, state, local, tribal, and IC partners to increase the effectiveness of information sharing and also to coordinate efforts to combat violent extremism.

Performance and Investment Integration: Each year, OMB and the National Security Staff issue programmatic guidance for the federal budget describing ISE priority areas. The implementation of this guidance moves each of the agencies closer to collaborative endeavors—eliminating redundancies, identifying reuse options, leveraging best practices, and consolidating similar projects across organizational boundaries. Partner agencies continue to strategically invest in the ISE and to indicate alignment of their information technology investments to the ISE priorities. Initial use of enhanced Exhibit 53 reporting allowed analysis of federal agency information technology spending aligned to ISE priorities.

The ISE continues to employ a performance management process to report on results. The PM-ISE monitors performance across strategic investments, mapping the ISE strategic vision to initiatives and outlining clear measures.

Stakeholder Engagement: The PM-ISE engages ISE mission partners through live events across the country, roundtables, the ISE website (www.ISE.gov), and the use of social media. This year, PM-ISE placed a special emphasis on engagement with industry. Standards organizations and industry consortia

assist mission partners in developing, coordinating and maintaining technical standards, and provide a means to communicate ISE requirements to industry while providing industry with a means to communicate potential solutions to ISE mission partners.

Refreshing the Strategy: In 2010, the Executive Office of the President asked the PM-ISE to refresh the 2007 *National Strategy for Information Sharing* in order to outline an updated vision and strategy for responsible information sharing and protection. Input from our ISE mission partners is critical to ensure that this refreshed strategy supports the counterterrorism mission and provides complete solutions for ISE mission partners. To accomplish this, the PM-ISE invited partners to provide their vision for the ISE, as well as input on various topics for incorporation into the new Strategy.

Culture: Achieving a culture in which responsible information sharing is the norm rather than the exception is a major goal of IRTPA. Federal agencies continue to expand their programs to include information sharing and collaboration as part of the recruitment, orientation, and performance evaluation of all employees; to increase and improve mission specific training programs; to encourage the use of incentive awards for collaborative efforts; to encourage joint duty-like assignments to foster knowledge sharing; and to create communities of interest around particular topics.

Improving Information Sharing Activities

The PM-ISE's responsibilities extend to addressing and facilitating improved information sharing between and among the intelligence, defense, homeland security and law enforcement communities. Significant progress has been made toward building a broad foundation for information sharing across the Federal Government, as well as with state, local, tribal, private sector, and international partners.

Suspicious Activity Reporting: The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) provides analysts, operators and investigators with another tool to "connect the dots" in the course of combating crime and terrorism by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR in a manner that rigorously protects the privacy, civil rights, and civil liberties of Americans. The NSI has made substantial progress toward standardizing ad hoc methods of reporting and analysis, and implementing these standards, policies, and processes within fusion centers. It has also developed training for front line officers, analysts, and chief executives regarding the behaviors and indicators of terrorism related criminal activity. To date, nearly 50,000 officers have received line officer training.

Over the past year the NSI Program Management Office (PMO) has also been coordinating closely with the Department of Homeland Security (DHS) on the "If You See Something, Say Something™" campaign—a simple and effective program to raise public awareness about indicators of terrorism, crime, and other threats, and to emphasize the importance of reporting suspicious activity to the proper authorities.

The FBI and the NSI PMO are integrating the FBI's eGuardian system to enhance information sharing among all mission partners in order to protect the security of the homeland. This initiative helps formalize the sharing of information currently taking place between state, local, and tribal partners, and leverages the already successful relationships between SLT partners and the FBI's Joint Terrorism Task Forces.

National Network of Fusion Centers: Located in state and major urban areas throughout the country, fusion centers are uniquely situated to empower front line law enforcement, public safety, fire service, emergency response, public health, Critical Infrastructure and Key Resources (CIKR) protection, and private-sector security personnel to understand local implications of national intelligence, enabling local officials to better protect their communities. In September 2010, federal, state, and local officials completed a Baseline Capabilities Assessment (BCA)—the first nationwide, in-depth assessment of fusion centers to evaluate fusion center capabilities and to establish strategic priorities for Federal Government support. Based on the results, fusion centers made progress in building their capabilities and in addressing identified gaps.

In 2010, all 56 FBI field offices conducted self-assessments on their relationship with fusion centers, providing a comprehensive understanding of how the FBI is currently engaging with fusion centers. The FBI plans to continue close collaboration at both the field office and headquarters levels to standardize processes; clarify procedures; and facilitate more effective engagement with fusion centers.

One of the Federal Government's priorities for coordinating support to fusion centers was to clearly define the parameters for the allocation of federal resources to fusion centers. The Fusion Center Sub-Committee of the ISA IPC developed the Federal Resource Allocation Criteria policy, which defines objective criteria and a coordinated approach for prioritizing the allocation of federal resources to fusion centers.

Representatives from federal, state and local agencies—including High Intensity Drug Trafficking Areas (HIDTAs), fusion centers, the DHS, the White House Office of National Drug Control Policy (ONDCP), the Department of Justice (DOJ), the FBI, the National Drug Intelligence Center (NDIC), and the PM-ISE—met in February to explore how best to leverage fusion centers and HIDTAs as uniquely valuable resources and partners. As a result of their discussions, these partners are continuing to build and formalize relationships within their states through business plans and concepts of operation to enhance intrastate coordination and execution of the statewide fusion process.

Interagency Threat Assessment and Coordination Group (ITACG): The ITACG facilitates information sharing between federal, state, local, tribal, and private-sector partners. Since March 2010, DHS Intelligence and Analysis (I&A) has solicited feedback on every intelligence product it has released, including products the ITACG is involved in producing. State and local feedback has been positive. Nearly 99 percent of the DHS products are either integrated into state and local finished intelligence products; shared with partners; or used for situational awareness, security preparations, or training purposes. Fusion center directors also indicated that reporting has become more frequent, more relevant, and more concise.

The Congress has recently expressed interest in knowing whether ITACG personnel have access to the information they need, within the scope of the ISE. ITACG personnel are exposed to the main stream of intelligence at the National Counterterrorism Center (NCTC). A significant indicator of the ITACG's access to information is their involvement with a special site exploitation effort currently ongoing at NCTC.

The second edition of the *Intelligence Guide for First Responders*, published in 2011, incorporates feedback from the field, and includes two new sections: "Reporting Suspicious Activity," which covers

participation in the NSI, and "Joint Partnerships," which highlights several joint federal, state, local, and tribal activities around the country.

Tribal Information Sharing: This past year the PM-ISE dedicated efforts to building a community to increase cooperation between federal, state, local, and tribal law enforcement agencies. The National Law Enforcement Telecommunications System (Nlets) links together state, local and federal law enforcement, justice and public safety agencies. This year, the first connectivity pilot program between four tribes in separate regions of the United States and Nlets was established.

PM-ISE has partnered with the NSI PMO to administer the NSI Line Officer Training to all tribal law enforcement partners, as an attempt to further integrate Indian Country into the NSI. Integration of tribal law enforcement personnel in fusion centers has occurred successfully in Oklahoma, Arizona, and Washington State.

Multimodal Information Sharing: ISE mission partners are pursuing information sharing initiatives aimed at protecting and reducing vulnerabilities at our borders, ports, and airports, and enhancing overall transportation security.

In January 2011, the Next Generation Air Transportation System (NextGen) Joint Planning and Development Office (JPDO) kicked off an effort to develop a Concept of Operations (CONOPS) for the Integrated Surveillance Initiative.

The U.S. Customs and Border Protection, U.S. Coast Guard, and Immigration and Customs Enforcement components of DHS are engaged in the Joint Targeting Architecture Project to improve information sharing relating to targeting protocols and procedures at seaports where the agencies have distinct authorities to protect the United States against persons, cargo, and other dangers posed by seaborne vessels.

The Multimodal Information Sharing Taskforce (MIST) is an interagency research effort designed to foster collaboration and to capture best practices in information sharing in a regional port environment. MIST has identified a number of best practices for collaboration, including the U.S. Customs Trade Partnership Against Terrorism program, the expansion of industry-run education programs for government employees, and the inclusion of industry in emergency preparedness activities and Integrated Operations Centers.

Weapons of Mass Destruction (WMD) Information Sharing: The PM-ISE supports DHS's Domestic Nuclear Detection Office by funding the initiation of their inter-governmental information sharing exchange. This mechanism will facilitate and standardize the real-time sharing of radiological and nuclear alarm adjudication data, as well as shipment and licensee data, and will improve analysis of post-seizure data.

Intelligence Community (IC) Intelligence Sharing Services: A variety of IC intelligence sharing services provides analysts, operators, and investigators on-demand electronic dissemination applications to facilitate information sharing at and across all levels of security. For example, NCTC CURRENT is the premier classified resource for counterterrorism (CT) reporting and analysis throughout the IC. *Intelligence Today*, the daily online compendium of analytic products from across the IC, marked its first anniversary on 22 March 2011 by posting its 48,450th article. Intelink recently crossed the 100 million

document threshold for records exposed to Intelink search services across the Unclassified, Secret, and Top Secret networks combined. In one month alone this year, Intelink recorded over two million searches. These milestones highlight the ability of IC personnel to access more information quicker and more effectively, enabling them to better share information and thus perform their missions.

Watchlisting and Screening: Since the development of the consolidated terrorist watchlist that is in use today, there have been many successes and improvements to watchlisting processes. Some of the more recent improvements include clearer definitions of the roles and responsibilities of federal agencies, streamlining and standardizing nominations processes, improving the use of biometrics for identification, and improving analytical and technological capabilities.

Private-Sector Information Sharing: Last year, the Office of the Director of National Intelligence (ODNI) and DHS I&A jointly established a program to develop partnerships between members of the private sector and teams of experienced IC analysts. The goal of this effort is to provide IC analysts with a better understanding of select national and homeland security-related industries.

The CIKR ISE is making substantial progress in providing useful critical infrastructure protection and resilience content to an increasing number of critical infrastructure sector partners to identify their risks, reduce their vulnerabilities, and respond to and recover from incidents.

Foreign Partner Information Sharing: Foreign partners are vital in the effort to combat terrorism by sharing key information, conducting surveillance, collaborating with U.S. overseas air passenger and maritime cargo screening, arresting members of terrorist cells, interdicting terrorist financing and logistics, and contributing to efforts in Afghanistan, Iraq, and other key places around the world. In February 2011, President Obama and the Prime Minister of Canada released the *Beyond the Border Declaration: A Shared Vision for Perimeter Security and Economic Competitiveness*, which identified information sharing, particularly along our shared border, as a key priority between the United States and Canada. The ISE is currently developing an online knowledge base that describes important core concepts, approaches, and best practices of the ISE, including governance, standards, policy, budget, performance management, privacy policies, and a process for SAR.

Recognizing the value that the National Information Exchange Model (NIEM) could provide for facilitating information sharing within the Canadian and Mexican governments and along their borders with the United States, both Mexico and Canada have shown interest in adopting NIEM in the public safety, law enforcement, and defense and disaster management domains.

Law Enforcement Information Sharing: The FBI's Criminal Justice Information Services (CJIS) is the focal point for some of the most important and relevant criminal history databases used by law enforcement. CJIS's National Data Exchange System (N-DEx) is a criminal justice information sharing system that provides nationwide connectivity to disparate local, state, tribal, and federal systems for the exchange of information. In March 2011, the final increment of the N-DEx system was delivered, increasing its power, speed, and accessibility while greatly improving the user's information-sharing experience.

Programs like the Technical Resource for Incident Prevention (TRIPWire), the National Law Enforcement Telecommunications System (Nlets), the Law Enforcement Information Sharing Initiative (LEISI) the Domestic Highway Enforcement Initiative (DHE), and INTERPOL I-24/7 have also provided significant improvements in information sharing.

In the wake of the tragic Fort Hood shootings in November 2009, a Department of Defense (DoD) board reviewing the incident cited the need to “adopt a common force protection threat reporting system for documenting, storing, and exchanging threat information. In 2010, the FBI’s eGuardian system was selected by DoD.

Homeland Security Standing Information Needs: Documenting information needs is key to enabling effective information sharing. In 2010, DHS reorganized its Homeland Security Standing Information Needs into 10 topics that align with the information needs of consumers. In November 2010, DHS launched a SINs development initiative for the private sector. This initiative included actively engaging interagency governmental partners, as well as owners and operators from the 18 CIKR sectors.

Establishing Standards for Responsible Information Sharing and Protection

PM-ISE is working with mission partners and standards organizations to identify the best existing standards for reuse and implementation across the ISE.

Advancing Existing Standards for Information Sharing and Protection: Functional standards set forth rules, conditions, guidelines, and characteristics of data and mission products to support ISE business process areas. The number of departments and agencies that are incorporating functional standards into the management and implementation of ISE-related mission business processes has steadily increased over the past year. The ISE Functional Standard for Suspicious Activity Reporting (ISE-SAR) is an example of a functional standard now advanced by mission partner-specific efforts via the NSI.

Coordination of Standards to Enable Interoperable Capabilities: Recognizing the critical role of standards in enabling the ISE and mission partner operations, in May 2011 the ISA IPC approved the creation of a Standards Working Group to coordinate efforts across departments, agencies, and levels of government.

The National Information Exchange Model (NIEM): NIEM is gaining significant adoption as a common framework for information sharing for a number of state, local and tribal agencies. In May 2011, PM-ISE collaborated with the NIEM PMO and members of the Object Management Group (OMG), a consortium of both industry and government members, in an effort to develop a Unified Modeling Language (UML) profile for NIEM that will further NIEM success and adoption.

PM-ISE is currently working with its mission partners on a strategic sourcing approach based on industry standards and implementation profiles. Strategic approaches like these will allow mission partners to procure products that are interoperable, cost-effective, and policy and standards-compliant.

Identity, Credential and Access Management: This year, the PM-ISE convened the leaders associated with the multiple logical access related management activities of the Federal Government. Leaders agreed to a broad vision of enabling these different standards to ultimately become aligned across all levels of government so that users accessing data could be authenticated and authorized appropriately for access.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions.

Security, Auditing and Cross-Domain Frameworks: Information security and assurance helps partners manage connections between what data people are allowed to access and share, in a way that promotes responsible information sharing across partners. In August 2010, the President issued Executive Order (EO) 13549 “Classified National Security Information Program for State, Local, Tribal and Private Sector Entities,” to all federal departments and agencies, which establishes a program designed to safeguard and govern access to classified national security information shared by the Federal Government with state, local, tribal, and private-sector entities.

Significant progress in the area of security reciprocity continued over the past year as evidenced by continued promulgation of harmonized National Institute for Standards and Technology (NIST)-Committee on National Security Systems (CNSS)-Intelligence Community Directive (ICD) standards. Progress also has continued with regard to developing the policy and procedural framework for reciprocity for information systems security.

Recently promulgated IC standards implement uniform information security requirements and procedures concerning audit information in the IC information environment, and address the use of collected audit data for insider threat detection. The IC’s experience in audit functions presents an opportunity for leveraging best practices for other federal, state, and local networks to improve the overall assurance of the ISE.

Enabling Assured Interoperability Across Networks

The Information Integration Sub-Committee (IISC) of the ISA IPC coordinates high priority interagency efforts to accelerate the delivery of the ISE, including interoperability among Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) and Secret networks, identification of best practices in support of data aggregation activities, and advancement of industry-based standards in support of all ISE activities.

Data Aggregation: The mission to disrupt terrorist acts before they occur is enabled by finding, sharing and collaborating on data that comes from trusted and reliable mission partners. The goals of data aggregation in the ISE are achieved through an established governance process that enables mission partners to obtain the data, through shared ISE enterprise services, that is necessary to perform their missions while protecting the privacy of persons for whom no nexus to terrorism exists.

Under the joint leadership of DHS and ODNI, the Data Aggregation Working Group (DAWG) was formally approved and chartered by IISC to focus on capabilities that are entity (identity)-focused, and to employ automated data discovery, data characterization, data correlation, and disambiguation algorithms to aggregate information from multiple domains into a mission-specific enterprise-level analytic service. The DAWG has completed a review of the U.S. Government oversight and governance structures that provide strategic policy as well as technical and mission guidance for terrorism-related data aggregation, data integration and data management efforts.

As DAWG identifies best practices and lessons learned, it is expected that mature technical solutions, that can be shared across the ISE will be identified.

Assured Secret Network Interoperability: The ability to effectively and responsibly share classified information among federal and non-federal mission partners is a key capability needed to support the counterterrorism mission and homeland security. In 2010 the ISA IPC chartered the Assured Secret Network Interoperability Working Group (ASNI WG) to serve as a forum for federal agencies operating Secret networks to work together to develop governance, to resolve interoperability issues, and to support assured information sharing among federal Secret networks. Over the past nine months, the ASNI WG has delivered a number of key incremental accomplishments towards increasing interoperability and information sharing. For example, ASNI WG partnered with the Fusion Center Sub-Committee to document, validate, and prioritize fusion center information needs. This establishes the foundational requirements needed to inform the development of technical connectivity and access to sensitive information for fusion centers.

The ASNI WG also supported progress on mission capabilities for fusion centers including: improved access to white-listed sites on DoD's Secret network, the Secret Internet Protocol Router Network (SIPRNet), via DHS's Homeland Secure Data Network (HSDN); preserved and expanded fusion center access via HSDN to *NCTC CURRENT* during its relocation to SIPRNet; expanded Secret-level video-conferencing capabilities as a shared service between FBI's Secret network and HSDN for fusion centers; and new access to the FBI's white pages and email directories through HSDN.

Assured Sensitive but Unclassified (SBU) Network Interoperability: The multiple SBU/CUI networks, portals, and systems currently in existence contain a rich variety of data and services. However, differences in policy and technology prevent authorized users from gaining access to many of those resources without having to individually log on to these multiple systems, using multiple credentials. The ability to login just once to an approved system, and to be granted access to an interoperable and protected SBU/CUI environment, commonly referred to as Simplified Sign On (SSO), is an overarching requirement for federal, state, local, and tribal law enforcement officers and analysts.

Over the past year, the Assured SBU Network Interoperability Working Group has made significant progress towards achieving SSO. For example, in December 2010, CJIS's Trusted Broker Version 2 became operational, providing SSO capabilities by allowing law enforcement online users to access Intelink-U, RISSNET, and many other systems. The Assured SBU Network Interoperability Working Group tracks the effectiveness of their efforts by monitoring a set of user metrics that are collected from partners on a monthly basis. Those metrics have been designed by the SBU partnership to indicate progress towards interoperability goals and to assist in fine-tuning particular interoperability efforts.

Controlled Unclassified Information (CUI): On 4 November 2010, President Obama signed EO 13556 "Controlled Unclassified Information," establishing a CUI program to manage all unclassified information that requires safeguarding and/or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. The EO identifies National Archives and Records Administration (NARA) as the Executive Agent to implement the EO and to oversee departmental and agency actions to ensure compliance.

On 9 June 2011, the NARA's CUI Office issued the "Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556." In the coming months, the CUI Office will lead an interagency process to establish an Executive Branch-wide definition and taxonomy of categories for CUI, and departments and agencies will submit CUI compliance plans by 6 December 2011. Federal agencies are expected to initiate efforts to develop CUI guidance specific to their agency and unique mission requirements.

Enhancing Privacy, Civil Rights, and Civil Liberties Protections (P/CR/CL)

IRTPA aims at the broadest possible sharing of information for counterterrorism purposes. It also explicitly recognizes that such sharing must respect P/CR/CL protections. A critical step in the safeguarding of P/CR/CL is the development and adoption of a written P/CR/CL policy that meets the standards of the White House ISE Privacy Guidelines. Nine out of 14 ISE departments and agencies have reported that they have developed ISE Privacy Policies. These agencies have also made measurable progress in implementing the ISE Privacy Policies by modifying business processes and updating sharing agreements to align with the new policies.

State, local, and tribal partners have worked to develop privacy policies that are "at least as comprehensive as" the ISE Privacy Guidelines, a standard prescribed as a prerequisite for receiving terrorism-related information from federal entities. For example, all operational state and major urban area fusion centers were determined to have privacy policies that are "at least as comprehensive as" the ISE Privacy Guidelines. The NSI PMO has also worked diligently with NSI participants to implement all of the elements of the NSI Privacy Framework for SAR.

All federal agencies reported that personnel receive training with a specialized privacy and civil liberties protection component at least annually.

The Privacy and Civil Liberties (P/CL) Sub-Committee was established under the ISA IPC in September 2010. Over the past year, the P/CL Sub-Committee has established three working groups: the Privacy and Civil Liberties Legal Issues Working Group, the Privacy and Information Technology Working Group, and the Compliance Review Working Group.

Ten Year Anniversary of 9/11

The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information.¹

"We have some planes!" The full import of that ominous sentence, spoken at 8:25 AM on September 11, 2001, by the hijacker pilot of American Airlines Flight 11, was not fully understood by Federal Aviation Administration and airline officials until more than a half hour later when Flight 11 had already crashed into the North Tower of the World Trade Center, United Airlines Flight 175 had crashed into the South Tower, and American Airlines Flight 77 was bearing down on Washington, DC for an attack on the Pentagon.² But those words were the first indications that the Nation was confronting multiple hijackings for the first time in its history and that the most devastating attack on the U.S. Homeland since Pearl Harbor—one that would kill almost 3,000 people from more than 70 countries —was underway.³



There is another quote from that day that serves as an effective counterweight. It was spoken by Todd Beamer to Lisa Jefferson shortly before 10:00 AM. Hearing on their cell phones of the earlier attacks, Beamer and fellow passengers on the fourth hijacked plane, United Airlines Flight 93, realized that the hijackers intended to use the plane to attack another target, possibly the U.S. Capitol or the White House, and decided to take action. The last words he spoke still resonate today as symbols of courage, resilience, and initiative in the face of chaos and mortal danger: *"Are you guys ready? Let's roll!"* Beamer and his fellow passengers then assaulted the cockpit, sacrificing their lives to thwart the hijacker's plans when the plane crashed in an open field near Shanksville, Pennsylvania.

The U.S. response to the events of 9/11 both honors and emulates the attitude and actions of Todd Beamer and his fellow passengers. We honor them by remembering and celebrating the lives and heroic actions of the victims, survivors, and families; we then seek to fully understand what happened and how

1 9-11 Commission Report, July 2004

2 *National Commission on Terrorist Attacks upon the United States*. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: [W.W. Norton & Company](http://www.wwnorton.com), 2004. pp. 1-14. Available at <http://www.9-11commission.gov/report/911Report.pdf>.

3 "9/11 By the Numbers," <http://nymag.com/news/articles/wtc/1year/numbers.htm>

and why it did; and finally we have taken and continue to take the actions necessary to minimize the chances of it happening again.

The 9/11 Commission Report, issued in the summer of 2004, concluded that a combination of factors—not one single cause—prevented us from detecting and preventing the planned attack. One of the factors cited by the Commission as among the “most serious weaknesses” leading to the attacks was a breakdown in information sharing among federal agencies and with state, local, and tribal governments. The Commission specifically called for “unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional government boundaries,” the first reference to what would eventually become the Information Sharing Environment (ISE).⁴ Removing legal, policy, procedural, and technological impediments to more effective sharing of terrorism-related information—in a way that still protects national security and privacy and civil liberties—thus became, and continues to be, one of the major focuses of the effort to help protect our nation against future attempts by terrorists.

This effort cuts across all levels of government and extends to the private sector and to international partners. It has been notably bi-partisan, championed by both Democratic and Republican administrations and congressional leaders. Even before the Commission Report was issued, Congress had taken preliminary steps to address some of the known information sharing deficiencies - both the USA PATRIOT Act and the Homeland Security Act of 2002 included provisions that improved information sharing among government agencies.⁵

It was, however, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) that gave the effort its focus and strategic direction. IRTPA implemented many of the Commission’s specific recommendations including establishing an ISE for terrorism-related information and requiring the President to designate a program manager (PM-ISE) to “plan for and oversee the implementation of, and manage, the ISE,” thus positioning the ISE as a critical part of the Nation’s efforts to combat terrorism. Six years after passage of IRTPA, some of the most significant barriers to federal, state, local, tribal, and private sector collaboration have already fallen and others are being aggressively addressed by the PM-ISE and mission partners.

On 1 May 2011 Osama Bin Laden was killed near Abbottabad, Pakistan. In the words of President Obama, “Tonight, we give thanks to the countless intelligence and counterterrorism professionals who’ve worked tirelessly to achieve this outcome. We give thanks to the men who carried out this operation, for they exemplify the professionalism, patriotism, and unparalleled courage of those who serve our country. And they are part of a generation that has borne the heaviest share of the burden since that September day.”⁶

4 9/11 Commission Report, p.400.

5 USA PATRIOT Act, PL 107-56, (October 26, 2001), Section 314, et al. and Homeland Security Act of 2002, PL 107-296, (November 22, 2002) Section 891, et al.

6 <http://www.whitehouse.gov/the-press-office/2011/05/02/remarks-president-osama-bin-laden>

In his remarks on the Senate floor regarding the resolution honoring the members of the military and the Intelligence Community (IC) who carried out the mission, Senator Reid stated, "Resolution is an appropriate name for this legislation. It honors the resolution to a problem that has lingered for nearly a decade—one whose weight has grown heavier each day on the shoulders of the families Osama Bin Laden traumatized and the many more he terrorized."⁷

The operation that resulted in Bin Laden's death was a significant achievement by the IC who collaborated across agencies to gather and analyze the information needed to conduct the assault. DNI Clapper stated, "In my nearly 50 years in intelligence, I have never seen a more remarkable example of focused integration, seamless collaboration, and sheer professional magnificence as was demonstrated by the Intelligence Community in the ultimate demise of Osama Bin Laden."⁸ Former Central Intelligence Agency Director Panetta added, "The raid was the culmination of intense and tireless effort on the part of many Agency officers over many years...Along with our partners at the NGA [National Geospatial-Intelligence Agency], NSA [National Security Agency] and ODNI [Office of the Director of National Intelligence], we applied the full range of our capabilities (and) produced the results that the American people expect of their intelligence service."⁹

Notably, the co-chairs of the 9/11 Commission also connected the successful operation to the implementation of the intelligence reforms that included the creation of the ISE. In a joint statement they concluded, "As a result of these reforms, there is much closer collaboration between intelligence and military components of the Federal Government."¹⁰

Nearly 10 years after the attacks of 9/11, our government is challenged by the evolving nature of terrorism. While al Qaeda itself continues to threaten the United States, al Qaeda also inspires an array of affiliated terrorist groups and there is an escalation of a significant new threat that takes advantage of radicalized violent Islamic extremists within our borders.¹¹ We will remain vigilant and continue to work to ensure that terrorism-related information, properly managed and protected, is shared in time to be used effectively to counter threats to our people and institutions. We will do this consistent with our open society, federated democracy, equality, and traditional American values of democracy and individual liberties. In this endeavor we must work with all the energy and commitment that the challenge demands. We can do no better than to adopt as our guiding maxim the words of Todd Beamer—"Are you guys ready? Let's roll!"

7 <http://democrats.senate.gov/newsroom/record.cfm?id=332678>

8 http://www.dni.gov/press_releases/20110502_release_clapper.pdf

9 <https://www.cia.gov/news-information/press-releases-statements/press-release-2011/justice-done.html>

10 This statement is available at http://www.nydailynews.com/opinions/2011/05/09/2011-05-09_winning_the_postbin_laden_war.html

11 Hearing of the Senate Homeland Security And Governmental Affairs Committee, Subject: "Nine Years After 9/11: Confronting The Terrorist Threat To The Homeland," September 22, 2010

1 Introduction

“President Obama's highest priority is to keep the American people safe. Effective and efficient information sharing and access are essential to enhancing the national security of the United States and the safety of the American people. As we move forward together on this important issue, it will be important that we make tangible, meaningful progress on the development of an effective information sharing environment.”

– John Brennan, Deputy National Security Advisor for Homeland Security and Counterterrorism, and Assistant to the President (2 July 2009)

1.1 Purpose and Scope of the Information Sharing Environment (ISE)

This Fifth Annual Report to the Congress on the state of the ISE is submitted in accordance with requirements in Section 1016(h) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended¹² and Section 210D(c) of the Homeland Security Act of 2002, as amended.¹³ This Report builds upon the mission partner accomplishments highlighted in the 2010 Report and reflects:

- Progress on ISE implementation by the bureaus and agencies of federal, state, local, and tribal governments and our private sector and international partners;
- The collective accomplishments of the terrorism and homeland security information sharing and access community;
- Individual agency initiatives that stand out as best practices in information sharing and that help form the fabric of the ISE; and
- Successful partnerships between the PM-ISE and federal and non-federal mission partners, involving terrorism, homeland security, and weapons of mass destruction (WMD)-information sharing.¹⁴

¹² Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, P.L. 108-458 (December 17, 2004), §1016(h).

¹³ Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, sec. 210D(c), codified as amended at 6 U.S.C. 124k(c), details specific reporting requirements pertaining to the Interagency Threat Assessment and Coordination Group (ITACG).

¹⁴ The IRTPA definition of Terrorism Information encompasses all terrorism-related information “whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities,” and was explicitly amended in 2007 to include Weapons of Mass Destruction information. For brevity, these types of information are collectively referred to as “terrorism-related” information.

This year, the Program Manager, Information Sharing Environment (PM-ISE) orchestrated a comprehensive effort to ensure broad-based agency participation in compiling the Annual Report. To most accurately report progress on the extent to which the ISE has been implemented, we used inputs from the 2011 ISE Annual Performance Assessment Questionnaire, which was issued to ISE departments and agencies; we solicited input from the ISE governance bodies that define goals for and monitor the progress of ISE mission partners; and we solicited descriptions of accomplishments from all mission partners, federal and non-federal, to ensure the best possible representation of the state of the ISE and information sharing across the enterprise.¹⁵ In addition, we leveraged data collected by the Office of Management and Budget (OMB) to determine the extent to which ISE priorities are being incorporated into agency Information Technology (IT) budgets.

Scope of the ISE

As depicted in Figure 1, the ISE provides integrated terrorism-related information to support analysts, operators and investigators as they carry out their responsibilities across the law enforcement/public safety, defense, intelligence, homeland security, and diplomacy communities. The ISE facilitates information sharing among federal agencies; across all levels of government—federal, state, local, and tribal; as well as with our private-sector partners and our international allies.



Figure 1. Scope of the ISE

The ISE comprises any mission process, anywhere in the United States, that is intended or is likely to have a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity. Examples include: terrorism watchlisting, person and cargo screening, suspicious activity reporting (SAR), and alerts, warnings and notifications.

¹⁵ IRTPA Sec 1016(i) requires the head of each department or agency that participates in the ISE to submit, at the request of PM-ISE, any reports on the implementation of the requirements of the ISE within its department or agency.

The ISE in Action

- ✓ A law enforcement officer conducting a routine traffic stop, queries the National Crime Information Center and is told to contact the Terrorist Screening Center to evaluate a potential match against the Terrorist Watchlist
 - ✓ An intelligence analyst uses the Library of National Intelligence, or A-Space, to collaboratively develop new intelligence products
 - ✓ Coast Guard personnel responding to the Gulf oil spill leverage DHS's Homeland Security Information Network and Federal Emergency Management Agency's (FEMA) Web Emergency Operations Center (these technologies and applications support ISE mission partners when responding to both man-made and natural disasters)
 - ✓ A local law enforcement analyst, a DHS Intelligence Officer, and an FBI Analyst, co-located at a fusion center, collaborate to develop finished intelligence products that support FBI Joint Terrorism Task Force investigations and to inform line officers of potential indicators and warnings of terrorist threats
 - ✓ A local law enforcement officer notices a suspicious activity and submits the information through eGuardian for vetting against the ISE-SAR Functional Standard.
-

The PM-ISE facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. Consistent with the direction and policies issued by the President and the Director of the Office of Management and Budget, the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE.¹⁶ The PM-ISE serves as a change agent and center for innovation and discovery in providing ideas, tools, and resources to mission partners and assists them in removing barriers, facilitating change, and ensuring that ISE implementation proceeds efficiently and effectively. The PM-ISE ensures that the ISE is built to improve sharing and protection of terrorism, homeland security, and weapons of mass destruction (WMD) information.

A practical way to think of the ISE is as an infrastructure and capability – analogous to the Interstate highway system. The ISE represents the structure and “rules of the road” – including commonly understood road signs, traffic lights, and speed limits – that allow information traffic to move securely, smoothly, and predictably. PM-ISE is not pouring the concrete – rather, it is providing leadership and

¹⁶ IRTPA Section 1016 (f)(2) requires the Program Manager to assist in developing policies, as appropriate, to foster the maturity and proper operation of the ISE.

coordinating a complex set of factors that make the highway safe and navigable: governance and engagement, strategy and policy alignment, business process harmonization, and guidelines, standards, and architecture. This leadership and coordination enables our mission partners – the general contractors building and managing the day-to-day operation of the highways – to build to common specifications. If built properly, everyone can use the roads within appropriate mission and policy context. Indeed, like other infrastructures, the ISE is a public good and has the potential to pay dividends

by supporting information sharing and protection beyond its initial mission space. Terrorism-related information can flow between partners, as can other classes of information such as those related to non-terrorism intelligence and law enforcement while ensuring the protection of privacy, civil rights, and civil liberties.

PM-ISE enables our mission partners to better perform their operations by facilitating access to information and services that contribute toward our shared anti-terrorism mission.

Our tools in this effort are: governance and engagement; strategy and policy alignment; business process harmonization; guidelines; standards; and architecture.

In January 2005, the Government Accountability Office (GAO) designated terrorism-related information sharing as “high risk” because it determined that there were serious challenges in analyzing key information and sharing it among federal, state, local, and other security partners in a timely, accurate, and useful way in order to protect

against terrorist threats. During the 2011 review, GAO found that the government has made progress during the past two years in sharing terrorism-related information among its many security partners, but that it does not yet have a fully-functioning environment in place. To facilitate the development of this environment, PM-ISE co-chairs, with the National Security Staff (NSS), the ISA IPC, which governs its direction and progress; and also partners with OMB.

It is primarily through the OMB/NSS–PM-ISE partnership that program direction, funding, and performance measurement are effectively achieved. Departments and agencies are responsible for developing, deploying, modifying and maintaining their respective investments; they play an active role in determining the policies, priorities, and direction of the ISE and are an integral part of the ISA IPC. In addition, the information they share and the tools used to share it are, by their nature, a part of the ISE. Working with OMB/NSS to provide integrated, cross-government guidance, we establish a framework for departments and agencies investments within the ISE. OMB/NSS programmatic guidance, our policy framework, and the ISE standards and guidelines provide the tools to effectively manage performance throughout the ISE and the ISA-IPC. These strategies, together with ISA IPC governance, the commitment of departments and agencies, and the above mentioned tools, support the strategic roadmap toward achieving a more robust ISE.

1.2 ISE Mission Partners

It is the mission of the bureaus and agencies of federal, state, local, and tribal governments, in cooperation with the ISE's mission partners in the private sector and internationally to help protect our people and our institutions. These agencies build, own and operate the ISE, and are accountable for information sharing that will enable end-to-end mission processes that support counterterrorism (CT).

The support of mission partners is critical to the success of the ISE. They have mission responsibility and a vital leadership role for the delivery, operation, and use of the ISE, and are accountable for delivering value by aligning policy, processes, and information. While the law granted the PM-ISE government-wide authority—a unique capability allowing the office to work with existing programs to facilitate assured information sharing—the actual point of implementation, the heavy lifting, is with mission partners. They are the engines that deliver the ISE. It is the agencies that conduct mission operations, develop and implement policy and procedures, and make investments to interconnect systems, networks, databases, and business processes.

The ISE is realized by the investment of mission partners—the bureaus and agencies of federal, state, local, and tribal governments and our partners in the private sector and internationally—and it is made relevant through its use by front line law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel.

In the six years since the Congress directed the creation of the ISE, mission partners have taken significant steps toward establishing a strong foundation. Important mission initiatives, such as the Nationwide SAR Initiative (NSI), and core capabilities and enablers, such as the National Network of fusion centers, the Federal Bureau of Investigation's (FBI) Field Intelligence Groups (FIGs) and Regional Intelligence Groups (RIGs),¹⁷ and the National Information Exchange Model (NIEM), have produced results and show ongoing promise. PM-ISE's role is to help mission partners find common mission equities, to help them implement functional and technical standards, and to drive resolution of policy issues.

Throughout this Report, mission partner achievements are highlighted to emphasize the many incremental steps taken throughout the ISE to build capabilities and ensure information sharing across domains and mission equities. The hallmark projects and achievements within the ISE have often been developed through many steps involving smaller combined efforts that have a significant cumulative effect. In the same way, we recognize the breadth of work and the investment our mission partners make to constantly enhance the success of the ISE. They are the essential pieces in a very large and important puzzle.

¹⁷ In 2010, the FBI created six Regional Intelligence Groups for the purpose of identifying regional threats and to facilitate information sharing from a national and local perspective. RIGs are also establishing a strong record in creating intelligence products regarding domain awareness to the state and local community, including the fusion centers. Information from the RIGs is also coordinated through the FIGs.

1.3 Strengthening Information Sharing and Information Protection

One of the biggest roadblocks to expanding information sharing is the fear by many agencies that other organizations will fail to adequately protect the information they are provided with. As the WikiLeaks story emerged, concerns were voiced that information sharing efforts would suffer a setback. This Administration is committed to improving information sharing by better protecting the information that is shared. Guidance throughout the Executive Branch has been consistent: we must continue to accelerate our information sharing in a responsible and secure way. As reinforced by Senate Homeland Security and Governmental Affairs' Chairman Lieberman, Ranking Member Collins, Secretary of Defense Gates, OMB Director Lew, and Director of National Intelligence Clapper, we must champion efforts to further strengthen information sharing as well as to protect that information.

"To ensure we share and protect information effectively, we must work to find the sweet spot between the two." – DNI Clapper

The WikiLeaks disclosures primarily involved classified information, but the fundamental challenges associated with sharing and protecting sensitive information span across all security domains. Missions do not stop at the security domain or at organizational boundaries. Fundamental policies and solutions should be framed to address all types of protected information, classified and unclassified, held by the Federal Government and by our state, local, tribal, private sector, and international mission partners. Across all mission partners, we

need to establish structural elements such as strong governance, strategy, and policy to promote common, comprehensive solutions and to discourage individual agency-based, bilateral, and fragmented approaches.

PM-ISE is leading the process, along with ISE mission partners, of developing the National Strategy for Information Sharing and Protection, which will update and replace the 2007 *National Strategy for Information Sharing*. While the new Strategy is still under development, it is clear that to make the ISE work, we need to focus on information—discovering it, sharing it, protecting it, fusing it, and reusing it. The ISE needs an information-centric approach in alignment with the original mandate for the ISE. Further, to "open the aperture" to the totality of terrorism-related information as directed by law, efforts must continue to enhance partnerships with mission partners across all five communities—law enforcement/public safety, defense, intelligence, homeland security, and diplomacy. Moving forward, solutions must have broad applicability to a variety of mission needs, including CT and homeland security.

1.4 Structure of this Report

Building the ISE is not a short-term effort. It is a process that must evolve and adapt to emerging technologies and threats. To remain relevant and effective, enhancements and extensions to the foundations of the ISE are critical. While we celebrate the achievements and progress made towards sharing information and disrupting terrorist attacks, we also recognize that improvement is always both possible and necessary.

This Report describes information sharing progress since July 2010, including information on major ISE projects and activities launched by mission partners that have contributed significantly to inter-governmental information sharing. The Report is organized into five central themes encompassing the specific requirements set forth in IRTPA, the guidelines and requirements supporting the creation and implementation of the ISE¹⁸ and the guiding principles and foundational elements included in the 2007 *National Strategy for Information Sharing*:

1. Strengthening Management and Oversight
2. Improving Information Sharing Activities
3. Establishing Standards for Responsible Information Sharing and Protection
4. Enabling Assured Interoperability Across Networks
5. Enhancing Privacy, Civil Rights, and Civil Liberties Protections

While primarily focused on terrorism-related initiatives, the Report also describes mission partner accomplishments, some of which may not have been developed explicitly to support CT, but which may ultimately become “best practices,” with applicability to information sharing and collaboration government-wide, including within the ISE.¹⁹

Classified Supplement

The PM-ISE is responsible for reporting on the state of the ISE and information sharing across the Federal Government. To more accurately inventory important developments that encompass terrorism-related information sharing, it is necessary to include a classified supplement that will be sent to Congress under a separate cover letter.

18 White House Memorandum for the Heads of Executive Departments and Agencies, SUBJECT: Guidelines and Requirements in Support of the Information Sharing Environment, 16 December 2005

19 The fact that the ISE can leverage these achievements is consistent with one of its key attributes identified in IRTPA—to build upon existing systems capabilities currently in use across the government.

2 Strengthening Management and Oversight

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, established the position of a Program Manager to "plan for and oversee the implementation of, and manage" the Information Sharing Environment (ISE), and to be "responsible for information sharing across the Federal Government."²⁰ Consistent with the direction and policies issued by the President, the Director

of National Intelligence (DNI), and the Director of the Office of Management and Budget (OMB), the Program Manager, Information Sharing Environment (PM-ISE) issues government-wide procedures, guidelines, instructions, and functional standards,²¹ as appropriate, for the management, development, and proper operation of the ISE. In strengthening the management and oversight of the ISE, the PM-ISE actively governs, integrates performance and investment, engages stakeholders, and encourages a culture of information sharing.

ISA IPC members include:

- Central Intelligence Agency
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of the Interior
- Department of Justice
- Department of State
- Department of Transportation
- Department of Treasury
- Federal Bureau of Investigation
- General Services Administration
- Joint Chiefs of Staff
- National Counterterrorism Center
- Office of the Director of National Intelligence

2.1 ISE Governance

The ISE is realized by the investment of mission partners and made relevant through its use by front line law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. To effectively coordinate and govern the many information sharing activities, the PM-ISE has been leading interagency policy harmonization.

2.1.1 Information Sharing and Access Interagency Policy Committee (ISA IPC)

The ISA IPC is the interagency forum for overseeing the planning and implementation of the ISE. The ISA IPC was formed by a White House memo in 2009²², which integrated the existing Information Sharing Council (ISC) established by IRTPA into the IPC framework and

²⁰ IRTPA §1016(f)

²¹ Ibid.

²² White House Memorandum, "Strengthening Information Sharing and Access," 2 July 2009

strengthened national information sharing efforts by bringing the work of the ISC's Sub-Committees and working groups under the auspices of the Executive Office of the President (EOP). The ISA IPC prioritizes interagency efforts and aligns policy to facilitate the implementation of the ISE.

In its capacity as the ISC, the ISA IPC formally charters Sub-Committees to provide advice and support to the IPC on a range of related issues within their designated portfolios, and inform ISE planning and implementation. Sub-Committees are generally chaired by ISE mission partners and supported by PM-ISE staff. The ISA IPC directs the actions and tasks assigned to the Sub-Committees and regularly monitoring their progress on goals and objectives.

ISA IPC Sub-Committees have formed a number of Working Groups to address discrete issues or topics within the Sub-Committees portfolio. For example, on 1 June 2011, PM-ISE hosted an information sharing and protection Standards Summit, kick-starting a new interagency working group across federal, state, local, and tribal government representative partners, focused on identifying "best of breed" information sharing standards in government. Unlike other federal initiatives which focus on standards for just one set of partners, this working group will include all federal as well as state, local, and tribal government representative partners. This initiative will reuse the best existing government standards for responsible information sharing and protection, refine them, and encourage industry adoption of their standards into commercial products the government can buy with interoperable standards "baked-in" from the start.

Figure 2 shows the Sub-Committees and Working Groups of the ISA IPC. The five Sub-Committees and their corresponding Working Groups are discussed in greater detail in this chapter and throughout this Report.

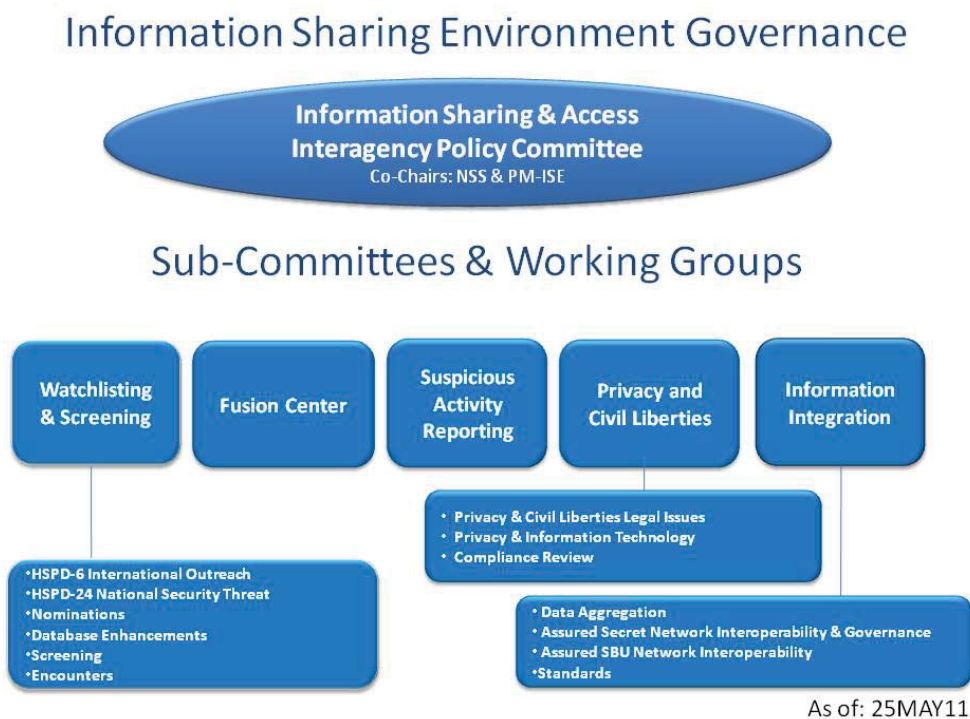


Figure 2. ISA IPC Sub-Committees and Working Groups

Since June 2010, the PM-ISE has served as a co-chair of the ISA IPC, along with a counterpart from the White House National Security Staff (NSS). This dual role for the PM-ISE is an acknowledgment that policies, business practices, architectures, standards, and systems developed for the ISE can be applicable to other types of information beyond terrorism and vice versa, because the scope of the IPC is broader than the scope of the ISE.²³ As co-chair, the PM-ISE helps ensure that there will be the closest possible alignment between the ISE and broader national security information sharing activities.

Since January 2011, ISA IPC Sub-Committees and Working Groups have organized and managed their efforts and report their accomplishments on a quarterly basis in line with annual and longer-term objectives and goals for the ISE. Sub-Committees and Working Groups derive these key objectives and areas of responsibility in the form of concrete goals aligned to the mission needs as specified in the annual ISE programmatic guidance, the *National Strategy for Information Sharing*, and priorities specified by the Administration. This process is discussed in the Performance and Investment Integration section below.

2.1.2 Working with State, Local, and Tribal Partners

Several of the ISA IPC Sub-Committees and Working Groups communicate and coordinate closely with representatives of non-federal organizations because they are recognized as valued partners by all ISE stakeholders. These representatives are chosen because they are members of an association, an advisory committee, or a wholly-owned national subsidiary of state or local governments. These representatives function as spokespersons for nongovernmental groups or stakeholders, providing the views and perspectives of their respective entities.

As of this Report, the following non-federal organizations coordinate closely with select ISA IPC Sub-Committees and working groups:

- **Criminal Intelligence Coordinating Committee (CICC)** – Fusion Center Sub-Committee and the SAR Sub-Committee
- **Global Justice Information Sharing Initiative (GLOBAL)** – Fusion Center Sub-Committee, SAR Sub-Committee, Information Integration Sub-Committee (Standards Working Group)
- **Regional Information Sharing Systems (RISS)** – Information Integration Sub-Committee (Assured SBU Network Interoperability Working Group)

²³ White House Memorandum, Subject: Appointment of the Program Manager, Information Sharing Environment (3 June 2010)

2.1.3 Interdependencies

Responsible information sharing is cross cutting and a number of dependencies can be found across the ISE governance organization. A key role of Sub-Committee and Working Group Chairs is to assist the ISA IPC in identifying these interdependencies and to collaborate on developing solutions. For example, a joint effort of the Assured Secret Network Interoperability Working Group of the Information Integration Sub-Committee and the Fusion Center Sub-Committee led to the development of the *State, Local, Tribal User-Validated Fusion Center Mission Requirements Initiative* report. This document communicates fusion center information needs to federal mission partners and application owners, and informs the technical access and connectivity solutions that are being developed by the Federal Government to securely share information with fusion centers.

2.1.4 Department and Agency Information Sharing Offices

More than half of the ISE departments and agencies have dedicated information sharing offices, directorates, divisions or executives. These offices serve as focal points for federal information sharing issues and direct department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards. The establishment of a single office to ensure full cooperation in the development of the ISE is a best practice and is encouraged across the ISE.

In October 2010, the DNI strengthened the responsibilities and title of the Intelligence Community Information Sharing Executive (IC ISE). The IC ISE is now directly accountable to the Principal Deputy Director of National Intelligence and works in close coordination with the Deputy Director of National Intelligence for Intelligence Integration, the Assistant Directors of National Intelligence, the PM-ISE, and IC elements. The IC ISE is developing a coordinated and comprehensive plan for responsibly managing information sharing activities within the ODNI, across the IC, and with all of its mission partners. To this end, the IC ISE has established an internal governance process, the Information Sharing Executive Group, for ensuring a coordinated information sharing approach within ODNI, and has refashioned and reinvigorated the IC ISE's engagement activities and governance across the IC, via the Information Sharing Steering Committee, to do the same. A close working relationship with PM-ISE helps ensure that information sharing and protection activities within the IC are consistent and interoperable with the steps being taken across the entire U.S. Government, as well as with state, local, tribal, and private-sector partners.

The Department of Homeland Security (DHS) designated the Under Secretary for Intelligence and Analysis (USIA) to concurrently serve as the Department's Information Sharing Executive. In that capacity, the USIA chairs the Department's Information Sharing Governance Board (ISGB), which was established in 2007 to serve as the Department's senior-level governance body for information sharing. The ISGB develops departmental policy recommendations and resolves issues involving information sharing across DHS components, as well as with federal state, local, tribal, territorial, private-sector and foreign partners. For the past year, the ISGB has identified information sharing priorities using the Quadrennial Homeland Security Review strategic framework. To continue to strengthen and mature the

information sharing governance structure, the ISGB is working to ensure that the Department's information sharing priorities are integrated within the Department's overall, Planning, Programming, Budgeting and Execution processes and are reflected in the Future Year's Homeland Security program. DHS also works closely with the PM-ISE to ensure alignment and coordination with the ISE. In January 2011, the DHS Chief Information Officer (CIO) established and filled an Information Sharing Executive position to ensure the removal of technical barriers associated with implementing the ISE.

The FBI established an ISE and a Chief Information Sharing Officer (CISO) position in 2008 to serve as the senior FBI official for information sharing and the principal advisor to FBI executives for information sharing matters. The CISO is the Executive Secretary of the FBI's Information Sharing Policy Board and coordinates internal and external information sharing policies. In February 2011, the Directorate of Intelligence (DI) created a new DI Branch, the Intelligence Integration Branch (IIB), to enhance information sharing and outreach efforts. The IIB is specifically charged with engaging federal, state, local, tribal, and IC partners to increase the effectiveness of information sharing and to coordinate efforts to combat violent extremism.

2.1.5 Other Interagency Policy Coordination and Implementation Bodies

In addition to using the ISA IPC as the primary interagency policy coordination body for information sharing and access, ISE mission partners also coordinate through a number of other IPCs related to national information sharing and protection functions. These include: the Transborder Security Portfolio's IPC, and its associated Sub-IPCs and associated working groups, which include topics such as maritime security, surface transportation, global supply chain, and aviation security; the Records Access and Information Security IPC, which addresses the protection and handling of sensitive information; the Information Communications Infrastructure IPC, which addresses cybersecurity issues; the Critical Infrastructure Protection and Resilience IPC; and the Countering Nuclear Threat IPC.

Additionally, PM-ISE coordinates with strategic and tactical efforts across interagency governance bodies that involve information sharing and access issues. These bodies include: the Federal CIO Council and its component committees, including the Information Security and Identity Management Committee; the IC CIO Council and its component committees; the Committee on National Security Systems (CNSS) and its component working groups; the Unified Cross Domain Management Office; the National Information Exchange Model (NIEM) Program Management Office at DHS, and the Controlled Unclassified Information (CUI) Program Office at the National Archives and Records Administration (NARA). By leveraging these bodies, PM-ISE ensures that equities related to information sharing and access are fully coordinated and that they are represented consistently across all federal departments and agencies and across all related disciplines, without duplicating efforts.

2.2 Performance and Investment Integration

Governance and decision-making across the ISE are supported by the integrated performance and investment process, shown in Figure 3. The PM-ISE actively monitors agencies' progress toward information sharing performance objectives and goals and ensures the integration of performance with investment.

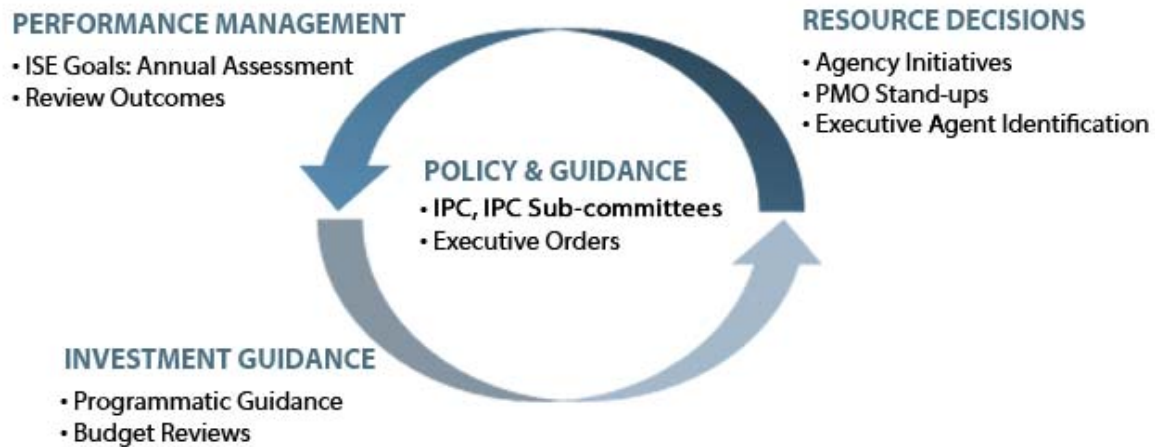


Figure 3. Performance and Budget Integration Process

2.2.1 Three-way Partnership (Agencies, OMB/NSS, and PM-ISE)

The ISE continues to embrace the whole of government approach as documented in the President's May 2010 National Security Strategy. Jointly, ISE member agencies, OMB/NSS, and PM-ISE are defining the way forward and have demonstrated their commitment to an interagency process dedicated to information access and sharing. The governance and decision-making process, tightly interwoven with budget and performance integration, has been keeping pace with this progress.

Performance and investment processes focus on ensuring that the ISE continues to make progress in advancing its goals and objectives. The ISE programmatic guidance, annual budgets and investments, and committee and staff work plans for each subsequent year are developed based on the prior year accomplishments and any relevant changes in policy, strategy, technology, and other external factors.

2.2.2 Programmatic Guidance

To codify the initiatives in the President's Budget, OMB/NSS issues programmatic guidance each year for the federal budget describing ISE priority areas. It provides direction to agencies for future spending on mission priorities, critical information resources, and supporting information technology investments focusing on increased federal collaboration with state, local and tribal governments, as well as with the private sector. The implementation of this programmatic guidance through the governance process moves each of the agencies closer to collaborative endeavors—eliminating redundancies, identifying re-use options, leveraging best practices, and consolidating similar projects across organizational boundaries.

Last year, ISE programmatic guidance was issued to agencies for the development of their fiscal year (FY) 2012 budget submissions. The FY 2012 ISE-specific programmatic guidance identified the following five priorities:

1. Building a national integrated network of fusion centers;
2. Continuing implementation of the NSI;
3. Establishing Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) network interoperability;²⁴
4. Improving governance of the classified National Security Information program; and
5. Advancing implementation of CUI policy.

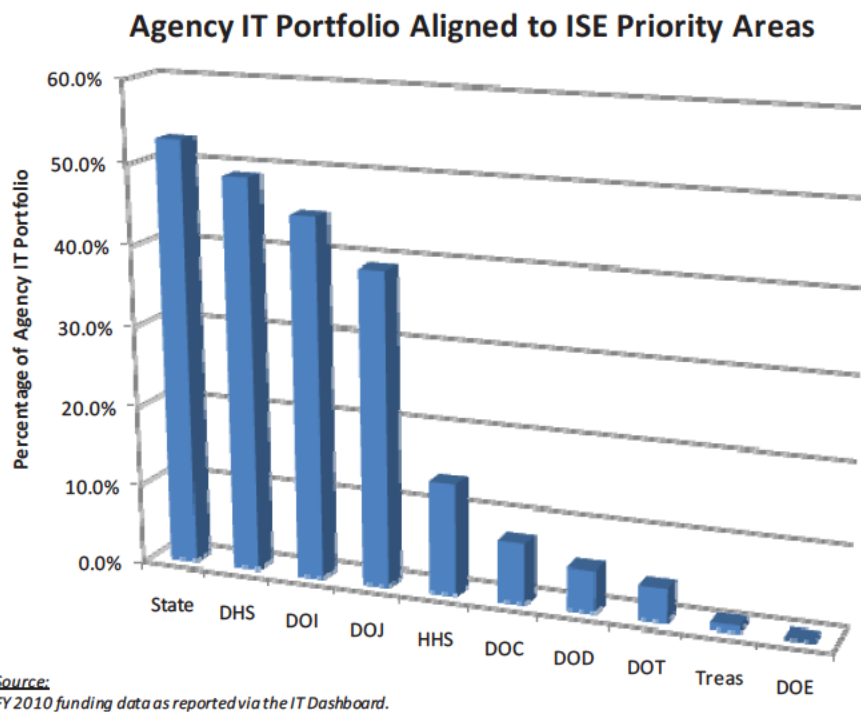


Figure 4. Percentage of the federal agencies' IT budget aligned with at least one of the ISE priority areas

24 On 4 November 2010, President Obama issued Executive Order 13556, "Controlled Unclassified Information," which addresses a broad scope of activities related to information previously labeled "Sensitive But Unclassified (SBU). On 9 June 2011, the CUI Office issued the "Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556." In implementing this guidance, references to "Sensitive But Unclassified (SBU)" will be phased out in future PM-ISE reporting.

2.2.3 Strategic Investment

Partner agencies continue to strategically invest in the ISE and indicate alignment of their information technology investments to the ISE priorities via OMB's annual agency Information Technology (IT) portfolio data request. The data captured via the OMB Circular A-11 Exhibit 53²⁵ reporting for FY 2012 is only one step of many used to understand the ISE priority area costs of mission partners. This data revealed that approximately 15 percent of the Federal Government IT spending is aligned to one or more of the ISE priorities. As reported by agencies, Figure 4 depicts the percentage of their agency's IT budget that is aligned with at least one of the ISE priority areas. This chart illustrates that several agencies—e.g. State, DHS, Department of the Interior (DOI) and the Department of Justice (DOJ)—continue to align a substantial portion of their IT budgets to the ISE priority areas.

Initial use of the enhanced Exhibit 53 reporting allowed analysis of federal agency IT spending aligned to the ISE priority areas focuses around the primary functional mappings to the lines of business (LOB) within the Federal Enterprise Architecture Business Reference Model (FEA BRM). As anticipated with IT investments, the strongest primary mapping was attributed to the FEA BRM IT management LOB (38 percent), as depicted in Figure 5. IT management is broad; it captures the coordination of information and technology resources and systems to support or provide a service.²⁶ The two largest sub-functions under the IT management LOB are IT Infrastructure Maintenance (30 percent) and Information Sharing (3 percent). The analysis also revealed significant primary mapping to other mission LOBs such as Homeland Security (18 percent), Community and Social Services (9 percent), Health (7 percent) and Law Enforcement (6 percent), demonstrating a focus of these investments toward advancing agency mission areas. Further analysis and improved data quality in future reporting will help to identify potential opportunities for investment decisions in these areas.

25 OMB Circular A-11 Section 53, 21 July 2010
(http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s53.pdf)

26 Federal Enterprise Architecture Consolidated Reference Model v2.3, October 2007 (<http://www.whitehouse.gov/omb/e-gov/fea/>)

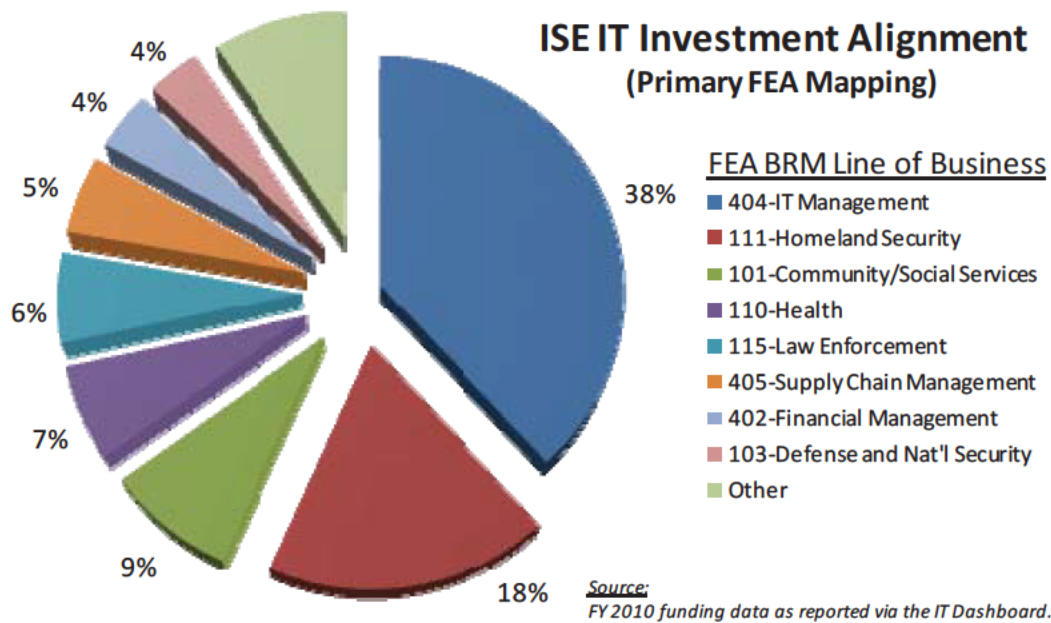


Figure 5. ISE IT Investment Alignment

Two of the ISE priority areas, SBU Interoperability and CUI, accounted for the vast majority of IT spending alignment. This is expected, as investments in these ISE priority areas tend to be larger, agency-wide IT initiatives. More detailed analysis will enable better understanding of how strategic investments in these areas can be effectively utilized, and how those investments can be encapsulated in larger IT infrastructure investments.

Based on agency reporting via the OMB Exhibit 53, depicted in Figure 6, more than half of agency IT investments aligned to ISE priority areas directly supported agency-specific mission objectives. This is an important perspective, as agencies with alignment to ISE priorities are focusing investments and resources toward supporting their mission objectives that capture the value of the ISE, versus focusing on supporting infrastructure-type activities.

*Table 1 – Investments aligned to the SBU
priority area*

Agency	SBU Investments
Department of Commerce	2
Department of Defense	1
Department of Energy	16
Department of Homeland Security	99
Department of the Interior	3
Department of Transportation	11
Department of Treasury	10
Federal Bureau of Investigation	16

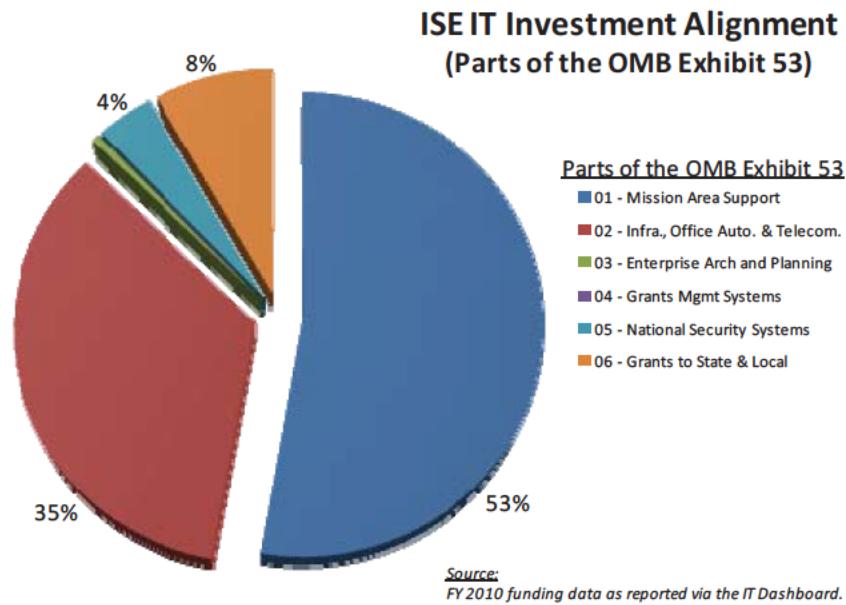


Figure 6. ISE IT Investment Alignment to Parts of OMB Exhibit 53

Continued collection of this data year-after-year will allow for trend analysis of programmatic efficiencies to better understand and account for ISE spending. For example, working closely with OMB/NSS, PM-ISE was able to focus on the ISE priority area for SBU systems, networks and portals. The initial funding submissions revealed 182 investments aligned to the SBU priority area. Based on this data, the PM-ISE created SBU inventory worksheets for agency validation and the current revised number of SBU investments is 158 investments, as depicted in Table 1. DHS identified the largest number of SBU investments, but already has efforts underway to reduce and consolidate the number of SBU systems. For example, the Homeland Security Information Network (HSIN) program, as a result of the Federal CIO TechStat session and recommendations in the 25 Point Plan to Reform Federal IT, has retooled its management and technical approach for the development of the new HSIN platform to ensure continuous user input and feedback, delivery of functionality in shorter timeframes, and will address recommendation that balance the need to share versus safeguard. Further analysis into the services and capabilities provided by these investments could potentially yield additional opportunities for increased SBU interoperability within and across partner agencies.

As data quality improves, PM-ISE analysis will be able to further identify gaps and areas of opportunities for strategic investments in innovative information sharing technologies and programs. Initial understanding of these gaps has led to focused investments for innovative ideas in the priority areas of cargo screening, SAR, standards, and privacy. Going forward, PM-ISE will continue to support innovative opportunity areas for advancements in ISE focus areas. The PM-ISE is working closely with OMB to improve the quality of data in subsequent cycles, and to support the strengthened use of data in resource allocation and planning processes.

2.2.4 Performance Management

The ISE continues to employ a performance management process to report on results. This will flow from the new National Strategy for Information Sharing and Protection (as discussed later in this chapter) and the priorities defined by the White House. As this process matures, ISE partners and stakeholders will be held accountable by monitoring operation and maintenance; self-reporting; mitigation of risks; and exercising the ISE through a combination of quantitative and qualitative measures. Each initiative will be assessed, measuring its progress and value to the overall ISE.

The PM-ISE works closely with each ISE agency to obtain feedback and gather insights on improving the processes and measures, with the intent of influencing the performance at each of the agencies. The results of this year's annual performance assessment can be found throughout this Report and in Appendix A.

The PM-ISE will continue to revise the existing performance framework to ensure alignment and build upon previous performance measurement best practices. The PM-ISE will monitor performance across strategic investments, mapping the ISE strategic vision to initiatives, and outlining clear measures. This systematic approach requires a clear strategic vision to define the expected mission capabilities, and requires full representation and performance measurement of all the ISE initiatives.

The Performance Framework will consist of the following four views:

1. **ISE Strategic View:** Defines the vision and scope and answers the questions, "Why?" and "Toward what outcomes are we working?"
2. **Initiative View:** Defines a work-breakdown structure that answers the question, "What are we doing to achieve the vision?"
3. **Measure View:** Describes the value to the community and answers the question, "How well are we doing in terms of achieving the vision?"
4. **Roadmap View:** Presents a schedule of the priority work that remains to be completed.

Because the ISE has made substantial strides in maturity, this effort will not only measure current progress, but also the community's collective capacity to achieve mission capabilities.

2.3 Stakeholder Engagement

Stakeholder engagement has remained a top priority for the ISE community this year and will continue to be a key component for strengthening management and oversight of the ISE in the months and years ahead. As such, the PM-ISE has focused on building a multi-tiered governance and engagement strategy driven by mission partners and inclusive of the technology industry.

First, the PM-ISE brings the voice of the analysts, operators, investigators, practitioners, and subject matter experts from across communities to a collective table. Regular engagement with these communities of interest (COIs), formed to promote collaboration, provides ISE mission partners with advice and recommendations on specific topics, activities, and operational needs. In January 2011, the PM-ISE met with the Executive Director of the International Association of Chiefs of Police (IACP). At this meeting a number of common goals were identified and related transactions were put into place to establish a partnership. For example, the IACP is now a listed partner on the ISE website, and information sharing success stories told in *Police Chief's* magazine (the official publication of the IACP) are highlighted on the ISE website.

The ISE also provides a means for mission partners to regularly communicate and collaborate with industry. Standards development organizations assist mission partners in developing, coordinating and maintaining technical standards that address the interests of their varied users.

As COIs naturally form around agencies, mission partners, and ISE initiatives based on their specific domains of activity, PM-ISE strives to engage these communities through live events and roundtables scheduled across the country; the ISE website; and the use of social media. The PM-ISE has actively engaged with representatives from every level of government; state, local, and tribal partners; industry; international allies; and the public. The Program Manager, or his delegate, has spoken at more than 40 events, reaching thousands of people. In the last year, the PM-ISE participated in the Law Enforcement Information Management Conference, the National Fusion Center Conference, Integrated Justice Information Systems (IJIS) Institute Briefings, the DoD Identity Protection and Management Conference, and many others. A list of events is included in Table 2.

The PM-ISE also recognizes that the community does much of its work online. This venue for communications enables bi-directional interaction and is critical for bringing our state, local, tribal, and international partners together with industry. Online tools are an essential complement to direct outreach enabling us to support the interaction called for by IRTPA, Section 1016. Accordingly,

Emphasis on Industry

This year, the PM-ISE placed a special emphasis on engagement with standards organizations and industry consortia. Standards organizations assist mission partners in developing, coordinating and maintaining technical standards that address the interests of their varied users. Industry consortia provide a means to communicate ISE requirements to industry and provide industry with a means to communicate potential solutions to mission partners. From here, mission partners can develop mission-driven requirements, standards and processes for the ISE which industry can then use for product development.

www.ise.gov received various upgrades and enhancements over the last year, and the site has become a robust, collaborative tool for our mission partners and stakeholders.

Intelink Symposium	Cisco Public Service Summit	Excellence in Government	Averting Armageddon
Google Innovation for the Nation	Central Command Visit	FBI InfraGard Critical Sector Forum	Special Operations Command Visit
National Fusion Center Conference	West Virginia Fusion Center Opening	GLOBAL Executive Steering Committee	National Indian Gaming Conference
Symantec Government Symposium	GLOBAL Intelligence Working Group	Northern Virginia Technology Council	Tribal Police Chiefs Mid-Year Meeting
Computers, Freedom, and Privacy Conference	Domestic Highway Enforcement Conference	Interagency Air Domain Awareness Summit	Object Management Group Technical Meeting
Symposium on Identity and Trust on the Internet	Maritime Information Sharing Taskforce	Global Maritime Information Sharing Symposium	TechAmerica Homeland Security Committee
FOSE Institute: Knowledge Management Conference	High Intensity Drug Trafficking Area Directors Meeting	South by Southwest Interactive Conference	Major Cities Chiefs Association Conference
FBI Criminal Justice Information Services Advisory Policy Board	Annual Symantec Government Symposium	Digital Policy Management Technical Exchange Meeting	Air Domain Awareness Summit Executive Session
FBI Global Justice Advisory Committee	International Open Government Data Conference	Architecture for Leaders Course at National Defense University	Regional Information Sharing Systems Policy Board Summit
IJIS Institute Summer and Winter Industry Briefings	Face Recognition Workshop: From Bones to Bits	TechAmerica's IdentEvent: Cyber Security and Identity	Federal Cybersecurity Conference and Workshop
Department of Defense Enterprise Architecture Conference	Regional Information Sharing Systems National Policy Meeting	Executive Board of International Association of Chiefs of Police	Committee on National Security Systems Annual Conference
International Association of Chiefs of Police Annual Conference	National Maritime Intelligence Center Conference on Collections	Homeland Security Information Network Advisory Council Meeting	Major Cities Chiefs Association Intelligence Commanders Meeting
Department of Defense Identity Protection and Management Conference	Forum on Leveraging Technology to Revolutionize Content-Centric Security	Government Technology Research Alliance Defense Gov Council Meeting	Legal Roadblocks to National Strategy for Trusted Identities in Cyberspace
Office of the Director of National Intelligence Identity Intelligence Conference	International Association of Chiefs of Police – Law Enforcement Information Management Conference	Armed Forces Communications and Electronics Association Homeland Security Conference	National Native American Law Enforcement Association Annual Conference
Association for Enterprise Information – Interagency Series on Responsible Information Sharing	Center for Strategic and International Studies National Strategy for Information Sharing Event	Oxford Internet Institute – Information Sharing for Counter-Terrorism and National Defence	NextGen Interagency Architecture Engineering Board – Joint Planning and Development Organization

Table 2 –Events with PM-ISE Participation

Specific upgrades include:

- **Mission Partner Pages** featuring our information sharing mission partners, latest news and social media updates
- **Multimedia Gallery** with informative podcasts, videos, and news
- **Collaboration Tools** that allow the community to provide feedback and discuss initiatives and policies
- **Calendar** to keep track of upcoming events and trainings
- **Document Library** offering important documents easily in our comprehensive repository
- **ISE Partners Resource Directory** to help locate key information sharing partners' websites
- **Improved timeliness** for news, featured stories, blog posts, and job opportunities



Figure 7. www.ISE.gov

2.3.1 Refreshing of the Vision for Information Sharing

In 2010, the EOP asked the PM-ISE to refresh the 2007 *National Strategy for Information Sharing* in order to outline an updated vision and strategy for responsible information sharing and protection. Leveraging the 2007 Strategy, the refreshed strategy will bring forward the foundational pieces of the 2007 document and will provide a target vision for the ISE which embraces a trusted, data-centric information sharing and protection vision. The new strategy will also anchor on the National Security Strategy's call for a 'Whole of Government' approach and focus on the mandates within the IRTPA to empower investigators, analysts, and operators with actionable and timely information and intelligence.

Input from ISE mission partners is critical to ensure this refreshed strategy supports the CT mission and provides complete solutions for ISE mission partners. To accomplish this, the PM-ISE is inviting mission partners and agencies to provide their vision for the ISE, as well as their valuable input on various topics

for incorporation into the new Strategy. For example, upon the request of the PM-ISE, the DOJ Global Justice Information Sharing Initiative (GLOBAL) Criminal Intelligence Coordinating Council (CICC) convened a task team to coordinate state, local, and tribal intelligence-related input and recommendations regarding the Strategy refresh. The PM-ISE efforts to develop a strategy for responsible information sharing and protection will continue over the next several months. The PM-ISE has engaged or anticipates engaging with the mission partners and agencies listed in Table 3.

Outreach To	Agency/ Partner
Information Assurance / Data Aggregation	CIA
DEA Chief of OPS & Intel	DEA
Special Operations Division	DEA
High Intensity Drug Trafficking Areas	ONDCP
Information Sharing Governance Board/Information Sharing Coordinating	DHS
DHS Intelligence and Analysis	DHS
DHS I&A State and Local Program Office	DHS
DHS Chief Information Officer Council	DHS
Directorate for National Protection and Programs (NPPD)	DHS
Office of Infrastructure Protection, NPPD	DHS
Office of Cybersecurity and Communications, NPPD	DHS
Critical Infrastructure and Key Resources (CIKR)	DHS
Private Sector Office	DHS
US VISIT, NPPD	DHS
DHS Technology Topics (DHS CIO)	DHS
U.S. Coast Guard	DHS
Customs and Border Protection	DHS
Immigration and Customs Enforcement	DHS
United States Secret Service	DHS
Transportation Security Administration	DHS
Federal Emergency Management Administration	DHS
U.S. Citizenship and Immigration Services	DHS
OSD CIV Policy	DoD
DoD CIO	DoD
Directorate of Information Sharing and Partner Engagement (ISPE), OUSD(I)	DoD
Office of the Under Secretary of Defense for Intelligence USD(I)	DoD
National Drug Intelligence Center	DOJ
Criminal Intelligence Coordinating Council (CICC)	DOJ/CICC
Global Justice Information Sharing Initiative	DOJ/GLOBAL
FBI National Security Branch	FBI
FBI Fusion Center Integration Unit	FBI
FBI Criminal Justice Information Services	FBI

FBI Directorate of Intelligence	FBI
FBI Intelligence Operations Branch	FBI
FBI Intelligence Integration Branch	FBI
FBI Counterterrorism Division	FBI
FBI Fusion Center Integration Unit	FBI
FBI National Threat Center Section	FBI
FBI Guardian Management Unit	FBI
FBI Information Technology Branch	FBI
FBI Office of the Chief Knowledge Officer	FBI
FBI Chief Information Sharing Officer	FBI
Privacy/Civil Liberties Executive Committee	Interagency
ISA IPC and Sub-Committees/Working Groups	Interagency
Identity Credential and Access Management (ICAM) Sub-Committee	Interagency
Tribal Working Group/DOJ Office of Tribal Justice	Interagency
NCTC Organization (general outreach)	NCTC
– Watchlisting Business Process	NCTC
– Information Integration Center/Gentle Breezes Tiger Team (GBTT)	NCTC
– Office of National Intelligence Management, Information Sharing Program and	NCTC
– Chief Scientist	NCTC
Information Assurance	NSA
R6	NSA
White House Coordination	NSS
– Transborder IPC	NSS
– Cyber Directorate	NSS
– Resiliency Directorate	NSS
– Counterterrorism	NSS
– WMD	NSS
– Office of National Drug Control Policy (ONDCP)	NSS
IARPA	ODNI
National Maritime Intelligence Center (NMIC)	ODNI
Private Sector Partnership Group (Industry)	ODNI
Partnership Engagement Office	ODNI
IC Information Sharing Executive	ODNI
Information Sharing Executive Group	ODNI
National Counter Intelligence Executive (NCIX)	ODNI
Consular Affairs	State
Office of Management Policy, Rightsizing, and Innovation	State
IJIS Biannual Meeting	IJIS
Office of Intelligence, Security, and Emergency Response	DOT

Table 3. Stakeholders Engaged in the Development of a Refreshed National Strategy for Information Sharing

2.4 ISE Culture Initiatives

Achieving a culture where responsible information sharing is the norm rather than the exception is a major goal of IRTPA that was further expressed in the 2005 *Presidential Guidelines and Requirements in Support of the ISE*.²⁷ The 2007 *National Strategy for Information Sharing* called for changing “government culture to one in which information is regularly and responsibly shared and only withheld by exception.”²⁸ However, changing the culture of an organization, particularly a large organization, is a formidable challenge. The breadth and complexity of the ISE compounds the task since the environment extends across all levels of government in the United States, into parts of the private sector, and includes foreign government partners as well.

Leaders who endorse and advocate for responsible information sharing are essential to meeting mission objectives in the post- 9/11 era. Information sharing has traditionally been an organizational prerogative, with a bias for protecting information, due to the perceived risks associated with information sharing. However, the events of 9/11 clearly demonstrated that the aversion to information sharing among governmental agencies in fact created risks to national security that far outweighed the benefits of protecting information.

In order to achieve a change in the culture, leaders at all levels of federal, state, local, and tribal government must set expectations and clearly demonstrate their commitment to responsible information sharing policies and goals. Positive use of appraisal system tools, commitment to quality training, and judicious, credible use of incentives by leaders at all levels of government can contribute to the imperative for cultural change.

The FBI reports that 16,082 employees (13,515 Special Agents and 2,567 Intelligence Analysts) have formally adopted ISE requirements for information sharing into their performance work plans.

(2011 ISE Annual Performance Assessment)

The PM-ISE identified concrete steps and business practices that could facilitate change in three broad areas: making information sharing an evaluation factor in performance appraisal systems; incorporating information sharing and collaboration modules into agency training programs; and encouraging agencies to recognize information sharing as part of their awards programs. These three key areas—appraisals, training, and incentives—are essential elements for changing behaviors of employees and promoting accountability.

Creating a culture of sharing involves changing the way people value information sharing and collaboration by encouraging behaviors that foster sharing and discouraging those that do not. Rewarding behaviors that foster information sharing and adoption of collaborative cross-agency work

27 Memorandum for the Heads of Executive Departments and Agencies, Subject: Guidelines and Requirements in Support of the Information Sharing Environment President’s Guidelines, December 16, 2005

28 NSIS, p.11.

teams will improve performance throughout the government and enhance efforts conducted with non-governmental partners. People who are held accountable, properly trained, and rewarded for sharing and collaborating not only provide short-term improvements but, by serving as role models for others, effect lasting long-term culture change.

While tangible progress has been made in all three areas, we recognize that culture change encompasses a much broader range of activities and involvement of all mission partners. For example, work underway to support building communities of trust has been instrumental in changing the way that law enforcement agencies work with local communities—an important culture shift. In addition, other activities related to the Administration’s Open Government Initiative are also relevant to culture change. PM-ISE also continues to utilize performance management and investment tools such as programmatic guidance to motivate, facilitate and reward information sharing behaviors and practices. Essentially, all of the work done within the ISE facilitates the development of a culture of information sharing, as we develop the capabilities, policies, and mutual trust necessary to ensure that sharing information is the way we do business.

2.4.1 Appraisal/Information Sharing Behavior

Federal agencies continue to expand their programs to include information sharing and collaboration as part of the recruitment, orientation and performance evaluation of all employees; to increase and improve mission specific training programs; to encourage the use of incentive awards for collaborative efforts; to encourage joint duty-like assignments to foster knowledge sharing; and to create COIs around particular topics. In October 2009, the Director, Office of Personnel Management (OPM) issued a memorandum to federal Chief Human Capital Officers in which he stated “information sharing and collaboration should be a common, core behavior across all departments and agencies.” Information sharing is also a component of the Performance Management System Requirements under Intelligence Community Directive (ICD) 651, requiring IC agencies to take steps to include sharing and collaboration in their professional standards and evaluation processes.

Each respondent to the 2011 ISE Annual Performance Assessment reported that their ISE-related employees have information sharing and collaboration as components of their performance appraisals, showing a 14 percent growth from 2010. Moreover, 10 out of 14 of these same responding agencies reported that these information sharing and collaboration components were even included in the performance appraisals of employees without ISE responsibilities. This marks an improvement of 30 percent over the past year and consistent commitment to promoting this value within the ISE. The FBI’s Senior Executives as part of their performance evaluations, are rated on “Collaboration and Integration” indicative of the Bureau’s interest in rewarding information sharing efforts. The DoD provides authority to individual components and managers to include information sharing in performance appraisals and organizations such as the Joint Intelligence Task Force for Combating Terrorism Defense Intel Unit have incorporated these criteria into performance evaluations. The Assistant Secretary of Defense for Homeland Defense and America’s Security Affairs also evaluates employees on information sharing and collaboration. Further, the CIA, DHS, DNI, DoD, DOI, DOJ, and NCTC reported that they have specific policies to ensure that information sharing and collaboration are included in personnel appraisals.

2.4.2 Information Sharing Training

Training staff to both appreciate the importance of information sharing at all levels of operation and to effectively share information through existing and emerging mechanisms is essential to ensuring progress. In 2009, PM-ISE issued an ISE Core Awareness Training as an introduction to the ISE and its components; this module continues to be publically available online and generates a foundational understanding of the ISE. This year, DHS continued to work towards ensuring all required staff completes the ISE Core Awareness Training. In addition to ISE Core Awareness Training, the FBI provides numerous courses to contractors and personnel, including U.S. Persons and Information Sharing and how to use various FBI information sharing systems such as LEO, N-DEX, and eGuardian. Various seminar opportunities are also provided such as the Knowledge Week Seminar on IC Information Sharing and the Information Sharing Technology Speaker Series, which often addresses information sharing.



Information sharing training promotes not only the importance of information sharing, but also the importance of teambuilding, collaboration, best practices, and the specific skill development needed to execute sharing activities. Ten out of 14 (71 percent) of respondents to the 2011 ISE Annual Performance Assessment reported that they have implemented mission-specific training that supports information sharing and collaboration; compared to 2010, this equates to a positive growth rate of seven percent. Training efforts in the ISE have been ongoing since the passage of the IRTPA, beginning with basic foundational training, and now advancing to more focused, mission-specific efforts. PM-ISE is dedicated to linking mission partners with similar interests and training priorities in order to identify potential joint projects resulting in better products and cost efficiencies. Almost all partners with a CT mission report having implemented training that supports information sharing. In fact, all departments under the purview of the DNI reported implementing mission specific training to support information sharing and collaboration in this year's ISE Annual Performance Assessment. The DoD provides several related training opportunities through its Joint Knowledge On-Line portal, enhancing availability and ease of education. DHS not only has information sharing training for its own employees; it has also initiated a project with the Federal Law Enforcement Training Center to develop an information sharing training tailored to the law enforcement community. Meanwhile, the DOI has implemented information training for both sworn and non-law enforcement personnel. All of these efforts reflect a collective commitment to enabling information sharing through personnel training.

The NSI Program Management Office (NSI PMO) has developed and conducted extensive training including executive briefings, analytic training, and line officer training. According to the NSI First Quarter 2011 Activity Summary, the NSI is making great strides in providing SAR training to law enforcement and support personnel to help ensure that they are trained to recognize behavior and

incidents identified by law enforcement officials and CT experts from across the country as being reasonably indicative of criminal activity associated with terrorism. The NSI has been working with the IACP, the Major Cities Chiefs Association, the Major County Sheriffs' Association, the National Sheriffs' Association, the Association of State Criminal Investigative Agencies, and others to help deliver this training as quickly and efficiently as possible to all law enforcement officers.

- The Washington State Patrol (WSP) posted the SAR Line Officer Training video on the WSP Web site, and as of 31 March 2011, more than 1,400 WSP employees have viewed the training.
- The Virginia Fusion Center pushed the training out to the Virginia State Patrol staff, officers, and personnel, and has successfully trained every state trooper.
- The Georgia Bureau of Investigation has worked to get POST credit for officers who take the required SAR line officer and CICC privacy trainings, and will mandate that training be completed by 15 July 2011.
- The Southern Nevada Counter-Terrorism Center (SNCTC) posted the line officer training to the SNCTC Web site, which has allowed access to all law enforcement officers in the state of Nevada.
- The Florida Fusion Center is one of the first fusion centers to develop a customized line officer training program through LEAPS.TV, which also offers individual jurisdictions the opportunity to customize the program by adding information on specific procedures and practices within their agencies to the basic NSI PMO program.
- The Los Angeles County Sheriff's Office and the Memorial Institute for the Prevention of Terrorism have partnered to provide training to all deputies.

In response to the 2010 Baseline Capability Assessment (BCA), the DHS Office of Intelligence and Analysis (I&A) and the Homeland Infrastructure Threat and Risk Analysis Center sponsored three deliveries of the Introduction to Risk Analysis Course. The five-day course was offered in September 2010, December 2010, and February 2011 and was intended to support fusion centers in building the capability to regularly assess the local implications of time-sensitive and emerging threat information, contributing to risk analysis. Participant feedback, collected voluntarily after the conclusion of each course, suggests that the course provided fusion centers with the resources they need to enhance their ability to assess the local implications of threat information through the use of a formal risk assessment process.

The Watchlisting community, led by the NCTC and FBI's Terrorist Screening Center (TSC), in coordination with nominating and screening agencies, is developing a standardized training course to educate the community on the updated Watchlisting Guidance. The course is designed to help standardize watchlisting and screening processes and decisions and to improve the quality of information regarding known and suspected terrorists. To date, NCTC has facilitated pilot training sessions and is planning additional pilots in late spring/early summer. The classroom-based training is scheduled to be fully implemented by July 2011. An additional, web-based training module is scheduled to for development after implementation of the classroom-based training.

Another indicator of success regarding the production and availability of appropriate training and educational materials to support information sharing, is that all mission partners responding to the ISE 2010 ISE Annual Performance Assessment responded that the currently available ISE training is sufficient to support their mission. In addition, all federal agencies reported that their personnel receive training with a specialized privacy and civil liberties protection component at least annually.

2.4.3 Incentives

Positive reinforcement also plays an important role in encouraging an information sharing culture. Routinely recognizing and rewarding effective information sharing, as well as expertise and competency development, will serve to increase its frequency and the desire of personnel to improve efforts. To this end, 86 percent of ISE departments and agencies reported offering an award that includes information sharing and collaboration directly or indirectly as criteria. Moreover, the number of responding ISE departments and agencies that have identified an increase in information sharing and collaboration award nominations has doubled over the past year. But only three agencies—the DOJ, the Department of Transportation (DOT), and the FBI—report offering agency-specific incentives to encourage information sharing, indicating a clear area for improvement. FBI created the Chief Information Sharing Officer Award to enhance awareness of information sharing goals and the central role they play in the FBI’s National Security and Criminal missions. DOT offers cash awards to employees to acknowledge their involvement in information sharing efforts. And DHS reports that they continue to work towards implementing an award program to recognize information sharing.

2.4.4 Exercises

As information sharing becomes institutionalized, we expect to see elements of the ISE reflected in organizational exercises. For example, the FBI recently created a “National Level Exercise (NLE) Coordinator” position to ensure that the FBI’s intelligence component is being fully integrated with the NLE process.

In 2011, PM-ISE began looking at exercises being conducted at the national and interagency levels to understand how operational reality impinges on theory. While neither conducting nor directly participating in the exercises, PM-ISE will endeavor to collect lessons learned, to identify exercise-driven requirements for the ISE, and as necessary, to provide general guidance on incorporating ISE elements into operational exercises.

Federal Geospatial Concept of Operations

Now in its third year of development, the Federal Geospatial Concept of Operations (Federal GeoCONOPS) effort, led by the DHS, has reached a state of maturity for inclusion in National Level Exercises and transition to routine operational use. The goal of the Federal GeoCONOPS is to assure that sharing geospatial information for situation awareness is conducted effectively and in alignment with the Incident Command System, Homeland Security Presidential Directive (HSPD) 5 “Management of Domestic Incidents,” and National Response Framework policy and doctrine. In accordance with incident response doctrine, the Federal GeoCONOPS is being developed as an all-threats, all-hazards, all phases of the emergency management lifecycle resource. The Federal GeoCONOPS provides comprehensive guidance on authoritative sources of information, defines the roles of Emergency Support Functions for the development and sharing of geospatial information, and addresses mission-specific areas such as life saving and damage assessment.

2.4.5 Best Practices

In order to facilitate the quick integration of new ideas, and more importantly, those that are proven to generate results, the ISE must readily identify, communicate, and implement best practices. Identifying and packaging them in a way that allows replication and innovation based on proven concepts is critical. To this end, PM-ISE is developing “Building Blocks of the ISE,” a toolkit that includes the many components of the ISE which work together to facilitate information sharing and protection. This web-based resource will allow ISE mission partners at any level (state, local, tribal, or international) to better understand what makes the ISE function with guidance on how replication is possible in different environments.

Building the Foundation

Six years after passage of IRTPA, some of the most significant barriers to federal, state, local, tribal, and private sector collaboration have been overcome and others are being aggressively addressed by the PM-ISE and mission partners.

- Comprehensive ISE Privacy Guidelines and implementation guidance are in place;
- A comprehensive program for designating, handling, and marking Controlled Unclassified Information (CUI) has been developed and will standardize more than 100 unique markings currently used for Sensitive But Unclassified (SBU) information;
- A solid blueprint for a standards-based ISE, founded on the National Information Exchange Model (NIEM)—ISE Enterprise Architecture Framework—is in place and helps guide federal agency architectures and IT investment planning;
- Common information sharing standards, such as the ISE Functional Standard for Suspicious Activity Reporting (SAR) Version 1.5, documents the rules, conditions, guidelines, and characteristics of business processes, production methods, and products that support information sharing; and
- An Executive Order designed to safeguard and govern access to classified national security information shared by the Federal Government with state, local, tribal, and private-sector entities, has been released.

In addition, much work has been done to improve sharing with state, local, tribal, and territorial (SLTT) governments. The establishment of a national, integrated network of state and major urban area fusion centers permits SLTT governments to: (1) receive classified and unclassified information from federal partners; (2) assess local implications of threat information through the use of a formal risk assessment process; (3) further disseminate threat information to SLTT authorities, and private-sector entities within their jurisdiction; and (4) gather, aggregate, analyze, and share locally-generated information with federal partners as appropriate.

Another significant example is creating the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with criminal activity—and establishes a standardized process whereby that information can be shared among agencies to help detect and prevent terrorism-related criminal activity. The NSI provides an interrelated set of common policies and mission processes which leverage ISE core capabilities and enable fusion centers, as well as the men and women on our nation's counterterrorism front line, to access and share the information they need to keep the country safe.

There has also been significant information sharing improvements by other mission partners. Perhaps the most significant and visible change in terrorism-related information sharing was the establishment of the National Counterterrorism Center (NCTC). Further, the Director of National Intelligence, in partnership with the Intelligence Community (IC) advanced integration of information sharing processes by issuing ground breaking Intelligence Community Directive (ICD) 501—*Discovery and Dissemination or*

Retrieval of Information. This directive promotes responsible information sharing by distinguishing between discovery (obtaining knowledge that information exists) and dissemination or retrieval (obtaining the contents of the information). And finally, the Interagency Threat Assessment and Coordination Group was established to bridge the intelligence information gap between traditional intelligence agencies and state, local, tribal, territorial, and private-sector partners.

3 Improving Information Sharing Activities

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) makes it clear the PM-ISE's responsibilities extend to addressing and facilitating improved information sharing between and among the components of the Intelligence Community (IC), the Department of Defense (DoD), as well as the homeland security and law enforcement communities. In addition, the PM-ISE is required to address

We are improving information sharing and cooperation by linking networks to facilitate Federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate. We are coordinating better with foreign partners to identify, track, limit access to funding, and prevent terrorist travel. Recognizing the inextricable link between domestic and transnational security, we will collaborate bilaterally, regionally, and through international institutions to promote global efforts to prevent terrorist attacks.

— *National Security Strategy*,
May 2010

and facilitate responsible information sharing between federal departments and agencies and state, local and tribal governments; federal departments and agencies and the private sector; and federal departments and agencies and foreign partners and allies. In ensuring responsible information sharing between all of these mission partners, the PM-ISE must also ensure the protection of privacy, civil rights, and civil liberties (P/CR/CL).²⁹

Since Congress called for the creation of the ISE, significant progress has been made to build a broad foundation for information sharing across the Federal Government, as well as with our state, local, and tribal partners and the private sector and international community. This chapter speaks to a wide range of mission partner activities improving information sharing between and among these vital ISE mission partners, encompassing the full range of mission activities.

Although the focus of this Report remains on terrorism-related initiatives, this chapter also describes mission partner activities, some of which may not have been developed explicitly to support counterterrorism (CT), but indirectly support the CT mission, or may ultimately serve as “best practices” with applicability to information sharing and collaboration government-wide, including the ISE.³⁰

²⁹ IRTPA Sec. 1016 (f)(2).

³⁰ The fact that the ISE can leverage these achievements is consistent with one of its key attributes identified in IRTPA—to build upon existing systems capabilities currently in use across the government.

3.1 Suspicious Activity Reporting

The findings in the 9/11 Commission Report³¹ and the Markle Foundation³² clearly demonstrated the need for a nationwide capacity to share information that could detect, prevent or deter a terrorist attack. IRPTA, followed by the 2007 *National Strategy for Information Sharing*, indicates both legislative and executive intent to establish locally controlled, distributed information systems wherein potential terrorism-related information could be contributed by the 18,000 state, local and tribal law enforcement agencies for analysis, to determine if there are any significant emerging patterns or trends. Following this guidance, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) was born.

The NSI is a partnership that establishes a capacity for sharing terrorism-related Suspicious Activity Reports, also known as ISE-SAR. “An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).”³³ The NSI provides analysts, operators and investigators with another tool for “connecting the dots” in combating crime and terrorism, by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR—referred to as the SAR process—in a manner that rigorously protects the privacy and civil liberties of Americans.

The SAR process is critical to preventing crimes, including those associated with domestic and international terrorism. In developing the standards and processes, the NSI leveraged the guidance and expertise provided by GLOBAL which serves as a federal advisory committee and advises the U.S. Attorney General on justice information sharing and integration initiatives. This includes leveraging the National Information Exchange Model (NIEM), which is the backbone of the technology component of the NSI process, as well as privacy guidelines and checklists, to develop a comprehensive program.

NSI in Action

In January 2010, a Los Angeles Police Department (LAPD) line officer who was trained in SAR discovered a store owner who was selling illegal cigarettes, brass knuckles, counterfeit name-brand purses and wallets, and drug paraphernalia. While conducting a search at the store, LAPD officers observed a bomb-making recipe taped to the wall. Subsequently, the store owner was arrested, the recipe was determined to be a viable bomb-making formula, and an investigation into possible terrorism financing is ongoing.

³¹ 9-11 Commission Report, July 2004

³² Nation At Risk: Policy Makers Need Better Information to Protect the Country, 1 March 2009

³³ ISE-SAR Functional Standard v. 1.5, http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf.

3.1.1 Implementation of the NSI – Building on Success

Every day, law enforcement officers observe suspicious activity or receive reports from concerned civilians, private security, and other government agencies about behaviors that could have a potential nexus to terrorism. Until recently, this information was generally stored at the local level and shared within the agency—or, at most, regionally shared—as part of an incident reporting system. Since the standup of the NSI PMO—led by the DOJ, Bureau of Justice Assistance (BJA), and implemented in partnership with the FBI and DHS—the NSI has made substantial progress with standardizing these ad hoc methods of reporting and analysis, and implementing these standards, policies, and processes within the National Network of fusion centers so that timely, relevant information can be shared across federal, state, local, and tribal law enforcement agencies, while also working to ensure that the privacy civil rights, and civil liberties of citizens are protected.

NSI Privacy Framework

The protection of P/CR/CL is paramount to the success of the NSI. Given this importance, the NSI has worked with key partners—including the American Civil Liberties Union and other advocacy groups—to develop protections that, when consolidated, make up the NSI Privacy Framework, which is derived from the protection requirements of the ISE Privacy Guidelines and has elements specific to NSI operations. The NSI requires each site to consider privacy throughout the SAR process by fully adopting the elements within the NSI Privacy Framework prior to NSI participation: development and adoption of a written privacy policy which addresses specific SAR protection requirements; designation of an official for privacy and civil liberties; adhering to the business processes of the ISE-SAR Functional Standard Version 1.5; and providing personnel with information on P/CR/CL protections through the NSI role-based training modules.

“In my twenty-five years of law enforcement experience this was without a doubt the best training session I have ever attended. I left Oklahoma City excited to bring this information back to my agency and get this training to the front line officers. I look forward to participating in the next phases of the InCop training program. I truly believe in this training and believe it is in the best interests of our nation’s safety to have every front line officer in every law enforcement agency trained in the InCop techniques.”

– Sergeant, Jersey City Police Department,
April 2011

In addition, NSI participant sites are strongly encouraged to engage in outreach with privacy, civil liberties, and community-based advocacy groups to foster transparency and trust as well as to obtain feedback and perspective on information sharing initiatives.

NSI Training

The 850,000 uniformed officers in the United States are the foundation for the NSI. To ensure that these officers are properly trained, the NSI PMO takes a multifaceted approach designed to increase the effectiveness of state, local, and tribal law enforcement professionals in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. The overarching goals of the training strategy are to facilitate agency implementation of the SAR process and to enhance a nationwide SAR capability. The NSI

has developed training for front line officers, analysts, and chief executives regarding the behaviors and indicators of terrorism related criminal activity. These training efforts focus on behaviors that have been previously established as potential precursors to criminal acts leading to terrorist activity – the “what,” not the “who.” Training is offered through direct and indirect programs, such as the Memorial Institute for the Prevention of Terrorism’s Information Collection on Patrol (InCop) and Train-the-Trainer (TtT) programs, and online through training videos. Participant feedback on these programs has been very positive. To date, nearly 50,000 officers have received direct, indirect, or on-line training.

NSI training will be enhanced this year to include language about placing a behavior into the NSI Federated Space and eGuardian if, based on their own training, experience, or location (target or critical infrastructure), a participant feels that an observation has a reasonable nexus to a potential terrorism event. In the end, the “totality of the environment” is the defining guidance. Also, leveraging resources and advancing integration, all FBI Joint Terrorism Task Forces (JTTF) personnel will receive full recognition of their own training.

To provide support to front line officers in particular, the NSI PMO, in partnership with the IACP, Major Cities Chiefs Association (MCCA), Major County Sheriffs’ Association (MCSA), National Sheriffs’ Association (NSA), the Association of State Criminal Investigative Agencies (ASCA), and the National Network of fusion centers, is working to deliver a training video for law enforcement and support personnel, training them to recognize those behaviors and incidents that are potentially indicative of criminal activity associated with terrorism. The goal is to have all officers trained by the fall 2011.

Implementation of NSI on America’s Rails

The SAR process has been fully implemented throughout the entire East Coast Amtrak network, which including SAR training for all Amtrak police and rail staff. Commuter rail systems that have implemented most elements of the NSI include: the Maryland Transportation Authority, Southeastern Pennsylvania Transportation Authority, New Jersey Transit, New York/New Jersey Port Authority, Massachusetts Bay Transportation Authority, and the New York Metropolitan Transportation Authority. Elements introduced or in place include staff and police training in behavioral recognition, messaging, SAR reporting, SAR analysis, entry of data into the Shared Space or eGuardian, and implementation of privacy policies that are in compliance with the ISE Privacy Guidelines. The next steps are to complete the East Coast implementation; move on to the national freight rail systems and Midwest Amtrak and Chicago; and begin implementation on the West Coast.

Stakeholder Outreach

The success of the NSI largely depends on the ability of law enforcement to earn and maintain the public’s trust. Therefore, NSI sites are encouraged to engage in outreach to members of the public, including privacy and civil liberties advocacy groups and private-sector partners, to explain how these new tools will be used, while ensuring the protection of citizens’ P/CR/CL. This has resulted in the creation of the Building Communities of Trust (BCOT) initiative, discussed later in this chapter.

Over the past year the NSI PMO has also been coordinating closely with DHS on the “If You See Something, Say Something™” campaign. This campaign—originally implemented by New York City’s Metropolitan Transportation Authority—is a simple and effective program to raise public awareness of the indicators of terrorism, crime, and other threats, and to emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities. Campaigns have been launched over the past several months with the National Football League, the National Collegiate Athletic Association, the Indianapolis 500, the National Basketball Association, the Mall of America, and the Pentagon Force Protection Agency.

DHS is also working to align the efforts of the “If You See Something, Say Something™” campaign with a similar program within the Coast Guard, “America’s Waterway Watch” (AWW). AWW engages public and private stakeholders to be aware of suspicious activity along U.S. ports and waterways and report suspicious activity via a 24x7 hotline, 877-24WATCH. The “If You See Something, Say Something™” campaign and AWW recently developed a joint outreach program for the Washington State Ferry System and are planning on rolling out this joint awareness campaign to include all major ferry systems.



The NSI also recognizes the importance of incorporating the private sector—which owns and operates more than 80 percent of the Critical Infrastructure and Key Resources (CIKR) in our country—and has therefore been working with the DHS Office of Infrastructure Protection (IP) to incorporate the 18 identified sectors into the future NSI process.

Interagency Coordination Bolsters the NSI

DHS IP is providing additional avenues of communication between critical infrastructure owners and operators and the SAR process through the Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE), the primary private-sector component of the ISE. In support of Secretary Napolitano’s “If You See Something, Say Something™” campaign, IP created a standardized format for stakeholders to submit reports. The SAR for Critical Infrastructure tool, currently in the pilot phase for two sectors, will allow stakeholders to share SAR reporting within their sector and with the National Infrastructure Coordinating Center (NICC) through portals on the Homeland Security Information Network-Critical Sectors (HSIN-CS). The NSI PMO’s strategic engagement plan for critical infrastructure highlights and supports expanded availability of the tool for additional sectors upon the completion of this pilot.

Since the inception of the “If You See Something, Say Something™” campaign in July 2010, the NICC Watch has observed a significant increase in SAR reporting. Once a SAR is received from sector partners, the NICC analyzes the information and, if the SAR has a potential

nexus to terrorism, generates a report called a “Patriot Report.” A redacted version of the Patriot Report is shared with cross-sector critical infrastructure stakeholders through HSIN-CS and with the National Operations Center (NOC) Fusion Desk. The NICC Watch also disseminates the full Patriot Report within the Federal Government to include the DHS Office of Intelligence and Analysis (DHS I&A), the NOC-Intelligence Watch and Warning, the FBI, and the NSI.

Enabling Technology

To support the operational mission, the NSI Federated Search facilitates information sharing using NIEM. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations, with data formatted in a semantically consistent manner. NIEM is being used to standardize content (actual data exchange standards), provide tools, and managed processes. By utilizing NIEM, the NSI has made it possible for agencies to search and share terrorism-related SAR across a federated environment.

There are several ways in which NSI participants can make their SAR information available to the NSI Federated Search: by installing an NSI Shared Space Server; by using an existing legacy Computer Aided Dispatch/Record Management System that is in line with NIEM standards; or by creating an eGuardian account. NSI participants can access NSI Federated Search through either RISSNet or LEO, and participants will be able to access the search through Homeland Security Information Network-Law Enforcement (HSIN-LE) sometime in the future.

Standardized Processes

The standardized processes and policies established by the NSI PMO provide federal, state, local, and tribal law enforcement with the capability to share timely, relevant SAR information that has been determined to have a potential nexus to terrorism while ensuring that P/CR/CL are protected. The National Network is a critical part of this connectivity. The NSI PMO has closely coordinated with the State and Local Program Office within DHS I&A, which has the lead for providing support to fusion centers and has also been tasked with providing NSI training and implementing NSI processes within all relevant DHS components. This continued relationship will be critical as the NSI completes the initial implementation and capability of accessing these tools within state and major urban area fusion centers, and moves toward sustainment and utilization of these capabilities.

Focus over the next year will turn to continued implementation within the Federal Government, including all DHS and DOJ law enforcement components, as well as key partners within the private sector and non-traditional homeland security sectors.³⁴

³⁴ DoD is already using eGuardian as discussed later in this chapter

Information from Public Yields Arrest

On 28 October 2010, the FBI Public Access Center Unit received information submitted from an individual, via the Internet, reporting what he or she believed to be threats to the Washington D.C. Metro system. According to the source, the subject indicated, through his Facebook account, his intentions of placing pipe bombs on Metro trains in Washington, DC. The subject also discussed planting bombs in sewers in Georgetown neighborhoods. This information was entered into the FBI Guardian system where a terrorism assessment was initiated. At the same time, the information was pushed down from Guardian to the eGuardian system, ensuring that more than 1,000 eGuardian agency partners were also informed of the threat information.

Upon conclusion of the assessment, on 2 December 2010, the FBI Washington Field Office opened a case to investigate the threats. The investigative efforts resulted in the 14 December 2010 arrest of Awais Younis, a.k.a. Mohhanme Khan, a.k.a. Sundullah Ghilzai for communicating threats via interstate communications. On 14 December 2010, Younis was ordered to undergo a mental evaluation. He was subsequently indicted by a federal grand jury.

On 11 April 2011, Younis pled guilty to conspiring to provide material support to al-Qaida and collecting information for a terrorist attack on a transit facility. Younis' guilty plea was part of a negotiated plea agreement with federal prosecutors, and he apologized in court for his conduct. Younis is a naturalized U.S. citizen from Pakistan, who resided in Northern Virginia. He had conducted video surveillance of DC's Metro rail system and had suggested ways of bombing the Northern Virginia subway stations to inflict the highest number of casualties.

3.1.2 Suspicious Activity Reporting (SAR) Sub-Committee

The SAR Sub-Committee of the ISA IPC focuses on a standardized process in which SAR information can be shared among agencies to help detect and prevent terrorism-related criminal activity. The Sub-Committee is chaired by the DOJ, BJA with additional membership from the FBI, DHS, NSI PMO, PM-ISE, and ODNI.

In the last year, the SAR Subcommittee and the FBI's Joint Terrorism Task Forces (JTTF) worked together to incorporate the eGuardian system with the NSI shared spaces.

The SAR Sub-Committee is responsible for leading the development of strategy, guidance, and policy documents for gathering, analyzing and sharing SAR information; ensuring interagency coordination on related efforts; and resolving interagency issues. In the last year, the SAR Subcommittee and the FBI's JTTFs worked together to incorporate the eGuardian system with the NSI shared spaces. This helps formalize information sharing between state, local, and tribal partners, and leverages the already successful relationships between SLT

partners and the FBI's Joint Terrorism Task Forces. It also streamlines processes and aligns privacy policies among various partners.

In the coming year, the SAR Sub-Committee will focus on several initiatives aimed to further mature the NSI. These efforts include leveraging the Sub-Committee members to identify and improve the use of SAR in intelligence and homeland security threat documents; identifying the scope and requirements for development of an ISE SAR Functional Standard v2.0; creating a roadmap to better align SAR technology solutions; seeking the most efficient training and communications processes; and providing policy recommendations on incorporation of the private sector, including CIKR into the NSI.

3.1.3 Enhancing SAR Analysis

To further strengthen the strategic analysis of SAR data, the DHS SAR Initiative Management Group (DSI MG) is assisting components with engaging the NSI PMO. In addition to sharing their respective SAR with other NSI participants, components are providing an enriched SAR data set that can be leveraged by I&A for the purpose of producing analysis. Some of the products serve as tactical intelligence that assists the decision-making efforts of state, local, tribal and federal law enforcement agencies as they provide protective measures.

SAR Analysis Survey

DHS I&A conducted a survey in April 2011 with the goal of documenting SAR Analysis products that are being produced at the federal as well as the state, local, and tribal (SLT) levels, and recommending areas for future production by the community. The survey has spurred I&A's initiation of a regional analytical working group that will discuss current tradecraft and best practices as they relate to SAR-related intelligence products.

As of May 2011, the FBI, in addition to various offices within DHS, is regularly producing SAR products for use by DHS components, the IC, SLTT law enforcement, and the private-sector. Products range from stand-alone SAR products to routine analytic products that incorporate SAR data.

DOI Establishes Dam Sector Intelligence Working Group to Share and Coordinate SAR

This year, the DOI stood up the Dam Sector Intelligence Working Group to share and coordinate SAR on dams across the United States. The Working Group includes representatives from DHS, the U.S. Army Corps of Engineers, the Tennessee Valley Authority, and DOI. This effort has significantly improved the overall situational awareness regarding the safety and security of dams, some of which are national critical infrastructure. DOI is a member of the National Infrastructure Protection Plan's Sector Partnership as part of the Dams Sector and participates in the information sharing activities of the entire Dams Sector. The Dams Sector, under the CIKR ISE, initiated the first form of a sector-wide SAR process among the critical infrastructure sectors two years ago.

3.1.4 Building Communities of Trust (BCOT)

The BCOT initiative focuses on developing relationships of trust between police departments, fusion centers, and the communities they serve—particularly immigrant and minority communities—to prevent terrorist-related crime and to help keep our communities safe. Under the leadership of the NSI, the BCOT initiative expanded in 2010, with roundtables held in Chicago and Los Angeles. Several more meetings are planned for 2011. The NSI also partnered with the DHS Countering Violent Extremism (CVE) efforts with meetings held in Dearborn, MI and Minneapolis, MN.

In the fall of 2010, the *Guidance for Building Communities of Trust* was released at the International Association of Chiefs of Police (IACP) annual conference in Orlando, Florida. This guidance provides advice and recommendations to law enforcement, fusion center personnel, and the community on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities that appropriately distinguish between innocent cultural behaviors and behaviors that may legitimately reflect criminal enterprise or terrorism precursor activities.

Maritime SAR initiative

The Maritime SAR initiative, led by the National Maritime Intelligence Center (NMIC), aims to establish a process or to leverage NSI's process for maintaining and disseminating all maritime SAR; to work with the global maritime community of interest to populate the NSI Shared Space with maritime-related information to maximize information sharing; and to establish and designate a Federal Maritime SAR entity with analytical responsibilities. This initiative is also aimed at training maritime-related industry employees on SAR reporting. Further, it is imperative that as a nation we ensure that maritime SAR data is brought together for dialog and trending analysis.

3.1.5 Leveraging the SAR Experience

In addition to its successful use in the reporting of suspicious activities, the SAR process and its innovative use of common terminology to describe incidents, its use of NIEM as a methodology for data exchange, and its focus on training to achieve consistency of reporting are potentially scalable to other information sharing processes. In particular, the SAR process and its functional standard is being considered as a repeatable best practice which can be applied to the sharing of cybersecurity incident reporting information, a key element of the Comprehensive National Cybersecurity Initiative.³⁵ Accordingly, the NIEM Program Management Office is developing a NIEM Information Exchange Package Documentation (IEPD) for cybersecurity incident reporting, and PM-ISE is promoting the use of the SAR Functional Standard as a model for collaboration across six centers that are responsible for carrying out U.S. cyber activities.

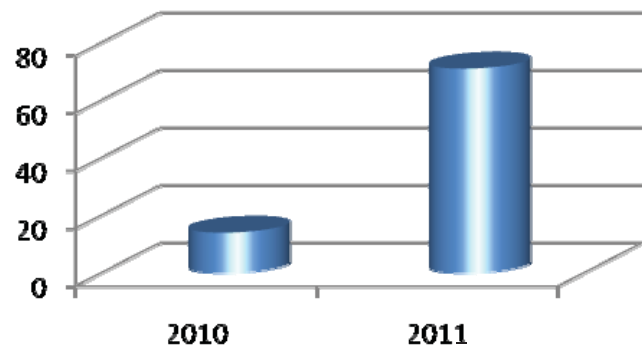
35 <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>

3.2 National Network of Fusion Centers

Fusion centers serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and state, local, tribal, and private-sector (SLTPS) partners. Located in state and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, CIKR protection, and private-sector security personnel to understand local implications of national intelligence, enabling local officials to better protect their communities. Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, and connectivity to federal systems, technology, and grant funding. Since June 2010, DHS has provided the following support to fusion centers:

- In partnership with DOJ, assisted 57 fusion centers with privacy policies, bringing the total number to 71 fusion centers with privacy policies, which represents a 407 percent increase since the last Annual Report (see Figure 8)
- Deployed the Homeland Secure Data Network (HSDN) to an additional 15 fusion centers, bringing the total number to 52 fusion centers with HSDN, which represents a 41 percent increase since the last Annual Report
- Deployed 12 DHS Intelligence Officers to fusion centers, bringing the total number to 70 deployed officers, which represents a 21 percent increase since the last Annual Report
- Granted 1,173 security clearances for state, local, and tribal fusion center personnel
- Delivered security liaison training to 68 fusion center security liaisons
- Deployed the CIKR ISE to five pilot fusion centers to support local and regional critical infrastructure protection

Figure 8. Number of Fusion Centers with Privacy Policies



3.2.1 Fusion Centers and the FBI

In 2010, all 56 FBI field offices conducted self-assessments on their relationship with fusion centers, providing a comprehensive understanding of how the FBI is currently engaged with fusion centers. During this process, the FBI program managers also worked closely with PM-ISE and DHS to evaluate and validate fusion center baseline capabilities and to address areas of common concern discovered during this process.

The FBI continues to assess and develop field office-fusion center engagement based on lessons learned and knowledge gleaned from the assessments, as well as improvements in fusion center capabilities.

The FBI plans to continue close collaboration at both the field office and headquarters levels to standardize processes; clarify procedures; and facilitate more effective engagement with fusion centers. The FBI understands the value of collaboration with other law enforcement entities in maintaining homeland security, and remains committed to strengthening ties at all levels of government.

FBI in Fusion Centers

Currently, 103 FBI personnel are assigned to 59 fusion centers, with 48 embedded full-time in 26 fusion centers and 55 working on a part-time basis in 33 fusion centers. Of these, 32 are Special Agents (SAs) and 71 are Intelligence Analysts (IAs). FBI Net, the FBI's primary network system for the daily investigative and administrative functions of the FBI, is available to 37 fusion centers. The FBI Net presence enables assigned FBI personnel to more fully collaborate with all fusion center personnel since FBI information is at their fingertips. Plans and equipment for FBI Net installation in 15 additional fusion centers is scheduled to commence in 2011 and be completed by fiscal year 2012.

3.2.2 Baseline Capabilities Assessment (BCA)

The most notable interagency effort in support of the National Network in 2010 was the BCA. In September 2010, federal, state, and local officials completed the first nationwide, in-depth assessment of fusion centers to evaluate their capabilities and to establish strategic priorities for Federal Government support. The BCA was designed to evaluate the fusion centers' Critical Operational Capabilities (COC) in an effort to understand the overall maturity of the National Network and to aid fusion centers in reaching their full potential as focal points within the state, local, tribal, and territorial

environment for the receipt, analysis, gathering, and sharing of threat-related information. The BCA also evaluated the fusion centers' capability to protect P/CR/CL, a key enabling capability for the fusion process. On behalf of the DHS, the 2010 BCA was conducted by the PM-ISE, in coordination with Fusion Center Directors, the DHS, the FBI, and other federal interagency partners.

In September 2010, PM-ISE, in coordination with Fusion Center Directors, DHS, FBI and other federal interagency partners, completed a comprehensive assessment of each of the operational fusion centers' capabilities. While the assessment reflected that some fusion centers were more mature than others, efforts are underway to strengthen the capability of the National Network.

In response to DHS Secretary Napolitano's challenge for state and major urban area fusion centers to reach an enhanced level of capability for all four COCs and P/CR/CL protections by 31 December 2010, DHS, in coordination with Fusion Center Directors and interagency partners, developed the COC Gap Mitigation Strategy. This strategy consisted of both short- and long-term activities for mitigating gaps in fusion center capabilities. The short-term approach outlined immediate actions to help fusion centers execute the COCs during situations involving time-sensitive and emerging

threat information. The long-term COC gap mitigation activities will support fusion center efforts to maintain the COCs and P/CR/CL protections. From September 2010 through December 2010, DHS, in coordination with interagency partners, focused its support to state and major urban area fusion centers on the activities identified in the short-term strategy. These activities provided fusion centers with the skills, tools, and resources to support the development and implementation of their plans, policies, and standard operating procedures, enabling the effective execution of the fusion process in situations involving time-sensitive and emerging threat information.

Beginning in January 2011, DHS launched an effort to evaluate both the results of the short-term COC gap mitigation activities and the effectiveness of their support in building fusion center capabilities in line with each COC. As part of this effort, a survey was developed for Fusion Center Directors to help assess each center's progress toward achieving the short-term gap mitigation objectives. To help gauge the Department's support, the survey asked questions regarding the federal assistance to fusion centers. Fusion Center Directors overwhelmingly responded that DHS provided a clear understanding of the intent and expected timeframe associated with the short-term strategy and offered adequate guidance to meet the short-term gap mitigation objectives. A majority of the Directors also agreed that DHS offered adequate resources to meet those objectives. In addition to the survey, DHS also leveraged a variety of other data sources, including the 2010 BCA, official activity after action reports, and data from other federal departments and agencies. Based on the results of this evaluation, fusion centers made progress from September 2010 to December 2010 in building their capabilities and addressing gaps identified in the BCA in each of the four COCs and P/CR/CL protections. Fusion centers continue to build their capabilities in these critical areas. These findings have been captured in the April 2011 COC Short-Term Gap Mitigation Strategy Progress Report.

Fusion Centers in Action

In October 2010, an advisory was sent out by the New York Police Department concerning a suspicious tractor-trailer whose driver reportedly diverted its route to Times Square in New York City in exchange for \$10,000. The deployed DHS Intelligence Officer (IO) in New York informed several fusion centers in the affected area. Subsequently, the Rhode Island Fusion Center discovered that the original owner of the truck was a California native and requested a background check from the Northern California Regional Intelligence Center. Within two hours of the advisory's release, information from these two fusion centers was used to coordinate with the Connecticut Intelligence Center, which assisted the Connecticut State Police in locating the vehicle before it reached its reported target. Ultimately, officials concluded that there was no threat, but the fact that these fusion centers, supported by the DHS IO, were able to resolve this SAR in a matter of three hours demonstrates the value of the National Network.

* * *

The Arizona Counter Terrorism Information Center supported a five-month investigation led by a tribal partner, the Tohono O’odham Nation (TON) Police Department and the Bureau of Indian Affairs (BIA) Division of Drug Enforcement. This investigation led to the arrest of 10 suspects and the apprehension of weapons, cash, vehicles, cocaine, marijuana, and Ecstasy—the largest drug enforcement operation in TON history. The investigation marked a key opportunity to collaborate with tribal partners and opened information sharing initiatives between several other agencies, including the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and other police departments in the area.

* * *

In the fall of 2010, the FBI’s Western Regional Intelligence Group and Sacramento Field Intelligence Group began collaborating with the California State Threat Assessment Center on threats to the Southwest Border. As a result of this federal and state partnership, in April 2011, the Center released their first detailed assessment on widespread criminal effects of Mexico’s drug war. This product drew accolades from the Los Angeles Police Department, the DHS, and state executives from Texas and California. Due to this partnership with the FBI, collaboration has increased throughout the state of California.

3.2.3 Fusion Center Sub-Committee

The Fusion Center Sub-Committee of the ISA IPC focuses on coordinating federal support to fusion centers by providing the guidance and standards necessary to support interconnectivity to help ensure information sharing between and among fusion centers and all levels of government. The Sub-Committee is chaired by DHS and the FBI, and includes members from DoD, the Joint Staff, DOJ, ODNI, PM-ISE, and the White House Office of National Drug Control Policy (ONDCP). The Fusion Center Sub-Committee advises and supports the ISA IPC by:

- Recommending priorities for federal support to fusion centers;
- Developing strategies for strengthening and maturing the National Network;
- Preparing guidance and policy on fusion center-related activities;
- Providing a forum for sharing best practices, lessons learned, and resolving interagency issues; and
- Serving as a resource to SLTTPS partners for the sharing of homeland security, terrorism, and law enforcement information.

The Fusion Center Sub-Committee is facilitating a number of near- and mid-term projects intended to mature the National Network including the development and implementation of a Federal Resource Allocation Criteria Policy; a common operational and sustainment cost reporting system; and a repeatable BCA and gap mitigation process.

3.2.4 Federal Resource Allocation Criteria (RAC)

One of the Federal Government's first priorities for coordinating support to fusion centers was to clearly define the parameters for the allocation of federal resources to fusion centers. The Fusion Center Sub-Committee developed the Federal Resource Allocation Criteria (RAC) policy, which was formally issued in June 2011. This policy defines objective criteria and a coordinated approach for prioritizing the allocation of federal resources to fusion centers. The goal of this policy is to enhance the effectiveness of federal support to the National Network and strengthen support to fusion centers to execute the statewide fusion process.

Recognizing that while the Federal Government does not dictate where fusion centers should be built and maintained, it does have a shared responsibility with state and local governments to promote the establishment of a National Network to facilitate effective information sharing. Since 2001, the Federal Government has provided significant grant funding, training, technical assistance, exercise support, federal personnel, and access to federal information and networks to support fusion centers.



In the face of increasing demands and limited resources, the prioritized resource allocation established through the criteria in the RAC policy will enable the Federal Government to concentrate resources in a manner that will improve the efficiency of its support to fusion centers. The implementation of the RAC policy will enable fusion centers to mature their capabilities in order to effectively execute the statewide fusion process and fulfill their roles in the ISE.

The RAC policy is intended to guide the allocation of federal resources to fusion centers in a manner that:

- Collectively supports the development of a National Network;
- Effectively balances the need for supporting SLT as well as federal imperatives; and
- Ensures efficient information sharing across federal and SLT partners.

Implementing the RAC policy will help bring consistency and transparency to the process of prioritizing the allocation of federal resources to fusion centers. It is a key first step in establishing coordinated, long-term sustainment of the National Network.

The New York State Intelligence Center's Vigilance Project

The New York State's fusion center—the New York State Intelligence Center (NYSIC)—recently published a report titled, *The Vigilance Project: An Analysis of 32 Terrorism Cases Against the Homeland*. This report identifies trends and themes among 32 terrorism cases in the United States that have been investigated since 11 September 2001. The Center plans to regularly update the product with new terrorism investigation case information, so that it may be shared with law enforcement personnel to support their efforts in identifying patterns and trends that may be indicative of criminal or terrorist activity. The product

identifies 25 variables for analysis when looking for trends among the terrorism cases, including demographics of individuals, plot targets, and tactics. According to the report, "The variables selected for analysis best capture potential indicators of terrorist activity." Fusion center staff can use this tool to enhance their efforts in detecting and preventing terrorist activities by maintaining awareness of the trends noted in this product. It is also meant to provide law enforcement officers in the field with a greater ability to recognize and report suspicious activity and keep them engaged in the fight against terrorism.

3.2.5 Fusion Center – High Intensity Drug Trafficking Area (HIDTA) Partnership

On 10 February 2011, approximately 30 representatives from federal, state, and local agencies—including HIDTAs, fusion centers, DHS, ONDCP, DOJ, the FBI, the National Drug Intelligence Center (NDIC), and PM-ISE—met in Atlanta to explore how best to leverage fusion centers and HIDTAs as uniquely valuable resources and partners for its customers and participating entities. This session was a part of the Fusion Center Sub-Committee's effort to establish stronger partnerships between HIDTAs and fusion centers, and to further define the operational roles, responsibilities, and relationships among these unique yet complementary intelligence and information sharing entities.

The significant breadth of expertise and the cumulative years of experience represented at this meeting produced an incredibly valuable discussion. Throughout the session, several key themes continued to emerge:

- When done properly, the collocation and/or integration of fusion centers and HIDTA Investigative Support Centers into a unified command structure may bring significant benefits; but this should not be advocated as a universal approach.
- Directors do not generally view each other as competing for mission space as they do for quality resources, e.g. well-trained analysts; but mission drift can potentially dilute the unique value of each program.
- There is a need to continually reeducate and revalidate with customers, i.e. police chiefs and sheriffs, the value and respective capabilities available to their agencies through BOTH fusion centers and HIDTAs.
- Formalized requirements and collection processes would enable fusion centers to convey what to look for, but would also provide a process for better understanding what line officers are seeing, and feeding the NSI, as well as ultimately benefiting HIDTA investigations.
- Enhanced concepts of operation and commonly understood terminology (e.g. national security vs. criminal intelligence and threat vs. target) are necessary to help clear the uncertainty in the delineation between HIDTA and fusion center missions among both leadership and customers, as well as those working within the respective entities.

This meeting underscored the importance of the role of the National Network to the greater national security enterprise, as well as the need to ensure appropriate operational relationships with existing entities such as the HIDTAs.

In addition to the meeting in Atlanta, a panel at the National Fusion Center Conference (NFCC), entitled *Promoting Stronger Partnerships with Fusion Centers*, highlighted ongoing efforts to strengthen relationships between fusion centers and major cities intelligence units, as well as fusion centers and HIDTAs. Building upon the meeting in Atlanta, the objectives of this panel were to further discuss the common obstacles and key enablers to effective coordination and communication among fusion centers and stakeholders; to learn about best practices currently being implemented throughout the network to address information sharing challenges, and to discuss tools and resources to assist fusion centers with building more effective partnerships with their customers and partners.

As a result of discussions at the NFCC, these partners will continue to build and formalize relationships within their states through business processes and concepts of operation, and to enhance intrastate coordination and execution of the statewide fusion process. Both fusion center and HIDTA directors are essential partners in leading these efforts.

3.2.6 Improving Information Sharing On Threats to the Southwest Border

On 27 April 2011, DHS hosted the “2011 Southwest Border Law Enforcement Intelligence and Information Sharing” meeting for more than 100 local, state, and federal law enforcement and IC participants at the El Paso Intelligence Center. The purpose of the meeting was to bring Southwest Border security stakeholders together to examine ways to improve information sharing on threats to our Southwest Border.

The meeting focused on perceptions of the threats along the Southwest Border, intelligence needs to combat those threats, information sharing challenges, and information holdings which might be useful to a broader group. This meeting recognized that state and local authorities require more focused and timely analysis from their federal partners and need better collaboration with federal, state, and local authorities, as well as with the HIDTAs and fusion centers. It was also noted that increased HIDTA and fusion center collaboration will support efforts to meet state and local information sharing needs and to avoid duplication of efforts.

3.2.7 Major City Chiefs Intelligence Unit Commanders Group

Over the past year, DHS hosted a series of regular meetings with the Major City Chiefs Intelligence Unit Commanders Group. These meetings provided an opportunity to improve information sharing efforts among these stakeholders, discuss existing information sharing challenges, and examine and identify agency-specific information needs. These meetings also provided an opportunity to discuss best practices, lessons learned, and opportunities to further enhance the operational roles and relationships between major city intelligence units and fusion centers.

3.2.8 National Fusion Center Conference (NFCC)

In March 2011, nearly 1,000 federal, state, local, tribal and territorial fusion center stakeholders attended the fifth annual NFCC in Denver, Colorado. The conference served as a forum for fusion center stakeholders to discuss key policy issues and receive training, technical assistance, and other support to achieve a baseline level of capability through a series of plenary and breakout sessions. Attendees included Fusion Center Directors, state Homeland Security Advisors, fusion center analysts, and homeland security and law enforcement professionals representing all levels of government. This annual

conference also informs and advances the efforts of the Fusion Center Sub-Committee, providing a vital feedback loop to the directors, and an opportunity to engage them in preparing future work plans. In Denver, fusion center personnel and federal partners collectively identified priorities for the upcoming year to enhance the national network:

- Reaffirm the four COCs;
- Continue to use partnerships to advocate for fusion center sustainment;
- Strengthen statewide fusion process activities; and
- Engage in performance management efforts

National Terrorism Advisory System (NTAS)

The NTAS went live on 26 April 2011.³⁶ Under the new, two-tiered system, DHS will coordinate with other federal entities to issue formal, detailed alerts regarding information about a specific or credible terrorist threat. Each of these alerts will include a clear statement that there is an “imminent threat” or “elevated threat.” Each alert will also provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals and communities can take.

Depending on the nature of the threat, the alert may be sent to a limited, particular audience like law enforcement, or a segment of the private sector, like shopping malls or hotels. Or the alert may be issued more broadly to the American people distributed—through a statement from DHS—to the news media as well as via the DHS website and social media channels such as Facebook, Twitter and blogs.

A key component of the new NTAS process is that it incorporates points of contact from across the Federal Government, state and local representatives, and the public sector, as applicable, to coordinate input prior to issuing the NTAS alert. This process will ensure that NTAS alerts are tailored for a specific sector, including components of the Federal Government; state, local, and tribal entities; critical infrastructure entities; and selected private-sector partners, as needed, to facilitate appropriate action. In addition, all NTAS alerts require a set duration date, so that information can be re-evaluated on a regular basis.

NTAS was developed in that same collaborative spirit: it was largely the work of a bi-partisan task force that included law enforcement, former mayors and governors, and members of the previous Administration.

³⁶ Presidential Policy Directive – 7, National Terrorism Advisory System (NTAS), directed the Secretary of Homeland Security to establish the NTAS as a refinement to the Homeland Security Advisory System.

3.3 Interagency Threat Assessment and Coordination Group (ITACG)

The end-state goal of the ITACG is improved information sharing between federal and state, local, tribal, territorial, and private-sector partners to help deter and prevent terrorist attacks. To achieve this goal, the ITACG Detail, housed at the NCTC, assists analysts in integrating, analyzing, and otherwise preparing versions of intelligence products, derived from information within the scope of the ISE, that are either unclassified or classified at the lowest possible level and suitable for dissemination to these mission partners. The ITACG Detail is directed by a senior intelligence official appointed by the DHS. A deputy director is appointed by the FBI. ITACG detailees, who are representatives of state, local and tribal homeland security, law enforcement, fire, and health agencies, serve on a one-year fellowship sponsored by the DHS. PM-ISE is responsible for monitoring and reporting on the efficacy of the ITACG.^{37,38}

3.3.1 Assessment of the Detail's Access to Information

The Congress has recently expressed interest in knowing whether ITACG detailees have access to the information they need, within the scope of the ISE, at the NCTC to accomplish their mission.³⁹ In December 2010, the ITACG Detail was realigned under NCTC's Deputy Director for Operations Support (DD/OS). Based on interviews with NCTC leadership and ITACG personnel, this realignment served to improve detailees' access to information by exposing them to the main stream of intelligence at NCTC. According to the DD/OS, the detailees have more than adequate access to information at NCTC for what they are expected to do.

A significant indicator of the ITACG detailees' access to information is their involvement with a special site exploitation effort currently ongoing at NCTC. From the outset, the detailees were brought in "front and center" for the primary purpose of determining what is important to SLTPS consumers for classified and unclassified "tearline" products.⁴⁰ According to the DD/OS, the decision to involve the detailees was easy—"no one even had to think about it." The ITACG Detail is integrated into NCTC operations and their involvement with the special site exploitation effort is evidence of both their access to information at NCTC, and their centrality to the effort to produce relevant information for SLTPS partners. ITACG Detailee Lieutenant Sam McGhee, from the Aurora (Colorado) Police Department, summarized it best by stating, "In my 30

"In my 30 year tenure as a law enforcement officer, I never would have thought I would have this level of access. It's a testament to the commitment in improving information flow to prevent something bad from happening again."

– ITACG Detailee Lieutenant
Sam McGhee, Aurora Police
Department (Colorado)

37 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, sec. 210D(c), codified as amended at 6 U.S.C. 124k(c).

38 The last report was dated November 2010, and can be found at: www.ise.gov. Future reporting on the ITACG will be included in PM-ISE's Annual Report to the Congress on the State of the ISE.

39 Reducing Over-Classification Act, Pub. L. No. 111-258, 124 Stat. 2648, sec. 5(c).

40 Portion of an intelligence report which has been cleared for disclosure or release.

year tenure as a law enforcement officer, I never would have thought I would have this level of access. It's a testament to the commitment in improving information flow to prevent something bad from happening again."

While all detailees are faced with a steep learning curve initially, they become quickly acclimated and gain a deep appreciation of how much information is available to them. According to one detailee, "access is not an issue—it's more than adequate. The real challenge is how to manage the deluge of information, and use it in a manner that makes a difference." The permanent federal intelligence analysts assigned to the ITACG—by the FBI, NCTC, and DHS—are key to the ITACG detailees' success. These analysts provide the detailees with on-the-job training, assistance in performing their day-to-day activities—including conducting intelligence-related activities—and help in preparing and delivering presentations.

3.3.2 ITACG Involvement in Intelligence Production

Since June 2010, the ITACG Detail reviewed 128 draft intelligence products and 254 daily summaries in support of SLTTPS partners. In addition, the Detail authored, co-authored, or recommended the production of 27 Roll Call Release products—a collaborative DHS, FBI, and ITACG product line—intended for "street-level" first responders.

"NYPD and FDNY find the Roll Call Releases to be extremely useful...it's just what the doctor ordered. The bullet point format is ideal for police officers and firefighters who must retain a great deal of information which is necessary to help them protect their own lives and the lives of others, and which makes them alert to questionable activities that they may witness in a given situation."
– NYPD Representative

Another critical function of the ITACG Detail is to identify intelligence products that should be downgraded in classification, for release to SLTTPS partners. Since June 2010, the ITACG Detail has requested 64 product downgrades of which 39 have been approved and disseminated.

3.3.3 ITACG Performance

Since March 2010, DHS I&A solicited a customer feedback survey on every intelligence product it released, including products the ITACG is involved in producing. While this feedback is not necessarily a *direct* reflection on ITACG's performance, since the ITACG *is not responsible for* DHS I&A intelligence production, the surveys provide insight into how customers use products ITACG is involved with, to include a rating on how relevant the product is to their missions.⁴¹

State and local survey feedback during the period March 2010 to March 2011 was positive. Approximately 80 percent of the respondents rated the intelligence products as either "very important" or "critical" to their mission. In addition, DHS I&A tracks product

⁴¹ DHS I&A also submits an annual report to the Congress on voluntary feedback on DHS intelligence or other information products, as required by Section 210A9(g) of the Homeland Security Act of 2002, as amended. The third annual report was submitted in November 2010.

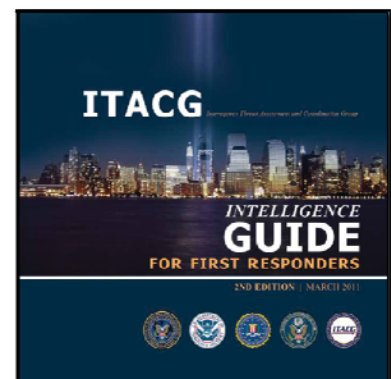
utilization and found nearly 99 percent of its products are either integrated into state and local finished intelligence products; shared with federal, state, local, and private-sector partners; or used for situational awareness, security preparations, or training purposes.

Another indicator of ITACG's performance is reflected in the feedback gathered from state and major urban area fusion centers. During the Fusion Center BCA, fusion center directors were asked to comment on the utility of federally-produced intelligence. The majority of the directors noted distinct improvements in the intelligence products provided to them, especially over the past year. They indicated that intelligence reporting has become more frequent, more relevant, and more concise, and attributed these improvements to the leaderships' focus on improving intelligence dissemination. They specifically indicated that joint-seal DHS I&A and FBI products, including Roll Call Releases, contribute significantly to their ability to fulfill their missions.

3.3.4 Intelligence Guide for First Responders, 2nd Edition

The first edition of the *Intelligence Guide for First Responders* was published in October 2009. Seventy-five thousand copies of the guide were mailed to more than 16,000 police departments and more than 32,000 fire departments across the country, including to Hawaii, Guam, Puerto Rico, and the Virgin Islands. The state and local response to the Guide has been overwhelmingly positive, and based on continued requests for additional copies, the ITACG has requested to print an additional 50,000 copies.

The 2nd edition of the *Intelligence Guide for First Responders* incorporates feedback from the field, and includes two new sections—"Reporting Suspicious Activity," which covers participation in the NSI, and "Joint Partnerships," which highlights several joint federal, state, local, and tribal activities around the country. This edition has been sent to the fusion centers and the JTTFs for further dissemination to state, local, and tribal partners. The guide is also posted to ise.gov, nctc.gov, leo.gov, and all HSIN portals.



3.3.5 Guide for Public Safety Personnel

In addition to the First Responders Guide, ITACG, in collaboration with DHS, DOJ, the FBI, and NCTC, has produced the *Countering Terrorism: ITACG's Guide for Public Safety Personnel*. This reference guide is designed to assist first responders in recognizing activities or conditions that may be indicative of potential terrorist activity. The Guide focuses on three key areas: Indications and Warning; Tactics and Targets; and Chemical, Biological, Radiological, Nuclear, and Explosive threats. ITACG is producing 250,000 copies of this Guide for dissemination to fusion centers and JTTFs, for further dissemination to state, local and tribal mission partner.

3.3.6 Federal Community Orientation Program

A critical function of ITACG is educating and advising intelligence analysts about the needs of SLT homeland security and law enforcement officers, and other emergency response providers. Last year, ITACG instituted the Federal Community Orientation Program to facilitate direct interaction with IC member agencies in the Washington, DC region. During each site visit, ITACG personnel explain the

ITACG mission, receive briefings about the host agency's mission, and tour the components' operations centers. To date, ITACG detailees visited the Terrorist Screening Center, the Transportation Security Operations Center, the National Security Agency, and the Open Source Center.

3.4 Tribal Information Sharing

3.4.1 Information Sharing Implications of the Tribal Law & Order Act (TLOA)

On 29 July 2010, President Obama signed into law the TLOA.⁴² The TLOA establishes accountability measures for the federal agencies responsible for investigating and prosecuting reservation crime, and provides Indian tribes with additional tools to combat crime locally. Specifically, the TLOA strengthens tribal law enforcement agencies' criminal intelligence information sharing capabilities by permitting federally-recognized Indian tribes to access national criminal information databases for the purpose of either entering information into these databases or obtaining information from these databases.

Indian Country covers an expansive area of the United States; nearly 56.2 million acres, encompassing ports and spanning international borders. For example, the Chippewa Tribal Nation is located at the port of Sault Ste Marie, Michigan—a key point where cargo passes into the United States from Canada—and the Tohono O'odham Indian Reservation includes 75 miles of the U.S. Southwest Border. Tribal governments counter threats to homeland security, alongside their federal, state, and local counterparts, every day. Gaps in information sharing with tribal partners could result in either criminal and/or violent extremist activity going undetected. According to the DOJ's National Drug Intelligence Center, most illicit drugs available in the United States and thousands of illegal immigrants are smuggled into the United States across the Southwest Border. Of some concern to law enforcement officials is the potential for cross-border drug smuggling routes to be used to move terrorists or weapons of mass destruction (WMD) into the United States.⁴³ Therefore, seamless information sharing between federal, SLT, and international partners is necessary to address smuggling and to combat transnational threats.

3.4.2 Building the Community

This past year PM-ISE dedicated efforts toward building a community to increase cooperation between federal and SLT law enforcement agencies. Increasing Indian Country representation in the ISE required focused outreach efforts, including outreach to:

- DHS I&A
- Fusion centers
- NSI PMO
- FBI Criminal Justice Information Services (CJIS)

⁴² Public Law 111-211

⁴³ U.S. Southwest Border Smuggling and Violence, National Drug Threat Assessment 2010, February 2010, available at: <http://www.justice.gov/ndic/pubs38/38661/swb.htm>

- FBI Indian Country Unit
- DOI Bureau of Indian Affairs
- National Law Enforcement Telecommunications System (Nlets)
- International Association of Chiefs of Police (Indian Country Section, Intelligence-Led Community Policing, and Victim Services)
- Michigan Tribal Chiefs Association
- California Tribal Police Chiefs Association

3.4.3 Providing Access to all Tribal Front Line Officers

The National Law Enforcement Telecommunications System (Nlets) links together and supports every state, local, and federal law enforcement, justice and public safety agency for the purposes of sharing and exchanging critical information. Because tribes are sovereign nations, each tribe interacts with state, local, and federal law enforcement in different ways. Tribes in some states, for example, have comprehensive law enforcement agencies that can access Nlets through their state-owned systems. However, the majority of tribes with law enforcement organizations have less sophisticated systems that limit their access to the state systems. The sharing of information between law enforcement and tribes is essential to ensure that state, local, and tribal law enforcement officers approach vehicles with all the information necessary for a safe traffic stop. Recently, the Nlets Program Management Office asked PM-ISE to assist in improving Nlets access for tribal law enforcement organizations. PM-ISE reached out to Indian Country, expanded their knowledge of Nlets benefits, and established the first ever connectivity pilot with four tribes in separate regions of the United States.



KOMOnews.com

3.4.4 Tribal Integration with NSI and Fusion Centers

The Tribes have used SAR-like approaches for many years, particularly those that have gaming facilities. PM-ISE has partnered with the NSI PMO to administer the NSI Line Officer Training to all Tribal law enforcement agencies, as an attempt to further integrate Indian Country into the NSI. As a result of this initiative, NSI PMO has mailed NSI training materials to 172 out of approximately 200 tribal law enforcement agencies.

Fusion centers are also expanding their participation with Indian Country. PM-ISE, in coordination with federal partners and various state authorities, is supporting the integration of tribal law enforcement personnel in fusion centers. Successful examples of these efforts have occurred in Oklahoma, Arizona, and Washington State. Tribal presence in fusion centers is most often realized through their participation in liaison programs, serving as liaison officers, or as embedded analysts. These programs allow the fusion centers to support robust information sharing on lands that are under the complete control of tribal governments, giving a full threat picture of the region.

3.4.5 FBI and Tribal Integration

The FBI is responsible for developing and implementing strategies to address the most egregious crime problems in Indian Country where the FBI has responsibility, as well as supporting joint investigative efforts with the Bureau of Indian Affairs-Office of Justice Services (BIA-OJS), tribal law enforcement, and Safe Trails Task Force (STTF) personnel.

The FBI has approximately 105 Special Agents working in support of Indian Country investigations. Criminal jurisdiction in Indian Country is a complex maze of tribal, federal, and state jurisdictions. The FBI has investigative responsibility for approximately 200 Indian Reservations out of the 565 federally-recognized Indian Tribes in the United States. The FBI initiated and leads the STTF, program which is designed to unite federal and SLT law enforcement agencies to combat crime and enhance information sharing practices in Indian Country. There are 19 active FBI-led STTFs in the United States.

3.5 Multimodal Information Sharing

Building on a strong foundation of information sharing between and among federal, state, local, and tribal governments as well as international and private-sector partners, ISE mission partners are pursuing information sharing initiatives aimed at protecting and reducing vulnerabilities at our borders, ports, and airports, and to enhance overall air, maritime, and transportation security, consistent with the National Security Strategy. PM-ISE supports multiple aspects of information sharing in the air and maritime domains, primarily to promote cross domain information integration, and is also participating in efforts to develop core concepts for the *National Strategy for Global Supply Chain Security*.⁴⁴

Air Domain Awareness Initiative

The Department of Transportation (DOT), in coordination with the Federal Aviation Administration (FAA), played a leadership role in the Information Sharing Working Group within DHS's ongoing Air Domain Awareness (ADA) initiative. The initiative was begun to develop an integrated, 'whole of government' approach to ADA, with the ultimate goal of fusing intelligence, surveillance data, and analysis across federal, state, local, and tribal governments, as well as private entities and foreign partners with aviation safety and security responsibilities. Throughout this past year, the Information Sharing Working Group established a Sub-Committee focused on identifying and offering solutions to existing information sharing barriers, and coordinated with DHS to stand up a collaborative online ADA information sharing portal for the ADA community of interest.

⁴⁴ This strategy, and the subsequent National Action Plan for Global Supply Chain Security, will provide the framework to better secure the global supply chain and identify opportunities to improve the sharing of threat information as it relates to intermodal cargo transport.

3.5.1 Information Sharing in the Air Domain

In response to the need for a whole of government approach to achieving Air Domain Awareness (ADA), stakeholders participated in a series of ADA Summits that provided the impetus for development of a governance structure to provide direction and oversight for ADA implementation. From these summits, the concept for an ADA Board emerged, along with four working groups: the Information Sharing Working Group; the Capabilities and Resources Working Group; the Policy, Guidance, and Governance Working Group; and the Air Surveillance Working Group. The ADA Board will coordinate interagency activities and leverage the National Security Staff Transborder Security Interagency Policy Committee (IPC) when required.

In January 2011, the Next Generation Air Transportation System (NextGen) Joint Planning and Development Office (JPDO) kicked off an effort to develop a Concept of Operations (CONOPS) for the Integrated Surveillance Initiative. The goal of this effort is to provide multi-agency integrated aviation surveillance capabilities by 2016. The CONOPS includes cross-community sharing of pre-flight information, enhanced information sharing and situational awareness, and automated sharing of in-flight updates and changes to flight characteristics. The planning and creation of the Integrated Surveillance Initiative will facilitate the use and reuse of data from the entire aviation community of interest, saving time, money, and efficiencies.

PM-ISE is supporting these air domain initiatives by actively participating at the ADA Summits and in the working groups; by providing technical assistance in their development of information sharing architectures; and by sharing ISE best practices and tools to promote information sharing in the air domain.

The DoD Civil Aviation Intelligence Analysis Center (CAIAC)

In July 2010, the Under Secretary of Defense for Intelligence designated the Department of the Air Force as the lead DoD intelligence representative for the civil aviation intelligence mission, to establish the DoD CAIAC. This new Center, which is expected to reach Full Operating Capability in FY 2013, will serve as a Department-level shared resource that brings in-depth knowledge and expertise of the global commercial aviation industry to the nation's most challenging intelligence problems. The CAIAC will also provide a critical link in an emerging coordinated interagency approach to Air Domain Awareness.

3.5.2 Information Sharing in the Maritime Domain

The National Maritime Intelligence Center (NMIC) and PM-ISE are analyzing opportunities to improve information sharing between federal and SLTPS entities in the maritime domain. Currently several port-based, cross-governmental programs and initiatives exist to monitor and track vessel, cargo, and passenger data. The standardized sharing of vessel, cargo, and passenger data would maximize situational awareness and emergency response across transportation domains. Some of the agencies and offices that can contribute to dissemination methods, such as a common or user-defined operating picture, shared space, or dashboard, include the DOT's MARVIEW, the Coast Guard's Interagency

Operations Centers, Navy Maritime Operations Centers, JTTFs, port authorities, and state, county, tribal, and municipal law enforcement and safety offices.

The U.S. Customs and Border Protection (CBP), U.S. Coast Guard (USCG), and Immigration and Customs Enforcement (ICE) components of DHS are engaged in the Joint Targeting Architecture Project to improve information sharing relating to maritime targeting protocols and procedures, since all three agencies have distinct authorities to protect the United States against persons, cargo, and other dangers in the seaports. In addition, in March 2011, DHS held an Executive Summit for the DHS Small Vessel Security Implementation Plan Report to the Public. This included stakeholders from the private sector, USCG, CBP, and other federal and SLT authorities.

To increase Maritime Domain Awareness (MDA), the National MDA Coordination Office approved the MDA Interagency Solutions Analysis to identify and prioritize interagency MDA capability gaps and to identify collaborative interagency solutions to address and mitigate those gaps.⁴⁵ The Office has also asked the DoD Executive Agent for MDA to develop a national architecture for sharing unclassified MDA information. This funded effort is tasked with improving the real-time sharing of data regarding vessel arrivals, vessel tracking, and related U.S. threat response activity. PM-ISE is providing planning, technical, and governance support to this whole of government initiative.

Additionally, on the MDA Information Portal—www.mda.gov—the “Maritime Domain Awareness Information Exchange” has been implemented and designed to provide a collaborative environment where members of the maritime community of interest can learn and share information that will enhance and improve situational awareness within the maritime domain.

Maritime Safety and Security Information System

The Maritime Safety and Security Information System is a multilateral non-classified data-sharing system to improve the MDA of the United States and its allies and partners through the sharing of Automatic Identification System data through an Internet-based system. This initiative has obtained international acceptance as a standard for the exchange of maritime data and has become a maritime data sharing system of choice by more than 60 nations.

Multimodal Information Sharing Taskforce (MIST)

The MIST is an interagency research effort designed to foster collaboration and capture best practices in information sharing in a regional port environment. MIST creates a structure for collaborative problem solving that focuses on uncovering unique local issues and communicating these to national policy makers. The fourth MIST workshop, held in Philadelphia in September 2010, provided a venue for private-sector input into the development of information sharing processes. MIST findings show that industry-government collaboration is improved by providing financial and social incentives to industry; by improving two-way communication; by addressing issues with interagency collaboration; and by increasing cultural awareness. MIST also surfaced a number of best practices for collaboration, including

⁴⁵ These issues were captured in the MDA Interagency Solutions Analysis 1.0 Report, 31 January 2011.

the U.S. Customs Trade Partnership Against Terrorism program, the expansion of industry-run education programs for government employees, and the inclusion of industry in emergency preparedness activities and Integrated Operations Centers.

The Maritime Exchange

To promote and protect maritime commerce for the Delaware River maritime community, the Maritime Exchange⁴⁶ developed and operates the electronic information center for ship and cargo processing in the Delaware River and Bay. Maritime On-Line provides comprehensive web-based services to fulfill a variety of commercial, security, and safety-related maritime needs. The system includes ship schedules, navigational safety information, electronic cargo and vessel clearances through multiple federal agencies, notice of arrival/departure, real-time position information, and crew list reporting. Developed under the specific direction of the members of the maritime business community and the federal and state government agencies that regulate them, Maritime On-Line is the one-stop information source for Delaware River and Bay international commerce activity. Live data feeds are also provided, in real-time, to the Pennsylvania Criminal Intelligence Center. There, analysts review data and collaborate on tactical operations in concert with federal, state, and local partners.

3.6 WMD Information Sharing

As introduced in the 2010 ISE Annual Report, PM-ISE supported DHS's Domestic Nuclear Detection Office (DNDO) by funding the initiation of their inter-governmental information sharing exchange. This mechanism will facilitate and standardize the real-time sharing of radiological and nuclear alarm adjudication data, shipment and licensee data, and will improve analysis of post-seizure data.

In July 2011, DNDO, with the cooperation of DHS/CBP, Defense Threat Reduction Agency (DTRA), and state and local representatives in Los Angeles and Kansas City will demonstrate the real-time information exchange of radiological/nuclear alarm adjudication data derived from the screening, scanning, or inspection of transient cargo. Participants committed to this live exchange include: LAPD, LA County Sheriff, LAFD, LA County Fire, Long Beach Fire Department, federal entities (DNDO, CBP, DTRA), and the Kansas City Terrorism Early Warning Center. This effort is included in DHS's Information Sharing Governance Board for executive sponsorship, oversight, and intra-departmental support.

⁴⁶ The Maritime Exchange for the Delaware River and Bay is a non-profit trade association which serves as "the voice of the port" for the Delaware River maritime community.

3.6.1 Securing the Cities (STC)

STC was launched in July 2006 as way to protect a high-risk urban area, such as the New York City (NYC) region, from a potential radiological or nuclear attack. The initial emphasis was on building a regional enterprise architecture for the NYC region that will allow real-time sharing of data from fixed, mobile, maritime, and human portable radiation detection systems. The NYC program is entering into a new phase where a greater emphasis will be placed on integration of state and local Preventive Radiological Nuclear Detection (PRND) capabilities into federal operations. In addition, the President's FY 2012 budget has called for the expansion of STC into one additional Urban Areas Security Initiative region.

3.6.2 West Coast Maritime Pilot

The West Coast Maritime Pilot was intended to assess capabilities that reduce vulnerabilities from nuclear and radiological weapons and materials delivered via small vessels across maritime borders. DNDI provided technical assistance to local authorities in the Puget Sound and San Diego areas to develop a nuclear detection architecture that reduces high-consequence maritime vulnerabilities. The pilot, which began in 2007, involved four phases: 1) collect information on existing maritime PRND capabilities in each port area; 2) design an enhanced maritime PRND architecture including development of response protocols; 3) deploy capability, including training and equipment; and 4) assess and document each pilot. The pilot training evolutions, exercises, and drills successfully concluded in 2010, and a final report was released in February 2011.

3.7 Intelligence Community (IC) Intelligence Sharing Services

A variety of IC intelligence sharing services provide analysts , operators, and investigators with on-demand electronic dissemination applications to facilitate information sharing at and across all levels of security.⁴⁷ Through these services, intelligence products are shared to appropriately cleared consumers via the Joint Worldwide Intelligence Communications System (JWICS), the Secret Internet Protocol Router Network (SIPRNet), and the Internet.

3.7.1 NCTC CURRENT

In September 2010, *NCTC CURRENT* replaced *NCTC Online*. *NCTC CURRENT* is the CT Community's premier web site for reporting and analysis. It allows users to easily browse titles and summaries, with full text articles, graphics, and multimedia presentations just a point and click away. *NCTC CURRENT* also features links to related articles, maps, photos, and videos, as well as the ability to search analytical products published by the IC and other important partners. *NCTC CURRENT* is available on JWICS with a valid public key infrastructure (PKI) certificate and on SIPRNet with a valid Passport account.

3.7.2 Worldwide Incidents Tracking System (WITS)

NCTC's WITS is the U.S. Government's authoritative database of terrorist attacks, compiled exclusively from open source information. WITS supports both the NCTC Report on Terrorism and the State

⁴⁷ IRTPA, Sec. 1016(b)(2)(F)

Department's annual Country Report on Terrorism. Policymakers, intelligence analysts, adjudicators, academics, and foreign partners use WITS data for a variety of purposes.

NCTC has recently launched the next generation of the WITS. WITS NextGen includes a page that incorporates all of the information and links from the previous WITS Classic public site, which was decommissioned on 31 August 2010. WITS NextGen is available to the public at <https://wits.nctc.gov> and includes the following features:

- Incident maps – WITS NextGen enables users to plot incidents using Google Maps or Google Earth (Google Earth plug-in required). The data can be plotted using cluster maps, heat maps, or density maps.
- Time maps – This feature allows users to plot incidents on maps over time, showing chronological changes by merely sliding a pointer.
- Improved search filters – WITS users can easily add and remove search filters to tailor their searches and find the exact data that is desired.
- Intuitive menu tabs – Once the WITS database delivers search results, users can “tab” through the results, further tailoring the results by criteria such as event types or locations.
- Customizable views – Column headings for search results can be added or removed, allowing for greater flexibility in viewing the data.

3.7.3 Intelligence Today

Intelligence Today, the daily online compendium of analytic products from across the IC, marked its first anniversary on 22 March 2011 by posting its 48,450th article. *Intelligence Today* uses the power of the secure Internet to produce an online newspaper for more than 9,600 IC and policymaker subscribers. Products are drawn from more than 60 sites, and organized into a “front page” with links to top stories, individual sections devoted to geographic and subject matter areas, and archives of previously published material. *Intelligence Today's* readers are drawn from more than 30 agencies and organizations across the policymaking realm, the IC and the military. About 1,150 readers visit the site on a daily basis.

3.7.4 Intelink

Intelink is a suite of web-based applications, tools, and services (including search) provided by the Intelink Enterprise Collaboration Center. It exists on JWICS, SIPRNet, and on the Unclassified network DNI-U. Intelink recently crossed the 100 million document threshold for records exposed to Intelink search services across the Unclassified, Secret, and Top Secret networks combined. In one month alone this year, Intelink recorded over two million searches. These milestones highlight the ability of IC personnel to access more information quicker and more effectively, enabling them to better share information and thus perform their missions. In addition, Intelink's user base passed the 200,000 mark in the spring of 2011. Increased use by the DoD and the law enforcement community over the past year have contributed to the growth, nearly doubling use on the Secret and Unclassified networks.

3.8 Watchlisting and Screening

The Watchlisting and Screening Sub-Committee of the ISA IPC focuses on the identification of watchlisting, screening and sharing policies, business processes, and technology, with particular focus on the Counterterrorism Watchlisting Community's end-to-end nomination and screening processes. The Sub-Committee is chaired by the National Security Staff and includes additional members from the CIA, DOT, DHS, DoD, DOJ, DOS, ODNI, the FBI, and the FBI-managed TSC.

Since the development of the consolidated terrorist watchlist that is in use today,⁴⁸ there have been many successes and improvements to watchlisting processes. Some of the more recent improvements include clearer definitions of federal agencies' roles and responsibilities, streamlining and standardizing nominations processes, improved use of biometrics for identification, and improved analytical and technological capabilities.

Despite the many successes and improvements to terrorist watchlisting and screening that have been institutionalized across the community since 9/11, the attempted bombing of Northwest Airlines Flight 253 on Christmas Day 2009 demonstrated that challenges still remained and improvements to the watchlisting and screening processes were necessary to keep our nation safe.

The National Security Staff led an effort to review current processes and provided recommendations to improve watchlisting business processes and rules while safeguarding the P/CR/CL of Americans.

3.9 Private-Sector Information Sharing

3.9.1 Collaborative Partnerships between the Private Sector and the IC

In March 2010, the ODNI Private Sector Partnerships office and the ODNI Analysis office sponsored a joint pilot project that brought together experts from the private sector with experienced IC analysts to develop collaborative partnerships. The goal of this effort is to provide IC analysts with a better understanding of select national and homeland security-related industries. It seeks to increase the depth of expertise among the participating analysts and is not intended as a mechanism either for operational activities or for formal coordination between industries and the IC.

The six-month pilot was successful and in March 2011 the Analyst-Private Sector Program was launched as a joint ODNI and DHS I&A program. Beginning in 2012, DHS I&A will serve as the executive agent of the program for the IC with oversight from the ODNI Private Sector Partnerships office.

3.9.2 InfraGard

InfraGard is an FBI information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants who are dedicated to sharing information and

48 Per HSPD-6

intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories and have more than 42,000 members.

3.9.3 Domestic Security Alliance Council (DSAC)

The DSAC is a strategic partnership between the FBI and the U.S. private commercial sector and enhances communications and promotes the timely and effective exchange of information. The DSAC advances the FBI mission in preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information. The DSAC membership consists of 400 individuals representing 211 companies.

3.9.4 Tripwire Program

The FBI's "Tripwire" program is designed to involve private-sector entities in identifying groups or individuals whose suspicious behavior may be a precursor to an act of terrorism. Tripwires are used by the private sector to alert authorities to activities which may not have risen to the level of law enforcement or intelligence scrutiny.

Terrorist Plot Thwarted in Texas

On 22 February 2011, Khalid Aldawsari, a chemical engineering major studying at South Plains College in Levelland, Texas, was arrested by federal authorities on the charge of attempted use of a weapon of mass destruction. One of the many targets of his plot was the home of former President George W. Bush in Dallas, Texas. Aldawsari came to the United States on a student visa to study at Texas Tech University, transferring to South Plains College in the fall of 2010.

Aldawsari raised the suspicions of North Carolina chemical supply company representatives when he unsuccessfully tried to receive a shipment of phenol, a chemical that can be used to manufacture explosives.⁴⁹ Aldawsari was informed that such a shipment could not be sent to his residence due to safety regulations. Aldawsari subsequently provided a Texas address of the freight company as an alternative shipping destination. When the shipment arrived at the freight company, officials refused receipt and it was sent back to the chemical supply company.

When the shipment was returned to them, representatives from the chemical supply company in North Carolina contacted the FBI to report Aldawsari's attempted purchase. Additionally, in Texas, officials from the freight company contacted the Lubbock Police Department with their concerns. These two phone calls placed by private citizens, provided critical information that assisted in the investigation and the subsequent arrest of Aldawsari.

⁴⁹ As outlined in the ISE-SAR Functional Standard 1.5, the acquisition of unusual quantities of chemicals is one of the behaviors reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

3.9.5 Critical Infrastructure Information Sharing

The CIKR ISE, developed and operated by DHS IP, supports the critical infrastructure protection and resilience homeland security mission. It is making substantial progress in providing useful critical infrastructure protection and resilience content to an increasing number of Critical Infrastructure Sector partners to identify their risks, reduce their vulnerabilities, and respond to and recover from incidents. It has also demonstrated that it successfully supports two-way information sharing across agencies, between all levels of government, and between public and private sectors.

The CIKR ISE includes Sensitive But Unclassified/Controlled Unclassified Information (SBU/CUI) and classified information. It delivers more than 12,000 SBU/CUI or unclassified products, reaching more than 30,000 federal and SLTTPS partners. The CIKR ISE also provides the private sector entry into the NSI via the SAR Tool for Critical Infrastructure, and is a mechanism for fusion centers to share regional infrastructure protection information directly with their private-sector partners via the Homeland Security Information Network–Critical Sectors (HSIN-CS) platform. IP also operates the Private Sector Clearance Program, which has granted more than 1,300 national security clearances for CIKR owners and operators of nationally critical assets in order to receive classified physical and cyber threat and vulnerability briefings as well as to provide subject matter expertise to the IC to develop useful actionable products at the unclassified level for broader distribution.

In addition to core information exchange, the CIKR ISE also serves as a comprehensive training, education, and collaboration tool. Accomplishments in critical infrastructure information sharing include a marked increase in the number of active users participating in the environment, increased availability and dissemination of actionable content, and the development and usage of relevant training, a form of information delivery in itself.

- The increase in new and active users registered on the CIKR ISE information-sharing platform HSIN-CS exemplifies its relevance for enabling decisions to protect and enhance the resilience of the nation's critical infrastructure. The number of active users grew by 67 percent over the last year. Currently, a new user registers every 1.5 hours.
- New content is made available on HSIN-CS at a rate of every 2.5 hours. As of the end of the 2nd quarter of FY 2011, 12,250 documents were available, representing a 100 percent increase over the same time last year.
- During the Deepwater Horizon Oil Spill, the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produced and posted 31 products to HSIN-CS and the Homeland Security Information Network-Emergency Management (HSIN-EM) to facilitate information-sharing across the broad spectrum of response operations.
- TRIPwire Community Gateway (TWCG), part of HSIN-CS, is designed to provide improvised explosive device (IED) awareness information specifically for the nation's critical infrastructure owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private-sector partners anticipate, identify, and prevent IED incidents. Over the past year, the number of registered users increased by 63 percent.
- HSIN Connect was utilized over the past year to host more than 28 educational events for approximately 17,500 critical infrastructure stakeholders. Briefing topics include CIKR resilience, threat detection, protective actions, best practices, and specific methodologies or CIKR tool training.

The foundation for the development and sustainment of the CIKR ISE is the National Infrastructure Protection Plan (NIPP) Sector Partnership, under the Critical Infrastructure Partnership Advisory Committee (CIPAC) framework. It consists of more than 700 active private sector and government leaders from every critical sector and from relevant government agencies at all levels, who develop the requirements, promulgate the processes, and execute the information sharing operations on a regular basis. They drive and deliver the CIKR ISE.

Most of the information that is shared day-to-day within the CIKR ISE consists of information necessary for the coordination and management of risks resulting from natural hazards and accidents. There is substantial overlap between how the CIKR sectors secure and build resiliency against natural disasters, accidents, and terrorist attacks. Natural disasters occur on a relatively predictable annual basis in the United States—hurricanes in the Southeast and on the East Coast, tornadoes in the Midwest, earthquakes and floods on the West Coast, snowstorms in the Northeast, and wildfires in the Southwest. Consequently, the foundation for sustainability for CIKR information sharing comes from leveraging the structures, processes, and mechanisms already in place. When there is a terrorist incident, the relationships will already be in place, and training for the use of tools, as well as familiarity and experience with executing the roles and responsibilities for operational coordination and information sharing will already be established.

Additionally, DHS, DoD, and the Financial Sector signed a memorandum of agreement in December 2009 initiating a pilot to address cyber threat information sharing. This pilot, which is ongoing, is based on lessons learned developed as a result of DoD's ongoing collaboration with approximately 35 companies in the voluntary Defense Industrial Base Cyber Security/Information Assurance program. This program is in the process of transitioning from a pilot to a program in 2011 and is opening up to all qualified cleared defense contractors through a rule in the Federal Register.

DHS Information Sharing Partnerships in the Field

The DHS investment in federal, state, local, tribal, public and private information sharing is much more than its investment in fusion centers alone. Fusion centers depend on and benefit from the expertise and information resources of tens of thousands of DHS component field personnel whose partnerships and collaboration venues turn information sharing into operational action nearly every day. Direct support to the fusion centers is one of many information sharing responsibilities of DHS components in the field. Here are just a few of the numerous examples of DHS information sharing partnerships in the field.

U.S. Customs & Border Protection (CBP)

CBP is developing an Operational Integration Center near Detroit which supports and improves information sharing, threat assessment, and joint response tactics between border security stakeholders in the Great Lakes region, so that CBP and its mission partners have a complete view of Northern Border security across their operating areas.

Immigration & Customs Enforcement (ICE)

Information sharing between fusion centers and the ICE Border Enforcement Security Task Force teams has increased the effectiveness of law enforcement operations, resulting in several major arrests and seizures within four ICE areas of operations. Also, through ICE's administration of the DHS Law Enforcement Information Sharing Initiative (LEISI), LEISI has engaged in extensive outreach to law enforcement partners within and external to DHS in an effort to promote law enforcement information sharing.

U.S. Secret Service (USSS)

The USSS leads a nationwide network of 31 Electronic Crimes Task Forces, bringing together federal, state and local law enforcement as well as prosecutors and representatives of private industry and academia. Their common purpose is to prevent, detect, mitigate, and aggressively investigate cyber-related crimes and cyber attacks on our nation's financial and critical infrastructures, with a primary focus on prevention. The USSS also makes the Targeted Violence Information Sharing System available to federal, state, and local law enforcement agencies with protective responsibilities to facilitate threat assessments.

U.S. Coast Guard (USCG)

USCG, as designated lead agency for the DHS Interagency Operations Centers program, is developing new information sharing procedures and capabilities to support federal, state, local, tribal, public and private partners in up to 35 U.S. critical ports. This program is improving joint targeting, prevention, and response collaboration with DHS and non-DHS partners in seven ports to date.

3.10 Foreign Partner Information Sharing

The United States and its foreign partners are committed to information sharing and cooperation in the prevention, investigation, and prosecution of terrorism-related offenses. Foreign partners are vital in the effort to combat terrorism by sharing key information, conducting surveillance, collaborating with U.S. overseas air passenger and maritime cargo screening, arresting members of terrorist cells, interdicting terrorist financing and logistics, and contributing to efforts in Afghanistan, Iraq, and other key places around the world.

3.10.1 International Information Sharing Pacts

In December 2010, the United States and the European Union (EU) began negotiating a new Passenger Name Record (PNR) agreement, to replace the 2007 pact that is temporarily in force. The United States is also in the process of negotiating an umbrella Data Privacy and Protection Agreement with the EU that will further facilitate the sharing of information. These negotiations began on 28 March 2011.⁵⁰

The State Department, along with DHS and DOJ, also continues to work bilaterally on Preventing and Combating Serious Crime (PCSC) initiatives with countries that participate in the Visa Waiver Program. PCSC agreements, like HSPD-6—Integration and Use of Screening Information—are designed to increase border security and law enforcement cooperation between the U.S. government and its foreign partners, and also authorize the spontaneous sharing of information for the purpose of detecting and preventing terrorist and criminal activity. Under PCSC, each party agrees to provide the other with electronic access to their fingerprint databases.⁵¹

One of the notable projects that the US-VISIT program is involved in is the Five Country Conference High Value Data Sharing Protocol. This protocol allows for biometrically-based information sharing among the United States and the four other member countries: Australia, Canada, New Zealand, and the United Kingdom. Separate bilateral Memoranda of Understanding (MOUs) that facilitate the matching of immigration and nationality cases against each others' biometric databases, and the exchange of relevant information in cases where biometric matches are made, for the collective benefit of the participants, were developed between all of the partner countries. All participating countries are using this biometric-information exchange to aid in immigration decisions. There have been several cases where immigration or law enforcement officials of participating countries have received new case information and/or taken direct action as a result of this biometric information sharing.

In February 2011, President Obama and the Prime Minister of Canada released the Beyond the Border Declaration: A Shared Vision for Perimeter Security and Economic Competitiveness, which identified information sharing, particularly along the northern border, as a key priority between the United States and Canada.

The FBI has also expanded its operations and is viewed as a global organization for a global age. Besides its 56 field offices and almost 400 resident agencies in the United States, the FBI has more than 250 special agents and support professionals in more than 60 overseas offices, pursuing terrorist, intelligence, and criminal threats with international dimensions in every part of the world. The Legal Attaché Program and the strategic placement of FBI offices has enhanced information sharing with international law enforcement and intelligence agencies. The FBI also takes part in all manner of global and regional crime-fighting initiatives, including with INTERPOL and Europol; the Budapest Project; and Resolution 6, which co-locates FBI agents in DEA offices worldwide to combat drugs.

50 Statement for the Record, Ambassador Daniel Benjamin, Coordinator For Counterterrorism, Counterterrorism Cooperation With Europe And Eurasia, House Foreign Affairs Committee, Subcommittee On Europe And Eurasia, 5 May 2011

51 Ibid.

Finally, in February 2011, President Obama and the Prime Minister of Canada released the *Beyond the Border Declaration: A Shared Vision for Perimeter Security and Economic Competitiveness*, which identified information sharing, particularly along the border, as a key priority between the United States and Canada. In response to the Declaration, the National Security Staff formed an interagency working group to prioritize initiatives and develop action plans for implementing the cross-border information sharing priorities outlined in the Declaration.⁵²

3.10.2 Sharing Best Practices

A goal of the ISE's efforts for international information sharing is the sharing of ISE best practices. The ISE is currently developing an online knowledge base that describes important core concepts, approaches and best practices of the ISE, including governance, standards, policy, budget, performance management, privacy policies, and a process for suspicious activity reporting. The knowledge base will be available to international partners, including Canada, to assist them in developing and adopting similar models and applying ISE concepts to new environments. As this initiative is underway, Canada and Mexico have already reached out to their U.S. counterparts to inquire and learn about some of these concepts, such as utilizing NIEM and interoperability standards and solutions for inter-departmental and inter-jurisdictional information sharing with international allies. In addition, the United States, Canada and Mexico are considering several pilot programs using NIEM to demonstrate information sharing in the public health or law enforcement arenas. The ISE is supporting and encouraging these information exchanges through outreach with international partners and participation in internationally attended conferences.

3.10.3 Cross-Border Sharing Empowered by the National Information Exchange Model (NIEM)

Recognizing the value that NIEM could provide for facilitating information sharing within the Canadian government and along the border with the United States, the Canadian government has shown strong commitment to adopting NIEM in the public safety, law enforcement, defense, and disaster management domains.

Recognizing the value that NIEM could provide for facilitating information sharing within the Canadian and Mexican governments and along their borders with the United States, both Mexico and Canada have shown interest in adopting NIEM in the public safety, law enforcement, defense, and disaster management domains. The ISE is supporting and encouraging these information exchanges through outreach with international partners and participation in internationally-attended conferences and forums, such as North American Day.

Annually, the United States, Canada and Mexico participate in the North American Day conference, a meeting of national Chief Information Officers (CIO) and government

⁵² <http://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord>

representatives. The purpose of North American Day is to exchange ideas and approaches for improving electronic government (e-government), including information sharing programs, interoperability, standards, investments, and partnerships between the private and public sector, among others. One of the outcomes from North American Day 2010 included a commitment from the three countries to conduct an international information sharing pilot program using NIEM. Since then, portions of the Canadian government, particularly Public Safety Canada, in coordination with the NIEM PMO, have explored and initiated two NIEM proofs-of-concept with Canada's Royal Canadian Mounted Police and the Canadian Association of Chiefs of Police. In addition, Canada has launched a web presence through the NIEM website, *niem.ca*, for public use and consumption.

The next North American Day, scheduled for July 2011, will include a continued and renewed commitment to e-government and information sharing among the three countries. One of the goals of the meeting is to confirm a three-way, pilot project between the United States, Canada, and Mexico, using NIEM to demonstrate information sharing in the public health or law enforcement arenas. The meeting is planning to conclude with the signing of an MOU, formalizing the commitment of the three countries to international information sharing, which has been agreed to in principle.

Canada's Chief Information Office is also working to develop common interoperability standards and solutions for inter-departmental and inter-jurisdictional information sharing. To address this challenge, Canada is standing up an Interoperability Centre of Excellence that is investigating interoperability frameworks that are likely to be instrumental in forming an interoperability solution for the Government of Canada, which includes the solutions and ideas currently underway with U.S. NIEM and ISE efforts. PM-ISE and the ISE (particularly the NIEM PMO) have been supporting this effort by providing information on the current NIEM-ISE architecture, best practices, and lessons learned from the ISE's interoperability efforts.

3.11 Law Enforcement Information Sharing

Because of the threat of terrorism within our homeland, state, local, and tribal law enforcement agencies have adopted an "all crimes, all threats, all hazards" business model to protecting life and property within their jurisdictions. Coupled with an arsenal of law enforcement information sharing systems, police officers today are better able to identify threats. While the focus of the ISE is terrorism-related information, public safety information sharing techniques and tools are not bifurcated between terrorism and law enforcement. For a trooper patrolling America's highways, his or her next stop might be a potential terrorist.

3.11.1 Criminal Justice Information Services (CJIS)

The FBI's CJIS is the focal point for some of the most important and relevant criminal history databases used by law enforcement including: wanted persons, stolen property, stolen vehicles, the national sex offender database, and the national domestic violence database, as well as databases for offenders who may not legally purchase firearms. The nationwide reach and application of CJIS proves that information can be shared and accessed securely on a large scale and ensures that an officer can discover if a suspect in rural Texas presents a danger to his safety, even if the criminal history was documented in urban California.

National Data Exchange System (N-Dex)

FBI's National Data Exchange System (N-DEX) is a criminal justice information sharing system that provides nationwide connectivity to disparate local, state, tribal, and federal systems for the exchange of information. Through N-DEX, law enforcement officers have the ability to search, link, analyze, and share investigative information (e.g., incident and case reports), but the data that is shared through N-DEX remains with the law enforcement agency that provided it. In March 2011, the final increment of the N-DEX system was delivered, increasing its power, speed, and accessibility while greatly improving the user's information-sharing experience. As of April 2011, the N-DEX system had approximately 8,000 registered users and approximately 100 million records contributed by 26 local, state, regional, and federal information sharing systems, consisting of the FBI and more than 3,600 other agencies.

N-DEX in Action

A Hood River County detective in Oregon investigating a homicide developed a list of persons of interest living outside the state using N-DEX. The detective found that one of the subjects of the investigation had contacts in California, and two of the records provided a telephone number in the Los Angeles area. The Oregon detective contacted the Los Angeles Sheriff's Department, which provided vital information on the subject. As a result, the detective located the suspect in Los Angeles, and the Sheriff's Department arrested the suspect. After the detective interviewed the suspect in Los Angeles, the suspect was then extradited to Oregon and is currently awaiting trial.

A Colorado state trooper was assigned to assist in an organized crime case initiated by a local law enforcement agency. During the investigation, a person of interest was identified, but a current address and other valuable information could not be found in accessible databases. Through N-DEX however, the trooper discovered prior charges against the subject in a closed federal drug case in another state; additional drug-related cases in California; and learned that the subject was a known Armenian Power Gang member. This investigation uncovered the Armenian Power Gang's presence in Colorado. Colorado is now preparing awareness reports to notify law enforcement and is working on adding this gang to the state's database.

3.11.2 eGuardian Adopted by DoD

In 2010, the FBI's eGuardian system was selected by DoD to replace its previous threat reporting structure, which was terminated in 2007. After two years of analysis, review of more than 60 systems, and the culmination of a six-month pilot program in June 2010, DoD selected eGuardian.

The eGuardian system was developed by the FBI's Counterterrorism Division in response to mandates by IRTPA, other statutes and Executive Orders, and the National Strategy for Combating Terrorism. eGuardian is a complete, web-based reporting system where federal, state, local, and tribal law

enforcement officers, state fusion centers, regional intelligence centers, and FBI task force officers can share timely information about suspicious activity and terrorist threats. This system gives law enforcement and IC partners a greater degree of connectivity with regard to the collection and dissemination of suspicious activity and threat reporting.

By sharing such information in a near real-time system, partners can avoid jurisdictional and bureaucratic impediments that may delay communication between agencies. All partner organizations are able to contribute to and extract information from eGuardian according to their needs and can keep their reports continually updated.

In the wake of the tragic Fort Hood shootings in November 2009, a DoD board reviewing the incident cited the need to “adopt a common force protection threat reporting system for documenting, storing, and exchanging threat information related to DoD personnel, facilities, and forces in transit.”⁵³ The answer to this need for the DoD was the FBI’s eGuardian system.

3.11.3 Technical Resource for Incident Prevention (TRIPwire)

TRIPWire is DHS’s 24/7 online, collaborative, information-sharing network for bomb squad, law enforcement, and other emergency services personnel to learn about current terrorist IED tactics, techniques, and procedures, including design and emplacement considerations. Developed and maintained by the Office for Bombing Prevention within DHS IP, the system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to assist law enforcement in anticipating, identifying, and preventing IED incidents. Over the past year, the number of registered users has increased by 88 percent.

3.11.4 Next Generation Identification System (NGI)

The NGI program will incrementally replace the FBI’s CJIS Division’s existing Integrated Automated Fingerprint Identification System, in service since July 1999. The NGI improves, expands, and creates new biometric services, providing identification, criminal history, and investigative information to more than 18,000 law enforcement agencies, multiple federal partners, and authorized screening/employment agencies. On 25 February 2011, the FBI achieved Initial Operating Capability for its NGI System, with the deployment of the Advanced Fingerprint Identification Technology (AFIT). The AFIT provides the foundation on which the rest of the NGI services will reside and provides new advanced matching algorithms, elevating the systems current accuracy to greater than 99 percent. Due to the improved NGI AFIT accuracy, 910 additional candidates were identified during the first five days of service, quickly validating the anticipated superior AFIT performance. One noteworthy success resulting from this new technology emerged with a civil applicant fingerprint background check submission. The FBI received a submission for a person who was applying to provide housing for foster care and child placement. The NGI’s AFIT led to the identification of a subject with prior violent criminal charges, including armed robbery.

53 Protecting the Force: Lessons from Fort Hood, Report of the DoD Independent Review, January 2010

Another example of how the new services delivered by the NGI can benefit specific organizations and individuals is through the Repository for Individuals of Special Concern (RISC) Pilot project. The RISC Pilot allows officers on the street to use a mobile ID device to rapidly search a national repository of 1.2 million fingerprint records of “the worst of the worst” to quickly assess the threat level of any subject encountered during their normal law enforcement activities, receiving a response within seconds. In this pilot, Ohio, Florida, Maryland, Georgia, and Texas law enforcement agencies, using mobile ID devices, employ the CJIS Wide Area Network to securely transmit “live” fingerprints from the field to the RISC for a rapid search. As of 13 June 2011, 76,791 total RISC live submissions have been received, resulting in 1,357 hits. This RISC Pilot functionality will be enhanced and will be available nationwide in September 2011. One example of success with the RISC Pilot occurred on 23 January 2011 in Ohio, in the early morning hours, when the West Chester Police Department encountered an individual who was stopped for a vehicle equipment violation. The subject was nervous and was unable to provide proper identification. Officers captured the individual’s fingerprints on the mobile ID device and received a response from the state database as well as the FBI RISC. The responses confirmed the identity of the individual and provided information that the subject had warrants in Dearborn County, Indiana for felony drug charges.

3.11.5 United States Visitor and Immigration Status Indicator Technology (US-VISIT)

DHS’s US-VISIT Program provides homeland security decision-makers with a consolidated source of biometric and biographic information on visitors and immigrants entering and exiting the United States or applying for immigration benefits. Although the vast majority of US-VISIT information is non-derogatory immigration information, US-VISIT’s watchlist includes information about criminals, immigration violators, and known or suspected terrorists. US-VISIT helps federal, state, local, and international partners quickly and accurately identify individuals and assess whether these individuals pose a risk to homeland or national security.

US-VISIT and FBI Fingerprint Records Tie Suspected Serial Killer to Arrest Warrants

In August 2010, CBP officers at Atlanta’s Hartsfield-Jackson International Airport arrested a man after fingerprint records confirmed there were outstanding warrants for his arrest in connection with a murder in Michigan. The interoperability between FBI and US-VISIT systems helped CBP obtain the information they needed in a timely fashion. The man, suspected of several murders and assaults in Michigan and Virginia, was arrested as he attempted to board a flight bound for Tel Aviv, Israel. CBP officers took the man into custody and turned him over to law enforcement authorities.

US-VISIT Assists Joint Terrorism Task Force by Identifying Counterfeit Document

In November 2010, US-VISIT assisted in a case to determine the true identity and overstay status of a Turkish man attempting to gain employment at a nuclear power plant. It was determined that the subject was using a false document under a false identity to prove his legal status to reside and work in the United States. The subject was subsequently arrested by local DHS law enforcement authorities as an “overstay” and placed into federal custody awaiting removal proceedings.

US-VISIT Helps CBP Identify Illegal Alien with Outstanding Homicide Warrant and Considered Armed and Dangerous

In August 2010, the Border Patrol in Yuma, Arizona apprehended a man who had entered the United States illegally. The subject’s fingerprints were checked against the Automated Biometric Identification System and it was determined that he had two outstanding warrants, including one for homicide, and that he was considered armed and dangerous. He was taken into custody and faces charges in the 2004 stabbing death of his girlfriend in Oregon.

3.11.6 Law Enforcement Information Sharing Initiative (LEISI)

The DHS LEISI has engaged in numerous partnerships with law enforcement agencies in order to share and exchange law enforcement information. These bi-directional information sharing collaborations not only allow federal, state, local, and tribal agencies to access DHS law enforcement information, but they also afford DHS law enforcement officers access to critical law enforcement information held by their external law enforcement partners. This sharing of information is usually through access to computerized law enforcement information systems, and can sometimes be accessed from mobile devices. This quick access to law enforcement information can allow officers to make tactical adjustments in ongoing operations so as to increase the chances for a safe and successful operation.

- ICE agents in Arizona, using a Portable Digital Assistant (PDA), were able to access state and local law enforcement information through the Tucson Police Department’s law enforcement information sharing system and were able to make last-minute changes in the direction of travel during the surveillance of Drug Trafficking Organization suspects. With updated address information obtained through the PDA, the agents were able to maintain surveillance of the suspects and achieve the goals of the surveillance. The information also provided a mug shot of one of the suspects who was previously unknown to agents. The newly identified suspect was found to be armed during the surveillance, and the identification of the suspect allowed other agents to be alerted.

In the past year, through its LEIS Service, the LEISI has established a direct connection to Nlets making DHS criminal and enforcement biographic data available to all law enforcement personnel connected to Nlets. The LEISI is also in the process of establishing LEIS Service connections to the FBI/CJIS N-DEX. LEISI is also a proponent of NIEM and is currently developing metrics to measure the success of DHS law enforcement information sharing.

The LEISI continues to engage international law enforcement agencies in developing partnerships that will aid in international law enforcement information sharing. These efforts have been through PCSC initiatives with Spain, Germany, and South Korea, and have also been through negotiations with the government of Canada. Currently, DHS law enforcement information is made available to the Royal Canadian Mounted Police through the Nlets. DHS LEISI is also negotiating an information sharing agreement with Canada that will allow a bi-directional exchange of law enforcement information between RCMP and DHS.

3.11.7 National Law Enforcement Telecommunications System (Nlets)

Nlets paved the way for information sharing by implementing Extensible Markup Language (XML) and off-the-shelf technologies and spearheading the effort to provide crucial information, like criminal histories, to the CBP in real time. Currently, Nlets is teaming with the DOJ to pursue the necessary security measures for enhanced law enforcement information sharing. Recently, the Nlets Program Management Office asked PM-ISE to assist in improving Nlets access for tribal law enforcement organizations. PM-ISE reached out to Indian Country, expanded their knowledge of Nlets benefits, and established the first ever connectivity pilot with four tribes in separate regions of the United States.

3.11.8 Domestic Highway Enforcement Initiative (DHE)

U.S. highway troopers are a critical line of defense against all crimes, all threats, and all hazards, including terrorism in the homeland. For example, in July 2001, a police officer stopped and ticketed Muhammad Atta in Florida. In September 2001, Atta crashed a plane into the North Tower of the World Trade Center. In August 2001, Hani Hanjour was pulled over for speeding in Arlington, Virginia. Hanjour piloted the plane that crashed into the Pentagon. On 9 September 2001, a Maryland trooper stopped Ziad Jarrah for speeding. Two days later, Jarrah piloted the plane that crashed in Shanksville, Pennsylvania.

The DHE initiative promotes collaborative, intelligence-led, unbiased policing in coordinated and mutually supportive multi-jurisdictional law enforcement efforts on the nation's highways. The DHE improves the investigative efforts of HIDTAs and has a significant impact on traffic safety, homeland security, and other criminal activity. The DHE operational model has contributed to numerous success stories regarding the disruption of significant criminal activity along U.S. highways. For example, in February 2011, a DHE-supported Iowa Highway Patrol trooper seized more than \$49,000 during a routine traffic stop. Iowa Department of Narcotics Officers shared the information with their state fusion center, which passed along information to Minnesota authorities. Authorities in Minnesota seized another \$25,000 from a second suspect at the Minneapolis Airport. Intelligence information on the original suspect revealed that he had recently shipped \$40,000 in cash California. DHE-supported analysts and officers in Aptos, California, worked the case. They seized guns, processed marijuana and 1,400 marijuana plants in an indoor grow operation.

Information Sharing Improves Training and Enhances Interdiction

The Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) has partnered with the Drug Enforcement Administration (DEA) and the ONDCP in support of its Drug Interdiction Assistance Program (DIAP). This multi-agency information sharing effort has directly contributed to the apprehension of suspects on the terrorism watchlist, illegal aliens, and multiple seizures of contraband and drugs. In 2010, seizures from commercial vehicles included 769,696 pounds of marijuana, 16,612 pounds of cocaine, 297 pounds of methamphetamine, 15 pounds of heroin, and \$59.2 million dollars in illicit U.S. currency. Two recent examples include:

- In March 2011, an Alabama state trooper stopped a tractor trailer for a traffic violation. The trooper, remembering his FMCSA-DIAP criminal activity indicators training, decided to make inquiries to various law enforcement systems and determined that the driver was a known smuggler and a wanted fugitive. Subsequently, the trooper discovered 1,403 pounds of marijuana mixed in with the trailer's cargo.
 - Also in March 2011, an Iowa state trooper stopped a tractor trailer for a traffic violation. Based on his FMCSA-DIAP training, the trooper observed a number of visual threat and criminal indicators. The trooper obtained consent to search the vehicles which resulted in the discovery of \$2.5 million dollars of illicit currency in the trailer's modified wall and refrigeration unit.
-

3.11.9 INTERPOL I-24/7

The U.S. National Central Bureau of INTERPOL (INTERPOL Washington) serves as the statutorily-designated U.S. representative to the International Criminal Police Organization (INTERPOL) on behalf of the Attorney General. Through INTERPOL Washington, local, state, federal, and tribal law enforcement authorities can communicate in near real-time with their counterparts in the 187 other member countries of INTERPOL, either individually or with multiple countries simultaneously, by means of an encrypted, Internet-based virtual private network (VPN) known as I-24/7. This highly secure system provides a full messaging capability and access to INTERPOL databases containing vital international investigative information on wanted and missing persons, terrorists, fingerprints, biometric information, stolen and lost travel documents, stolen motor vehicles, as well as stolen and recovered works of art and significant cultural artifacts. In addition, I-24/7 supports the exchange of international humanitarian assistance requests involving death notifications, threatened suicides, and health and welfare checks on U.S. citizens overseas, and foreign nationals in the U.S. INTERPOL Washington has established secure network partnerships with the Nlets, RISS, the FBI's Law Enforcement Online (LEO), DOJ, DHS, and a number of other government law enforcement agencies, to facilitate secure information exchange and to allow access to the INTERPOL database for investigative assistance.

By providing access to INTERPOL's worldwide police-to-police communications and criminal intelligence network, INTERPOL Washington significantly enhances international investigative support and cooperation between U.S. law enforcement agencies and their foreign counterparts—cooperation that is oftentimes critical in the apprehension of a fugitive or the recovery of an abducted child.

INTERPOL in Action

In January 2011, a foreign national arrived in the United States and proceeded to travel to his ex-wife's residence in Alabama, where he kidnapped his five-year-old daughter. The father and daughter left the United States for France, but had to travel through the Netherlands. INTERPOL Washington coordinated communications and information with U.S. Justice Department officials, the Alabama Police Department, INTERPOL The Hague and INTERPOL France. Based on this exchange of information, the offender was arrested upon arrival in the Netherlands. The child was taken into protective custody and reunited with the custodial parent within three days.

In February 2011 a Colorado Police Department contacted INTERPOL Washington advising that an offender wanted for a sexual assault with serious injury had fled the United States on a commercial flight with a destination of Libya. As the offender's travel was to take him through the United Kingdom (UK), INTERPOL Washington immediately contacted INTERPOL London. Upon arriving in the UK, the offender was denied entry and placed on a flight back to the United States. After landing in Chicago, the offender was immediately taken into custody on the Colorado warrant.

In all instances, INTERPOL Washington coordinates U.S. law enforcement action and response, ensuring that the exchange of information is consistent with U.S. interests and law, as well as INTERPOL policies, procedures, and regulations. Even for U.S. law enforcement agencies with a well-developed international criminal investigative presence, INTERPOL Washington's services are complementary—not competitive or duplicative—and are available 24/7/365.

Law Enforcement Integrated Information Architecture

In October 2010, ONDCP, the Joint Interagency Task Force South, DHS's Office of Counternarcotics Enforcement, and DHS I&A sponsored an Interdiction Committee initiative to apply technology in the fight against drugs. Titled the Law Enforcement Integrated Information Architecture, this program will develop an information sharing architecture to create advanced analytical awareness, resulting in more actionable law enforcement intelligence, ultimately resulting in increased interdictions. This effort, focusing on the Southwest Border initially, is undertaken in partnership with ONDCP, DHS, the Southwest Border Intelligence Integration Working Group, and the DEA.

3.12 Homeland Security Standing Information Needs

Documenting information needs is essential to the production of intelligence that is responsive to consumers, and is key to enabling effective information sharing. In 2010, DHS reorganized its Homeland Security Standing Information Needs (HSEC SINS) into 10 topics that align with the information needs of other IC and HSEC Community of Interest (COI)⁵⁴ members. This alignment enhances the ability of federal, state, local and tribal partners to collaborate during every step of the intelligence cycle.

For example, HSEC COI partners have been asked to tag raw information reports and finished intelligence products with relevant HSEC SINS. The practice of tagging items using common categories enables partners throughout the HSEC COI to more effectively share information and intelligence with target audiences, ensuring that homeland security stakeholders are receiving what they have identified as important and relevant to their operations. DHS continues to work with state, local and tribal partners, through the fusion centers, to develop SINS that are relevant to each fusion center's area of responsibility. Documenting SINS provides fusion centers with a baseline to guide their information collection activities and it further enables fusion centers to effectively communicate their information needs with the broader HSEC COI.

In November 2010, DHS launched a SINS development initiative for the private sector. This initiative included actively engaging interagency governmental partners, as well as owners and operators from the 18 CIKR sectors, in the information needs identification process. The effort began with a pilot between DHS and the Oil and Natural Gas sector owners/operators, private-sector analysts, key trade association representatives, sector leadership, and analysts from the Department of Energy (DOE), DOT, and Transportation Security Administration (TSA). The pilot brought together interested government sector and intelligence personnel with private-sector personnel to educate each another about their respective missions, roles, and business processes. These sessions ended with a facilitated discussion of the sector's specific information needs.

The SINS identified by each CIKR sector will be integrated by DHS into the overarching HSEC SINS, and will enhance the ability of homeland security and IC partners to effectively collaborate with the private sector during every step of the intelligence cycle. Over the next year, DHS will continue to employ this new process for working with the other CIKR sectors to identify and address their information needs.

⁵⁴ Homeland Security Community of Interest (HSEC COI) is defined as DHS and its federal, state, local, tribal, territorial, and private sector stakeholders and homeland security partners.

Building Beyond the Foundation

The ISE is building beyond the foundation set over the last several years and is making critical improvements in responsible information sharing. The foundation of the ISE was built through strategic coordination and mission partner investment. The 2007 National Strategy for Information Sharing provided specific goals, guidance, and performance assessment criteria by which progress is measured. As the ISE moves into the next phase of implementation, PM-ISE is focusing its attention on new priorities, while ISE mission partners continue to sustain and grow existing capabilities. The PM-ISE is refreshing the National Strategy for Information Sharing to bring a new performance framework, with identified goals, objectives, and metrics for monitoring progress, into action.

Governance has emerging as a critical enabler and guiding force for accelerating the implementation of the ISE and coordinating efforts among multiple agencies at all levels of government and with the private sector. The Information Sharing and Access Interagency Policy Committee (ISA IPC) and its subordinate Sub-Committees and Working Groups are at the forefront of achieving effective interagency governance, coordinated implementation, and results measurement. Sub-Committees and Working Groups, which are chaired by senior representatives from throughout the ISE, are achieving consensus on how to develop a unified ISE and are realizing whole of government results for new and improved sharing and protection capabilities for all ISE partners. The ISA-IPC has reached a strong operating state, with a quarterly battle rhythm that drives progress toward the ISE goals.

The National Security Staff and the Office of Management and Budget issue annual ISE programmatic and implementation guidance that leads to cohesion and focus across the ISE. This and other Federal Government-wide guidelines, rules, procedures and functional standards are creating further momentum to enable the ISE to be an effective and efficient environment to responsibly share critical national and homeland security information. In addition to this top-down governance construct, communities of interest have formed around many key information challenges and these communities are accelerating progress and implementation of the ISE.

An ISE roadmap, with important components such as standards adoption, industry engagement, and strategic sourcing, will help steer the ISE in the right direction. Shared functional capabilities like identity management, information security, and auditing are necessary to provide a secure and functional technical space for information sharing. Further, continuing to develop human capital through enhancing training, conducting exercises, and replicating best practices remains a critical success factor for all ISE mission partners.

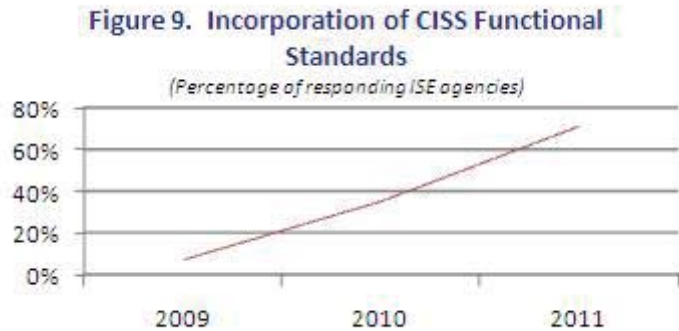
Increased interaction with all stakeholders, including industry and standards development organizations, is enabling standards-based procurement, strategic sourcing, and a deep collaboration that benefits all participants of the ISE. Ensuring that all mission partners are synchronizing efforts will ensure that the ISE continues to grow efficiently, and to enable analysts, investigators, and operators to prevent terrorist attacks and promote homeland security.

4 Establishing Standards for Responsible Information Sharing and Protection

The PM-ISE is working with mission partners and standards organizations to identify the best existing standards for reuse and implementation across the ISE. Following the Office of Management and Budget (OMB) direction on voluntary consensus standards in Circular No. A-119, the PM-ISE is leveraging and influencing industry standards to help make information transfer simpler and more predictable. Engagement with industry to build products based on standards both improves “off-the-shelf” interoperability of commercial solutions and ensures availability of technical solutions in shorter timeframes and at a lower incremental cost overall to mission partners.

4.1 Advancing Existing Standards for Information Sharing and Protection

To build the foundation of the ISE, the Common Information Sharing Standards (CISS) Program, was created to develop functional and technical standards to enable broader federal, state, local, tribal, and private sector access to, as well as the distribution and sharing of information. Functional standards set forth the rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas. There has been a steady increase in the number of departments and agencies that are incorporating functional standards into the management and implementation of ISE-related mission business processes; over the past year there has been a 36% increase to a total of 10 out of 14 departments and agencies (See Figure 9.)



The ISE Functional Standard for Suspicious Activity Reporting (ISE-SAR) is an excellent example of a functional standard now advanced by mission partner-specific efforts via the Nationwide Suspicious Activity Reporting Initiative (NSI). The ISE-SAR functional standard allows present and new participants in the NSI to use common terminology, data elements, and formats and also provides the necessary definitions, and outlines the behaviors, so that a police department in New Jersey, for example, can easily understand the details of a suspicious activity occurring in Los Angeles. Sixty-four percent of the ISE department and agencies indicate that functional standards such as ISE-SAR are helping to improve CT processes, interfaces to other ISE partners, and the structure of data/information for sharing in the ISE; this is a 21% improvement over the last year.

Similar functional standards currently being developed and implemented include:

- The NIEM AMBER Alert Specification, which improves the sharing of Amber Alerts between jurisdictions and across multiple communications networks and technologies.
- The Standard NIEM Prescription Monitoring Program Information Exchange, which assists law enforcement, health agencies, and prescribers in identifying potential abuse and diversion.
- NIEM-enabled Cyber Incident Information Sharing, which will bring cyber security specialists from around the world together to respond to cyber incidents as a collective force, to minimize loss and disruption.

CISS technical standards document the specific technical methodologies and practices used to design and implement information sharing capabilities into ISE systems. Many technical standards development efforts have evolved out of the growing needs of the Internet community, and are managed by industry consortia, often referred to as Standards Development Organizations (SDOs). These SDOs develop standards using robust methodologies and tools which are designed to simplify and unify the way in which applications communicate, interact and interface in order to handle their information exchange needs. At present, seven out of 14 responding ISE departments and agencies have incorporated CISS Technical Standards into their architectures, accounting for a 7% increase since 2010.

Technical standards also include a specific type of standard for securing information technology systems. Without commonly understood definitions for security controls and how they are implemented and maintained at the application, network, and enterprise levels, either costly retesting of security controls must be performed prior to interconnecting systems so they can share information, or significantly higher levels of risk must be accepted. In the federal space, several organizations have the authority, pursuant to the Federal Information Security Act of 2002 (FISMA; 44 USC §3541), to promulgate security standards, including: the National Institute for Standards and Technology (NIST) (the Special Publications 800 Series); the Intelligence Community (IC); the Department of Defense (DoD); and the Committee on National Security Systems (CNSS). This year the ISE has significantly increased coordination with these groups in order to adopt or establish common security standards. Increased standardization also enables industry partners to “bake in” common security controls in their products and services, thereby improving the overall security of such products and supporting downstream assured information sharing.

4.2 Coordination of Standards to Enable Interoperable Capabilities

Standards are critical enabling capabilities as they allow the ISE to deliver the decentralized, distributed, coordinated, and interoperable capabilities described in IRTPA. The way in which standards are identified, developed, adopted, and implemented requires significant cooperation and shared vision among interagency groups utilizing a rigorous governance structure that incorporates the values, expertise, and priorities of relevant partners.

Registry of USG Recommended Biometric Standards

The Registry of USG Recommended Biometric Standards (Registry), which was updated in February 2011, supplements the National Science and Technology Council (NSTC) Policy for Enabling the Development, Adoption and Use of Biometric Standards. This Registry lists recommended biometric standards for U.S. Government-wide use. It is based upon interagency consensus on biometric standards required to enable the interoperability of various federal biometric applications, and to guide federal agencies as they develop and implement related biometric programs. The NSTC Subcommittee on Biometrics & Identity Management will continuously review the content of this document, and release updated versions as required to assist agencies in the implementation and reinforcement process of biometric standards to meet agency-specific mission needs.

4.2.1 Standards Governance

Recognizing the critical role of standards in enabling the ISE and mission partner operations, in May 2011 the ISA IPC approved the creation of a Standards Working Group to coordinate efforts across departments, agencies, and levels of government. The Standards Working Group, which replaces interagency efforts previously under the Common Information Sharing Standards (CISS) Program, is developing a work plan focusing on standards and implementation profiles that should be coordinated and developed to ensure agreement, reduce duplication of effort, and influence existing standards efforts across the whole of government. The purpose of the interagency effort is to facilitate cross-domain, enterprise-wide interoperability and information sharing through standards. The initial goal of the group is to clearly define a process by which a standard is taken from need recognition to solution implementation, whether by adopting an existing standard, harmonizing or modifying a standard, or leading the creation of a new standard. To enable the government-wide approach, the Standards Working Group is also developing a shared lexicon, or term dictionary, wherein languages across many standards groups and domains can be aligned to prevent fragmentation or communication gaps. Another key to making standards work, is making them accessible, thus the working group is aiming to adopt a central repository so that government consumers will have a single location to locate and explore the available resources.

4.2.2 Industry Engagement

In 2011, PM-ISE joined both the Object Management Group (OMG) and the Organization for the Advancement of Structured Information Standards (OASIS). PM-ISE's aim in joining these organizations is to bring federal, state, local, and tribal government partners together to leverage existing work on specifying government standards and to harmonize those standards. Additionally, PM-ISE aims to work with OMG and OASIS to institutionalize those efforts as standards that industry can incorporate into their products and services.

In addition to engaging industry, PM-ISE is currently working with its ISE mission partners on a strategic sourcing approach based on industry standards and implementation profiles. Strategic approaches like

these will allow mission partners to procure products that are interoperable, cost-effective, and policy and standards-compliant. Mission partners can communicate these ISE-based requirements to industry in their requests for proposals (RFP) and realize targeted solutions which deliver the ISE. Industry reacts to customer demand (via RFPs, procurements, acquisitions) and this sourcing approach will encourage industry to create standards-based interoperable solutions for the ISE.

4.3 The National Information Exchange Model (NIEM)

NIEM is a “community-built” initiative that was born as a best practice developed by a handful of state and local practitioners. NIEM connects communities of people who share a common need to exchange information to advance their missions. The NIEM community is now a large partnership between federal agencies, state governments, the private sector and several international countries. NIEM is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM has become a well-tested and mature repeatable, reusable process for developing information exchange requirements that improves efficiency, saves time, reduces costs, and advances and fulfills organizational missions

Since its inception in 2005, NIEM has focused on data: understanding it, ensuring that it is discoverable, and standardizing it so that the data moves easily across departments and agencies. NIEM provides a commonly understood way to connect data to improve government decision-making for the greater good. This program has seen substantial mission area growth in the last several years, extending well beyond its original justice and homeland security roots. For example, this year saw the U.S. Department of Health and Human Services (HHS) joining the Federal Government’s NIEM Steering Group with HHS’s commitment to adopt NIEM into the health records data standardization process. NIEM has played a critical role in establishing a common vocabulary that has significantly enabled development of information exchanges, such as the SAR Information Exchange Package Documentation (IEPD), which defines the terms that would comprise a SAR anywhere a SAR is used if generated by participating partners at the federal, state, or local level, or by private-sector partners. These exchanges represent formal, machine executable models that ensure universal meaning even if the exchanging parties have no direct relationship with each other and do different jobs in different locations or agencies.

4.3.1 Advancing Use of NIEM Across All Levels of Government

NIEM creates a standardized way of doing business and as such, is a core process and framework for the ISE. In FY 2010, OMB provided guidance to all federal agencies to evaluate the adoption and use of NIEM as the basis for developing reference information exchanges. The initial results of the evaluation were very positive. To date, 12 federal agencies have committed to using NIEM. NIEM is also gaining significant adoption as a common framework for information sharing for a number of states, as well as local and tribal agencies. Seven more federal agencies and some international partners are evaluating the potential to use NIEM for their missions. Agencies that are not already using NIEM are required to exchange information with those that are, which will drive further adoption.

In April 2011, the Federal CIO Council released the NIEM adoption and use report. This Report indicates that:

- NIEM is gaining significant adoption as a common framework for information sharing. NIEM architecture allows the flexibility for different domains and agencies to leverage the common infrastructure and architecture offered by NIEM, while allowing them to maintain the information exchange requirements for their domains. This flexibility is a key contributing component for NIEM success and adoption.
- A growing number of federal, state, local, tribal and international mission partners are adopting NIEM for their information sharing needs
- Twelve federal agencies have committed to using NIEM. Seven more federal agencies and some international partners are evaluating the potential to use NIEM for their missions
- Recent additions to NIEM domains include Cyber security, Federal Health and Human Services, Youth and Family Services, and Agriculture

4.3.2 Advancing NIEM and UML Tools

To foster the evolution of the NIEM toolkit, the NIEM Program Management Office (PMO) and the PM-ISE, with support from SEARCH (the National Consortium for Justice Information and Statistics), are partnering with OMG to develop a Unified Modeling Language (UML) Profile for NIEM IEPD. A Request for Proposal (RFP) for developing this UML Profile was submitted to OMG by the Government Domain Task Force for consideration during the June 2011 OMG Technical Meetings in Salt Lake City. The RFP received a very strong response and OMG approved the issuance of the RFP to their community of U.S.-based and international government and private-sector industry membership. The next steps include submission and development of the UML profile, followed by the development of at least one commercial or open source product that will use the new NIEM UML profile.

The goal of this effort is that the standard, which mixes the best of NIEM with that of the UML standard is adopted by industry. Then government will be able to purchase commercial products with standardized information sharing “baked-in” from the start.

Advancing Industry Standards

In May 2011, PM-ISE engaged a multi-partner effort with the NIEM PMO and members of the OMG, a consortium of both industry and government members, to develop a UML profile for NIEM that will further NIEM success and adoption. This UML profile will be an industry standard that will enable NIEM developers to graphically develop models of information sharing across systems, agencies, and levels of government. NIEM’s success and adoption as a consensus standard has led to the recognition that we need better support and integration for NIEM in commercial products, enabling native support for NIEM throughout the Systems Development Life Cycle.

Recently, members of the NIEM community from outside the NIEM PMO—including both for-profit and non-profit organizations—have begun offering data standard development tools, signaling the maturity of NIEM and the formation of a robust market for like tools. The UML profile will specify a standard way of capturing IEPD content and structure in UML, the leading industry standard for modeling supported by dozens of tool vendors and open source projects. When the implementation profile is complete, and has been adopted as a standard by OMG, the NIEM UML Profile will be available for use in any number of UML tools available to the developer community today. NIEM support will be an extension of the existing tools and products, and IEPD developers will be able to use off-the-shelf UML tools to model exchanges and generate NIEM-conformant IEPDs from their models.

The resulting expansion of UML tools will encourage an ever-growing community of developers as they implement interoperable components for responsible information sharing across departments and agencies, across different levels of government, and between government and the private sector. All are welcome to join the efforts. The challenges and opportunities our modern world faces requires such interoperability, since they no longer exist in the domain of just one government department or jurisdiction.

4.4 Identity, Credential and Access Management (ICAM)

Responsible information sharing can occur when partners are able to share the identity of users requesting access to information in a form that is understandable to all partners. ICAM capabilities help with both tagging people in a form that can be recognized, and that can assist with the management of responsible information sharing across partners.

In November 2009, the Identity, Credential, and Access Management Subcommittee (ICAMSC) of the Information Security & Identity Management Committee (ISIMC) released the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Part A. This document provides common segment architecture and associated implementation guidance for use by federal agencies as they continue to invest in FICAM programs. The FICAM segment architecture will serve as an important tool for providing awareness to external mission partners and will drive the development and implementation of interoperable solutions. Part B of the FICAM Roadmap is scheduled for release in August 2011 and will include detailed implementation guidance for departments and agencies.

4.4.1 Implementing Federated Identity Standards into the ISE's Interoperability Efforts

Throughout the last year, ISE partners have participated in various forums addressing ICAM. In order to synchronize efforts, the PM-ISE convened the leaders associated with the multiple logical access related management activities of the Federal Government in May 2011. All leaders agreed to a broad vision of enabling these different identity frameworks to ultimately become aligned across all mission partners to provide the critical foundation for authenticating and appropriately authorizing access to information and systems.

There are at least five ICAM frameworks in use by federal agencies:

- The Federal CIO Council's FICAM Roadmap⁵⁵ and Personal Identity Verification - Interoperable (PIV-I) guidance for unclassified networks;
- The DOJ's and DHS's Global Federated Identity and Privilege Management (GFIPM) standards for unclassified networks and non-federal partners;
- The FBI's Criminal Justice Information Services (CJIS) Division Federated Identification and Management Service (FIMS) for unclassified networks and non-federal partners;
- The Committee on National Security Systems (CNSS) Public Key Infrastructure (PKI) for National Security Systems; and
- The IC's Identity and Access Management (IdAM) effort across all IC networks at all security domains.

Each ICAM framework covers separate communities and separate security domains. The goal in bringing all frameworks together is to achieve interoperability from both a horizontal – spanning all mission partners across a single security domain – and a vertical – spanning across security domains – perspective. Horizontal and vertical ICAM interoperability will eventually support key assured information sharing capabilities such as federated cross domain searching and discoverability, and insider threat detection and prevention. In the near term, the focus is on first achieving horizontal ICAM alignment to support assured information sharing across all mission partners within a security domain. For example, FICAM, GFIPM, FIMS, and IC IdAM at the unclassified level will need to be interoperable to achieve simplified sign-on (SSO) capability for the Assured SBU Interoperability Initiative. Similarly for federal Secret networks, CNSS PKI, IC IdAM at the Secret level, and other existing PKI solutions deployed on Secret networks will need to be aligned to preserve and expand assured intra-network access to mission critical information.

When fully implemented, the ISE's efforts at promoting federated identity, in concert with FICAM, will close identified security gaps in the areas of user identification and authentication, access control, and logging and auditing. These efforts support the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. The transformation of these business processes is vital to the security of the United States.

⁵⁵ http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

National Strategy for Trusted Identities in Cyberspace (NSTIC)

The National Strategy for Trusted Identities in Cyberspace (NSTIC) charts a course for the public and private sectors to collaborate on raising the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions. The NSTIC focuses on ways to establish and maintain trusted digital identities, which are critical for improving the security of online transactions. Online transactions are electronic communications among two or more parties, connected via networks, systems, and computers. Individuals, organizations, hardware, networks, and software are all participants in an online transaction; therefore, each of these may be identified, authenticated, and authorized. Technology and processes for identification (establishing unique digital identities) and authentication (verifying the identity of a user, process, or device) are at the forefront of this Strategy. In addition, the Strategy focuses on ways of providing trusted and validated attributes to enable organizations to make decisions about authorization (approving or giving consent for access benefits). Identification, authentication, and authorization provide the information and assurances necessary for the parties within a given transaction to trust each other. The strategy as laid out in the NSTIC is based upon the FICAM Roadmap and is foundational to satisfying the needs of the ISE to provide assured information sharing.

4.4.2 Advancing Attribute Governance and Backend Attribute Exchange (BAE)

A challenge for acceptance and usage of both the PIV and PIV-I credentials is how to make authentication decisions based on attributes of an individual user to allow access to information that is not held within the home organization- essentially, how can an organization verify the that an individual from an outside entity meets the required criteria to access their information. Attributes can be an affiliation with an organization, a role within that organization, specific training or certification, as well as information about the operating environment.

The BAE standard and service is intended to satisfy the enterprise-wide need to verify attributes: providing for the exchange of information between an Attribute Authority (i.e., the information's authoritative source) and a Relying Party (RP) to make access decisions. The RP requests specific attributes of the individual who is trying to obtain information. The Attribute Authority responds, returning requested information as appropriate. The RP uses the returned information as necessary to make authorization decisions.

In partnership, PM-ISE and U. S. General Services Administration (GSA) are leading the effort to develop a business case and life-cycle sustainment analysis which will fully develop the need for the BAE and outreach to stakeholders to gauge their level of involvement and document their commitment of support. This analysis will also include the development of attribute governance and a sustainability plan for the BAE.

4.5 Security, Auditing and Cross-Domain Frameworks

World events—starting with 9/11, continuing through the WikiLeaks disclosures, and most recently culminating in the take down of Osama bin Laden—have generated a number of questions related to the appropriate relationship between information security and information sharing. Information security and assurance helps partners manage connections between what data people are allowed to access and share, in a way that promotes responsible information sharing across partners.

Some world events have been characterized as evidence of the limits of safe information sharing, while others have been highlighted as positive examples. These questions and the continuing tension between sharing and protection illustrate the complexity of the situation mission partners collectively face in developing the ISE. This complexity cannot be simply described as an inverse relationship between sharing and protection; rather, it is a more nuanced relationship of appropriate calibration between sharing and protection aimed at effectively managing the risks associated with both.

In March 2011, ISE leaders from the State Department, DoD, the Office of the Director of National Intelligence (ODNI) and PM-ISE, testified before the Senate Homeland Security and Governmental Affairs Committee hearing, “Information Sharing in the Era of WikiLeaks: Balancing Collaboration and Security.” As the WikiLeaks story evolved over the past year, many voiced concerns that information sharing would suffer a setback. This hearing presented an opportunity to discuss the root causes as well as our efforts to accelerate and strengthen both information sharing and information security.

IRTPA recognized the complex relationship between information sharing and protection in its description of the characteristics associated with the ISE. Half of the fifteen characteristics identified as crucial for the ISE include elements of information protection – a clear recognition that protection and sharing are indivisible aspects of the ISE. Assured and responsible information sharing continues to be the overarching goal of the ISE.

4.5.1 Securely Sharing Classified Information with State, Local, Tribal, and Private-Sector (SLTPS) Partners

The need to share actionable and relevant classified information with SLTPS partners in support of homeland security is evident. Equally evident is the need for a unified, consistent program for the application of standardized security procedures for security clearance management and the safeguarding of classified information across the executive branch and in support of classified information sharing efforts with our partners in the SLTPS communities.

In August 2010, the President issued Executive Order (EO) 13549 to all federal departments and agencies, establishing the Classified National Security Information Program designed to safeguard and govern access to classified national security information shared by the Federal Government with SLTPS entities.

In August 2010, the President released EO 13549, “Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities,” designed to safeguard and govern access to classified national security information shared by the Federal Government with SLTPS entities.

This EO establishes a governance and oversight structure that will serve to ensure the uniform application of security standards within the executive branch and SLTPS communities while maintaining consistency with existing national policy and standards.⁵⁶ The EO also called for the establishment of the SLTPS Policy Advisory Committee (PAC) to discuss the program-related policy issues in dispute in order to facilitate their resolution. They will also recommend changes to policies and procedures that are designed to remove undue impediments to the sharing of information under the Program. The SLTPS PAC conducted its initial meeting on 11 January 2011.

The EO designated the Secretary of Homeland Security as the Executive Agent (EA) for the program. The Secretary subsequently assigned responsibility for the execution of the EO and the implementation, management, and oversight of the program to the DHS Office of the Chief Security Officer (OCSO). The OCSO is completing work with interagency and SLTPS partners to develop the implementing directive that will establish a governance and oversight structure to instill and promote the uniform application of security standards within the executive branch and SLTPS communities consistent with existing policies and standards.

In the coming months, the EA, in collaboration with other federal agencies and the SLTPS PAC, will work to fully implement the requirements of the EO. Among the efforts that will be addressed are the development of systems that are able to document and track the final status of security clearances and to maintain security implementation profiles of SLT facilities that have access to classified information and the development of an SLTPS Security Awareness and Training for program.

4.5.2 Policy and Procedural Framework for Security Reciprocity

Security reciprocity is an important means for developing a consistent, transparent approach to security that minimizes administrative burdens and cost for all mission partners. Through harmonizing the standards and processes used for security clearances for personnel, facilities security, and information technology systems security, mission partners can better understand the security measures used by one another, make well-informed risk management decisions, and achieve predictable security outcomes. Consistency and transparency in turn generate the trust that enables mission partners to accept the security determinations of one another and to minimize the administrative burden of re-examining security measures taken by others.

Significant progress in the area of security reciprocity continued over the past year as evidenced by continued promulgation of harmonized National Institute for Standards and Technology (NIST)-Committee on National Security Systems (CNSS)-Intelligence Community Directive (ICD) standards. These improvements are laying the foundation for an assured information sharing ecosystem among federal departments and agencies; state, local and tribal mission partners; private-sector owners of critical infrastructure; and international partners. At present, 9 out of 14 ISE departments and agencies responding to the 2011 ISE Performance Assessment have documented policies and/or implementation

⁵⁶ Executive Order (EO) 13526, "Classified National Security Information;" EO 12968, "Access to Classified Information;" EO 13467, "Reforming Processes Related to Suitability for Government, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;" and EO 12829, as amended, "National Industrial Security Program."

guidelines on IT security reciprocity, stating the conditions under which they will accept the security certification and/or accreditation of another organization.

Progress has also continued with regard to developing the policy and procedural framework for reciprocity for information systems security. Building on the key milestone achieved in 2009, the harmonization of security standards between national security and non-national systems security standards represented by the publication of the NIST Special Publication 800-53 Revision 3 and the CNSS Policy 1253 – NIST’s Joint Task Force Transformation Initiative continued its groundbreaking work to publish a suite of jointly-coordinated security standards. The suite of five IT systems security standards, shown in Table 4, will form a de facto common security standards baseline for all federal information systems.

NIST Special Publication	Date	Title
SP-800-30	July 2002	Risk Management Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
SP 800-53 Rev. 3	August 2009	Recommended Security Controls for Federal Information Systems and Organizations (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)
SP 800-37 Rev. 1	February 2010	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)
SP 800-53 A Rev. 1	June 2010	Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans (http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf)
SP 800-39	March 2011	Managing Information Security Risk: Organization, Mission, and Information System View (http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf)

Table 4. Key Publications Supporting Reciprocity, by Date of Release

Although individual organizations must tailor these standards to their specific operational environment, the harmonization among standards issued by NIST, DoD, and the IC lays a common foundation that will enable all federal agencies to reciprocally accept one another’s security testing results. This alignment will in turn enable state, local, and tribal mission partners to meet a common set of security requirements for interconnecting with federal systems, and significantly reduce the time and cost associated with practicing assured information sharing. Alignment of IT systems security standards across all federal communities will also facilitate responsible information sharing capabilities that operate horizontally across networks and vertically across security domains.

NIST Leads Effort to Harmonize Security Standards

The National Institute of Standards and Technology (NIST), an agency under the Department of Commerce (DOC), continued to lead the interagency effort to harmonize security standards among federal civilian agencies, DoD, and the IC, and published two additional security standards in the past 12 months. These harmonized standards represent the beginning of a single coordinated federal baseline for information systems security that will enable security reciprocity among federal mission partners, and will also enable reciprocity to be extended to non-federal partners such as fusion centers.

NIST also created the program management office for the National Strategy for Trusted Identities in Cyberspace (NSTIC) in April 2011. This strategy, which is aligned with key existing federal identity management efforts, will provide an important framework to enable interoperable identity management solutions among federal and non-federal mission partners, including state, local, and tribal governments and private-sector partners.

4.5.3 Information Assurance and Auditing

Generating records of individual activities on networks and in handling information provides an important part of the overall function that is information assurance. When individual users understand that their actions are being monitored, they are more likely to be vigilant in avoiding mistakes; they are also more likely to think twice about committing acts of deliberate malfeasance. Audit data and the analysis of patterns of use also constitute the means of predicting and detecting security problems as they occur.

However, to be useful in its role in information assurance, audit data must be shared effectively both vertically and horizontally. To assemble a comprehensive picture of data use, audit data covering activities on different networks and systems must be shared among mission partners. But audit data must also be shared or aggregated vertically across security domains to achieve a complete picture of use. Consequently, audit data present a uniquely broad challenge for information sharing.

Through the use of common standards for capturing audit data, and interoperable processes for aggregating it across networks and security domains, the complete picture of use becomes an achievable goal. The ISE, and the tools it employs to enable assured information sharing, is the optimal ecosystem for supporting an effective audit function.

In the past year, the IC has made progress in harmonizing audit data and procedures. Recently promulgated IC standards implement uniform information security requirements and procedures concerning audit information in the IC information environment, and address the use of collected audit

data for insider threat detection. These standards enable the capture and analysis of user activities to protect sensitive information, promote interoperability and efficiency, support identification of threats, and promote effective information sharing. The IC's experience in audit functions presents an opportunity for leveraging best practices for other federal, state, and local networks to improve the overall assurance of the ISE.

4.5.4 Information Sharing Across Security Domains

Security reciprocity and the use of common security standards and implementation profiles also support key ISE capabilities such as federated searching and the aggregation of audit data. In the future, security reciprocity and common standards will support capabilities that span horizontally across different networks at the same classification level, as well as capabilities that operate vertically across security classification domains, where appropriate. The ability to provide capabilities that cross security domains is necessary for certain functions, such as auditing (as previously noted), and it enables significant efficiencies for users in functions such as federated searching.

For example, an authorized individual operating on a classified domain should be able to search across both classified networks and unclassified networks. Inversely an individual operating only an unclassified domain may not see the classified results of a search; nevertheless, the search and discovery processes can trigger a notification to authorized individuals at the classified domain regarding interest from the unclassified domain for information. In the future, such a notification may then trigger actions to make some form of the classified information available to the unclassified domain. By achieving cross-domain federated search and information discovery, the ISE empowers members to find information actively and to have timely, relevant, and accurate information to find them. In both cases, use of interoperable security standards, privacy standards, and identity standards are a necessary condition to enable cross-domain functions.

4.5.5 Guiding Departments and Agencies

As part of previous efforts to establish the ISE through structural standardization, an Enterprise Architecture Framework was released in 2008 and continues to be utilized by many agencies. Sharing information in an electronic world requires agreement on the structures, policies, processes, and protocols under which sharing takes place. This is especially important in a distributed, decentralized environment like the ISE, where sharing takes place across a vast array of information technology systems and networks. This framework provided specific guidance to ensure that information technology investments are driven by the need for interconnectedness, interoperability, and seamless information sharing and collaboration. Its concepts and principles have been incorporated into OMB's Federal Segment Architecture Methodology (FSAM) as a best practice and are being adopted by other government-wide information sharing initiatives, such as the Next Generation Aviation Transportation System, the Maritime Domain Awareness Initiative, and the Federal Health ISE.

Adherence to ISE concepts has proven beneficial to members of the ISE community, to include ISE's broad guidance and recommendations to departments and agencies resulting in:

- Seven of 14 responding ISE departments and agencies applying Enterprise Architecture transition plans at key decision points in the investment cycle;
- Eleven of 14 responding ISE departments and agencies mapping at least one IT investment to its information sharing segment architecture, a 14% increase from 2010;
- Eight of 14 responding ISE departments and agencies representing all major ISE IT investments in their enterprise transition plans, a 7% increase from 2010; and,
- Five of 14 responding ISE departments and agencies including at least one information sharing measurement indicator for FY 2010 in Section E Performance Information table (Table I.E.1) of their annual OMB Exhibit 300s for ISE investments.

As the ISE continues to develop and move forward, a roadmap will continue to accelerate the provision of guidance and recommendations to departments and agencies, to focusing on standards adoption, industry engagement, and strategic sourcing across all levels of government.

Information Sharing and Protection Challenges and Opportunities

As the WikiLeaks story emerged, concerns were voiced that information sharing would suffer a setback. The guidance throughout the Executive Branch has been consistent: we need to accelerate our information sharing in a responsible and secure way. While complex and challenging, the imperatives to share and protect are not in conflict. In fact, as our information protection measures mature, are accepted by more and more mission partners, and become more and more transparent – our trust of one another’s practices and security controls will result in increased reciprocal acceptance of information systems certification and accreditation, Identity, Credential, and Access Management, and audit procedures. In this new trusted environment, information sharing is facilitated by the very protections put in place to prevent another WikiLeaks-type incident.

We do not yet enjoy the benefits of the trusted environment described above and the challenges highlighted by the WikiLeaks breach are complex and go to deeply rooted issues:

- Our legacy of agency-based, bi-lateral, and fragmented rather than common, consistent, transparent, and comprehensive solutions for trusted, assured information sharing and protection;
- Our inconsistent and uneven counterintelligence posture against the insider threat and related technical considerations;
- Our inclination to fix the surface-level problem, namely our focus on securing the specific classified network involved, while ignoring the fact that the challenge of sharing information in a secure manner applies to and spans all security domains.

A *whole of government approach* is necessary to effectively address these issues in a robust way. We cannot hope to build a truly trusted ISE without addressing the concerns and mitigating the risks of all ISE mission partners.

In addition, the ISE is mandated to address terrorism, homeland security, and weapons of mass destruction information regardless of classification. Fundamental policies and solutions must be framed to address all types of protected information, *classified and unclassified*, held by the Federal Government and by our state, local, and tribal partners, as our critical national and homeland security issues cut across security domains.

Finally, a strong and broadly applied *governance, strategy, and policy framework* is foundational to improving information sharing and protection. We can achieve the trusted environment that we want, but every entity that has an ISE equity must have a seat at the table and be incorporated into the strategic vision from the outset.

The ISE has, since its inception, focused on information sharing in a responsible and assured manner. The risk of future WikiLeaks-like incidents can be reduced; but, fixing these government-wide challenges is complex, difficult, and requires sustained commitment. To share and protect information effectively, we must work to find what the DNI has termed the “sweet spot” between these critical imperatives.

5 Enabling Assured Interoperability Across Networks

The Information Integration Sub-Committee (IISC) of the Information Sharing and Access Interagency Policy Committee (ISA IPC) coordinates high-priority interagency efforts to accelerate the delivery of the ISE, including interoperability among Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI) and Secret networks, identification of best practices in support of data aggregation⁵⁷ activities, and advancement of industry-based standards in support of all ISE activities, as discussed in Chapter 4. The IISC also ensures that both federal and non-federal partners (e.g., fusion centers, state and local law enforcement activities, and public safety endeavors) have appropriate input in guiding and implementing shared information integration capabilities, policies, and processes that satisfy their mission needs. The 2011 Annual Performance Assessment indicates there are opportunities for improving information integration across the interagency. For example, only five of 14 responding ISE departments and agencies have a plan for implementing interconnection capability for sharing terrorism and homeland security information across SBU/CUI networks.

The IISC accomplishes this mission through its Working Groups by coordinating functional and technical standards, interoperability, data methods, and other responsible information sharing efforts harmonizing governance, policy, and investments across agencies and departments. These efforts are further discussed in the sub-sections below.

5.1 Data Aggregation

The mission to disrupt terrorist acts before they occur is enabled by finding, sharing and collaborating on data that comes from trusted and reliable mission partners. Mission partners are continually producing and consuming data from a wide variety of sources. The goals of data aggregation in the ISE are achieved through an established governance process that enables mission partners to obtain the data, through shared ISE enterprise services, that is necessary to perform their missions while protecting the privacy of persons for whom no nexus to terrorism exists. Key to enabling the access and dissemination of aggregated data within the ISE will be the capability to authenticate users across the environment. Through positive user authentication, logging of data access, and auditing of data trails, the risks associated with the sharing of aggregated data are mitigated.

Under the joint leadership of Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI), the Data Aggregation Working Group (DAWG) was formally approved and chartered by the IISC to focus on capabilities that are entity (identity)-focused, and to employ automated data discovery, data characterization, data correlation, and disambiguation algorithms to

⁵⁷ Data aggregation refers to the collection of processes, policies, procedures, and technologies that allows for the detection of relationships between people, places, things and characteristics, linking information across organizations and helping analysts to identify the connections between data that are not obviously related.

aggregate information from multiple domains into a mission-specific enterprise-level analytic service. The objectives of the DAWG are to:

1. Provide a forum for sharing best practices, developing enterprise solutions, reviewing architectures, and resolving interagency issues related to data aggregation.
2. Explore options and provide recommendations to the IISC for implementing data aggregation approaches as part of the broader ISE.
3. Provide a forum for linking National Security-related matters with federal information technology, information systems, and architectural guidance as they relate to the data aggregation.
4. Evaluate options and provide recommendations to the IISC for enabling cross security domain search, discovery, and retrieval in aggregated data sets.
5. Serve as a technical forum of federal-wide engagement for assessing and providing recommendations to the IISC on the optimization of data-related processes, standards, and architectures that lead to data aggregation capabilities in support of non-traditional screening for terrorism.
6. Remain in synchronization with the Privacy and Civil Liberties Sub-Committee of the ISA IPC so that technical, policy, standards, and privacy issues related to data aggregation are consistent across multiple security domains.

The mission of the ISE is to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information to enhance national security and to help keep our people and our institutions safe. Under the joint leadership of DHS and ODNI, the Data Aggregation Working Group is identifying and characterizing systems and programs that aggregate ISE data.

The Working Group envisions the ISE as an enterprise and applies enterprise data management principles to precisely define, easily integrate, and effectively retrieve data for both internal applications and external communications and sharing. This approach supports a more flexible ISE with lower costs by leveraging partner systems and applications and data for re-use and re-purposing through aggregation.

Since its creation, the DAWG has completed a review of the U.S. Government oversight and governance structures that provide strategic policy, technical and mission guidance for terrorism-related data aggregation, data integration, and data management efforts. To complete its tasking from the IISC, the Working Group has created questionnaires and survey tools to:

- Develop an accurate inventory of programs that perform counterterrorism data aggregation across the U.S. Government. The goal of the inventory is to increase efficiencies by sharing best practices, lessons learned, and architectures for data aggregation programs with interagency partners;
- Increase information sharing by cataloging data sources (highly valued/consumed data) in a way that highlights technical and policy issues related to data sharing; and

- Identify best practices and architectures and make recommendations on moving forward and to set the standards by which next generation data aggregation systems are built across the U.S. Government.

As the DAWG identifies best practices and lessons learned, it is expected that mature technical solutions will be identified that can be shared across the ISE. The DAWG is collaborating with the Privacy and Civil Liberties sub-committee of the ISA IPC to identify legal and/or policy protection constraints over data discovery, access, ingestion, use, and retention for person-centric data. The group is also working with other joint agency teams and the working groups under the Watchlisting and Screening sub-committee of the ISA IPC to ensure that business processes and best practices can be leveraged.

Finally, as a complete picture of data aggregation efforts across the U.S. Government is completed, overlaps and/or gaps in analytic responsibilities and information sharing among the ISE agencies will be identified, and business practices that bridge or close the gaps in the counterterrorism (CT) mission will be proposed and implemented.

5.2 Assured Secret Network Interoperability

The ability to effectively and responsibly share classified information among federal and non-federal mission partners is a key capability needed to support the CT mission and overall homeland security. However, federal Secret networks were not built with information sharing capabilities in mind, and the cross-departmental governance structures to coordinate functions that would support assured sharing across all federal Secret networks—that is, to manage federal Secret networks as an enterprise—have not previously existed. This coordination is necessary to ensure that classified information can be shared consistently and predictably with the appropriate level of assurance – not only among federal departments and agencies, but also between the Federal Government and key mission partners, such as fusion centers.

In April 2010, PM-ISE completed a study of the current state of federal Secret network connectivity and accessibility by non-federal partners. The study identified the need for consistent processes for planning and coordinating implementation of assured information sharing capabilities across the Federal Secret Fabric, and the need for a cross-federal governance body in which to hold such discussions. Based on these recommendations, in 2010 the ISA IPC chartered the Assured Secret Network Interoperability Working Group (ASNI WG) to serve as a forum for federal agencies operating Secret networks to work together to develop enterprise governance for the Federal Secret Fabric, to resolve interoperability issues, and to support assured information sharing among federal Secret networks. A particular focus of the ASNI WG is to develop efficient and assured information sharing between Federal mission partners and fusion centers.

The goal of the ASNI WG is to coordinate and facilitate interoperability between Secret systems—through establishing effective governance and harmonizing standards, policy, and technology—in order to ensure effective and efficient enablement of national security missions. In doing so, the ASNI WG partners with other existing working groups and advises the ISA IPC on all issues that require, or would be most effectively addressed by, coordination across multiple departments and agencies related to the secure sharing of information through the interconnection of federal Secret-level computing environments. DHS currently chairs the ASNI WG.

Over the past nine months, the interagency ASNI WG has delivered a number of key incremental accomplishments towards increasing interoperability and information sharing among federal Secret networks and between federal Secret networks and fusion centers.

In 2010, the ASNI WG identified a requirement to better understand fusion center information needs in order to ensure an appropriate basis for coordinated network connectivity and access. A joint interagency team, representing a partnership between the Fusion Center Sub-Committee and the ASNI WG, conducted a study in the spring of 2011 that drew upon data gathered from existing fusion center reports as well as discussions with key analytic personnel. These information needs were aligned to the Homeland Security Standing Information Needs (HSEC SINS), further supporting the ability of federal, state, local and tribal partners to use a common lexicon as they engage in information sharing activities.

In 2011, the Assured Secret Network Interoperability Working Group partnered with the Fusion Center Sub-Committee of the ISA IPC to document, validate, and prioritize information requirements. This establishes the foundational requirements needed to inform the development of technical connectivity and access to sensitive information for fusion centers.

Documenting fusion center information needs will help in communicating these needs to federal mission partners and application owners and will inform the technical access and connectivity solutions that are being developed by the Federal Government in order to securely share information with fusion centers. The results of this study were also shared with the DAWG and the Assured SBU/CUI Interoperability Working Group.

The ASNI WG also supported demonstrated progress on mission capabilities on Secret networks for fusion centers, which were announced at the 2011 Fusion Center Conference. These capabilities included: improved access to white-listed sites on DoD's Secret network (SIPRNet) via DHS's Homeland Secure Data Network (HSDN); preserved and expanded fusion center access via HSDN to *NCTC CURRENT* during its relocation to SIPRNet; expanded Secret-level video-conferencing capabilities as a shared service between the FBI's Secret network and HSDN for fusion centers; and new access to the FBI's white pages and email directories through HSDN.

The ASNI WG also made progress toward several goals related to interoperability and governance of the Federal Secret Fabric. ASNI WG completed an initial study of DHS's authorities related to Secret network access provisioning and coordination for non-Title 10 and non-Title-50 organizations. The Working Group developed and began administering a survey to federal Secret networks to develop a body of information around network characteristics that impact information sharing. Finally, the Working Group began a study of the impacts on information sharing resulting from new security controls implemented after the WikiLeaks disclosures, raising awareness among the information sharing community of potential mission impacts.

Over the coming year, the ASNI WG will continue its work to improve coordinated classified connectivity and access, and to improve information sharing with fusion centers. It will also continue to develop governance among all Secret network stakeholders toward the overall goal of coordinating the Federal Secret Fabric to support assured information sharing. Key activities that will support this goal include completing work on developing a current picture of Secret network characteristics that support

information sharing; developing an end-state vision for protected sharing; and prioritizing gaps between the two, based on fusion center mission-based requirements for information and other use cases. The ASNI WG will also continue to strengthen linkages and to leverage activities between other coordination bodies related to Secret networks, such as the Committee on National Security Systems. Finally, the ANSI WG will monitor the impact of new WikiLeaks-related security measures on information sharing and will coordinate among member agencies to ensure that information security and information sharing on the Federal Secret Fabric increase in tandem.

Multi-Agency Collaboration Environment (MACE)

The Multi-Agency Collaboration Environment (MACE) develops interagency alliances of partners to demonstrate the power of data sharing within a common enterprise architecture. MACE and PM-ISE, in coordination with federal, state, local, and tribal entities, are sponsoring a pilot effort to demonstrate the value of interagency data sharing to disrupt the financial networks used to support threats to our national security, our economic interests, and our allies. Participating organizations will work together to facilitate information discovery, planning, and the execution of operations across departmental and agency boundaries. The impact of integrating architectures, data, and technology on operations, tactics, techniques, and procedures will also be analyzed. This pilot will act as a catalyst to accelerate the interoperability, policy, and security advancements needed to meet the challenges that will be encountered by our nation in the coming years.

5.3 Assured Sensitive But Unclassified (SBU) Network Interoperability

In the spring of 2010, PM-ISE conducted a user requirements survey with thousands of SBU system users. Those users identified that there are multiple SBU/CUI networks, portals, and systems currently in existence containing a rich variety of data and services that they regard as essential for doing their jobs. However, differences in policy and technology prevent authorized users from gaining access to many of those resources without having to individually log on to multiple systems using separate sets of credentials. System users stated that the ability to reduce the number of credentials needed to access SBU/CUI systems was their most desired requirement. Specifically, the overarching requirement is to provide federal, state, local and tribal law enforcement officers and analysts with the ability to log in just once to an approved system that would grant users access to an interoperable and protected SBU/CUI environment. Commonly referred to as Simplified Sign On (SSO) and branded by the SBU partnership as the “no wrong door” concept, achieving this capability has been identified by operators and analysts a top priority.

The SBU/CUI interoperability initiative has been in existence since 2007. To formalize this effort, the group was renamed the Assured SBU Network Interoperability Working Group, and it was brought under the Information Integration Sub-Committee of the ISA IPC. The Working Group (aka “SBU Partners”) is composed of representatives of four systems listed in Table 5. The goal of the Working Group is to coordinate and facilitate interoperability between SBU/CUI systems through efficient governance and establishment of standards. Reaching consensus on the standards and architecture

needed to achieve interoperability between these four key SBU/CUI systems will lead the way for interoperability between a broader set of SBU/CUI systems.

In February 2011, an ISA IPC meeting was held with senior interagency leaders to gather support to move quickly in addressing the SBU challenge. One recommendation was to have an SBU partner lead the SBU Working Group. Given the RISS program's long standing efforts to expand information sharing among federal, state, local, and tribal partners, it was decided that RISS would be the first partner to lead the group to ensure that the SBU effort continues its forward progress. PM-ISE will continue to support RISS in facilitating the agenda, objectives and meetings for the Working Group.

Law Enforcement Online (LEO)	Law Enforcement Online (LEO) is a state-of-the-art Internet system that is accredited and approved by the FBI's Criminal Justice Information Services (CJIS) for SBU/CUI information. LEO is used to support investigative operations, send notifications and alerts, and provide an avenue for remotely accessing other law enforcement and intelligence systems and resources. LEO provides all levels of the law enforcement, criminal justice, and public safety communities virtual private network access to its "anytime and anywhere" system for secure electronic communications, online training, and information sharing.
Intelink-U	Intelink-U and related services provide robust information sharing and collaboration capabilities for the IC and its national defense (U.S., allied, and coalition partners), homeland security, foreign relations, and law enforcement partners. The Intelink Enterprise Collaboration Center provides, in all three security domains, the operational means to deliver enabling services supporting the objectives of the National Intelligence Strategy. These community level services include: search, discovery, and delivery services (e.g., web-based content search, content indexing, personalized and group subscriptions, customer support); collaboration tools and services (e.g., email, chat, instant messaging, forums, wikis, blogs); web-based content and hosting in Community Shared Spaces; analytical support in the use Intelink resources; infrastructure services (e.g., mail relay, directory services, cross-domain platforms, public key infrastructure (PKI) certificates) and network management, monitoring and control. In the SBU/CUI realm Intelink services are accessible to more than two million users through existing interconnections and partnerships.
Homeland Security Information Network (HSIN)	HSIN, hosted by DHS, is a secure, web-based platform that enables SBU/CUI information sharing and collaboration capabilities among state, local, territorial, tribal, private sector, and international partners, and the Federal Government. HSIN supports several Communities of Interest in Law Enforcement, Intelligence, Emergency Management, Defense, and Critical Sectors.
Regional Information Sharing System Secure Intranet (RISSNET)	Regional Information Sharing Systems (RISS) is a nationwide information sharing and investigative support program that provides secure communications and investigative services to thousands of local, state, federal, and tribal law enforcement, criminal justice, and public safety agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, England, and New Zealand. RISS consists of six regional centers that serve the needs of their individual regions while working together on nationwide efforts. It offers diverse and unique services, facilitates rapid exchange of information, and provides secure, nationwide information and intelligence sharing capabilities through its secure Intranet, known as RISSNET. RISSNET has more than 60 partner agencies that leverage RISSNET through node connections to provide secure remote access to resources within their agencies.

Table 5. The Four SBU/CUI Partner Systems

5.3.1 Simplified Sign On (SSO)

Over the past year, the Assured SBU Network Interoperability Working Group has made significant progress towards achieving SSO. In December 2010, FBI's CJIS Trusted Broker Version Two became

PM-ISE hosted a Simplified Sign On (SSO) Technical Forum allowing SBU partners and experts to define the technical plan for federated SSO. Three SBU partners (Federal Bureau of Investigation's [FBI] Law Enforcement Online, RISS Secure Intranet [RISSNET], and Director of National Intelligence's [DNI] Intelink-U) have enabled simplified sign-on using the FBI's Criminal Justice Information Services' Trusted Broker.

operational, providing SSO capabilities by allowing LEO users to access Intelink-U, RISSNET, and many other systems that are not yet part of the SBU partnership. In addition, the CJIS Trusted Broker allows RISSNET users to access the Joint Automated Booking System (JABS) and Intelink-U without having to obtain separate accounts. In March 2011, RISSNET achieved interoperability with the Pennsylvania Justice Network via the National Information Exchange Federation (NIEF) mechanism, enabling SSO for users of those two systems. Also, as a prerequisite for SSO, HSIN successfully tested Identity Provider (IP) and Service Provider (SP) capabilities, with RISSNET complying with the Global Federated Identity and Privilege Management (GFIPM) reference federation. In order to illustrate SSO capabilities and communicate these accomplishments to leadership and the SBU user base, the partnership produced a series of demonstration videos illustrating specific SSO use-cases. Over the next year, the partnership

will continue to release additional videos that will demonstrate the services that are made available through the SBU/CUI effort.

5.3.2 Measuring SBU Progress

The Assured SBU Network Interoperability Working Group tracks the effectiveness of their efforts by monitoring a set of user metrics that are consistently collected from all partners on a monthly basis. These metrics have been designed by the SBU partnership to indicate progress towards the group's interoperability goals and to assist in fine-tuning particular interoperability efforts. Specifically, all partners report metrics on the total and external usage of their top services, such as web portals, document repositories, or instant messaging systems. External usage indicates user activity originating from one of the other three partners. Additionally, partners report the number of unique registered users each quarter (see Figure 11). This metrics collection effort has proven a valuable tool for fine-tuning SBU interoperability efforts and will continue to evolve as the SBU partnership adds additional participants in the future.

Unique Registered Users by SBU System

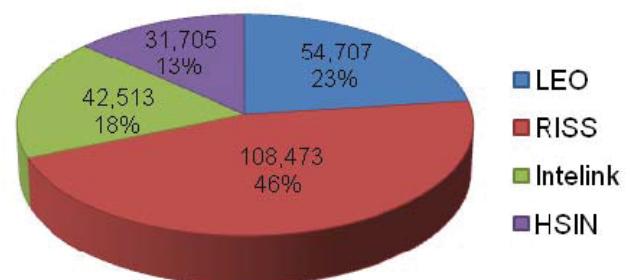


Figure 11. Unique Registered Users by SBU System

5.3.3 Future Plans

The SBU partnership has set goals for the coming fiscal year that are designed to further enhance interoperability among the partner systems. The group will continue to add IPs and SPs and to expand the user base that has access to an SSO capability. The group will also be focusing on other key capabilities, such as cross-partner federated search, discovery, and retrieval. In the 2010 SBU User Requirements Survey, the search capability was the second-most requested requirement, after SSO. The Working Group plans to demonstrate cross-partner federated search, discovery, and retrieval through a pilot before the end of fiscal year 2011. Finally, the SBU partnership intends to work to standardize system security practices to include user account vetting, user account de-provisioning, and system certification and accreditation reciprocity.

New HSIN COI Goes Operational on New Year's Eve in Times Square

Every year on New Year's Eve, approximately one million people gather in New York City's Times Square. Keeping them safe is the job of thousands of police officers, emergency service squads, drug and bomb-sniffing canine units, and counterterrorism personnel. As 2011 approached, New York's Mayor Bloomberg ordered the implementation of an information sharing program to connect the metropolis's 44 agencies, including six federal, 10 New York/New Jersey state, and 28 local agencies. In response, HSIN stood up the New York City Office of Emergency Management Community of Interest (COI) to connect the various citywide command posts of the New York City Office of Emergency Management and the Fire Department of New York. The COI went operational for the first time on New Year's Eve 2010, merging all the various emergency, law enforcement, and federal personnel, and feeding them up-to-the-minute information. It marked the first time an information sharing operation of this size and breadth has been conducted in the nation's largest metropolitan area.

HSIN Storms the Hill

The Legislative Branch Emergency Planners Group, composed of such elements as the United States House of Representatives, the United States Senate, the Capitol Police, the Architect of the Capitol, the Library of Congress, and many others, has adopted HSIN as their new command, control, and communications platform. They did so in order to increase situational awareness across three primary areas: exercises, general events (daily member movements) and special events (Presidential inaugurations, State dinners, State of the Union addresses, etc.). The site sponsor, the Office of the United States Senate Sergeant at Arms, was also interested in a centralized platform capable of coordinating information and manpower during emergencies such as the Capitol has faced in the past—gunmen on the grounds, anthrax mailings, etc. HSIN is now being used to compliment the emergency operations for 50 core users at the United States Capitol complex.

LEO Performance

- Approximately 54,700 active vetted users
 - Approximately 41,700 unique users log in per quarter
 - More than 960 Virtual Command Centers (VCC)
 - More than 1,100 Special Interest Groups created
 - An average of 28 new VCCs per user request activated monthly
-

5.3.4 Controlled Unclassified Information (CUI)

While interoperability between networks, systems, and data is critical to enabling information sharing among different partners, the imperative to achieve interoperability also applies to the rules by which information is marked. Historically, executive departments and agencies have employed ad-hoc, agency-specific policies, procedures, and markings to safeguard and control the dissemination of SBU information. As a result, there are more than 100 different policies and markings for handling such information across the Executive Branch. This inefficient, confusing patchwork system has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing.

On 4 November 2010, President Obama signed Executive Order (EO) 13556 “Controlled Unclassified Information,”⁵⁸ establishing a CUI program to manage all unclassified information that requires

In November 2010, the President released Executive Order 13556 “Controlled Unclassified Information,” establishing a CUI program to manage all unclassified information that requires safeguarding and/or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies

safeguarding and/or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. The Order identifies the National Archives and Records Administration (NARA) as the Executive Agent to implement the EO and to oversee department and agency actions to ensure compliance; and NARA established the CUI Office to manage the program. The Order also rescinded the May 2008 terrorism-related memorandum.

The designated bottom-up approach of EO 13556 prescribes an ongoing conversation between the CUI Office, departments and agencies, the private sector, representatives of the public, and state, local and tribal stakeholders to consolidate and standardize an Executive Branch-wide taxonomy and policy for CUI.

58 Executive Order 13556 “Controlled Unclassified Information,” 4 November 2010.

5.3.5 Progress on CUI

Per EO 13556, departments and agencies have reviewed all categories, subcategories, and markings used to designate unclassified information for safeguarding and dissemination controls, and in May 2011, they submitted their proposed categories, subcategories, and markings to the EA for review and approval. All approved CUI terms will be published in the CUI Registry, discussed below.

On 9 June 2011, the CUI Office issued the “Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556.”[1] This guidance applies to agencies that create or handle unclassified information requiring safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, or government-wide policy. During the directive development process, the CUI Office hosted multiple working group meetings and consulted with affected agencies and representatives of the public and private sector, as well as state, local, and tribal partners.

In conjunction with the issuance of Executive Order 13556, the CUI Office comprehensively updated its website to reflect the background, current status, and anticipated future direction of the CUI program. This website can be accessed at <http://www.archives.gov/cui/>. CUI Office staff represented the program at conferences, symposiums, and meetings for various audiences, including federal, state, local, and tribal governments, the private sector, law enforcement, military, academic, and public interest entities.

The CUI Office also produced CUI Awareness and Executive Order 13556 training modules. These computer-based tools are designed for stakeholders at all levels, and are publicly available at <http://www.archives.gov/cui/> for either direct access or download.

5.3.6 The Way Ahead

In the coming months, the CUI Office will lead an interagency process to establish an Executive Branch-wide definition and taxonomy of categories for CUI. After consultation with additional stakeholders and representatives of the public, the EA will create a public registry of all approved CUI terms. This Registry will consist of categories, subcategories, and markings of CUI and their definitions, along with applicable safeguarding, dissemination, and decontrol procedures to increase transparency and ensure consistent application. The CUI Registry will be available on the CUI website beginning November 2011.

Departments and agencies will submit CUI compliance plans to the CUI Office by 6 December 2011. The CUI Office will review and, in consultation with affected agencies and the OMB, will establish deadlines for phased implementation by agencies. Follow-on guidance will be issued as the CUI program and schedule is developed.

Federal agencies are expected to initiate efforts to develop CUI guidance specific to their agency and unique mission requirements. The CUI Office will serve as a resource for departments and agencies to ensure coordination of CUI policy government-wide. Outreach efforts will continue, with increased attention to stakeholder groups that are new to the CUI effort. Additional future progress may include the development of attribute-based rules for CUI information sharing, allowing the integration of the Assured SBU Network Interoperability efforts.

Senior Privacy and Civil Liberties Officers

As technology has changed, Congress has identified the need for empowered leaders to protect privacy, civil rights, and civil liberties (P/CR/CL) around federal agency collection, maintenance, use, sharing, and dissemination of personally identifiable information (PII). DHS was the first department to have both a statutorily-created Chief Privacy Officer and Office for Civil Rights and Civil Liberties under the Homeland Security Act of 2002, as amended (6 U.S.C. 552). In 2005, Congress, through the Violence Against Women and Department of Justice Reauthorization Act of 2005, established the position of Chief Privacy Officer in the Department of Justice. In 2007, amendments to IRTPA through the Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53) firmly established the Congress' expectation that "each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer." As directed by the 9/11 Act, senior privacy and civil liberties officers were appointed at ODNI, DOJ, State, Treasury, DoD and the CIA. In addition, the authorities of existing privacy officers, to include DHS, were enhanced.⁵⁹

Senior privacy and civil liberties officers work across their departments and agencies to ensure compliance with P/CR/CL requirements. P/CR/CL issues do not have "one size fits all" solutions, so these officers must rely upon policy, guidance, and compliance tools to fashion mission-appropriate protections. Using tools such as a Privacy Impact Assessment (PIA)⁶⁰ or a Civil Rights and Civil Liberties Impact Assessment,⁶¹ privacy and civil liberties officers work with program and system managers, developers and administrators to identify data needs and to mitigate risks associated with the collection, use, and maintenance of PII and protected activities. Tools such as a PIA help to ensure that the use of technology does not erode individuals' P/CR/CL. Privacy and civil liberties officers provide training to department and agency personnel on the importance of P/CR/CL protections in day-to-day operations. They also conduct outreach to their mission communities and to the P/CR/CL advocacy community. The ISE has leveraged these relationships with external groups to develop strong protections that are appropriately tailored to activities of the NSI and of fusion centers.

Over the past year, DOJ and DHS have worked to assist state, local, and tribal information partners in building a community of privacy and civil liberties officers within fusion centers. In 2010, the DHS Privacy Office and Office for Civil Rights and Civil Liberties provided core P/CR/CL "Train the Trainer" sessions to 68 fusion center privacy and civil liberties officers. DHS has hosted NSI supervisor training for fusion center analysts, which includes an extensive P/CR/CL protection component.

Going forward, the ISE is working to bridge the federal and state, local, and tribal communities to ensure that privacy and civil liberties officers at all levels of government can identify and address P/CR/CL issues impacting cross-cutting priorities and areas of focus. The ISA IPC Privacy and Civil Liberties Sub-Committee and other ISA IPC governance bodies will be venues for developing strong P/CR/CL protections necessary for cross-government efforts.

59 Most of these officers have extensive experience and hold professional certifications for P/CR/CL.

60 A PIA is a risk management tool for privacy required by the E-government Act of 2002 (Public Law 107-347).

61 DHS's Office for Civil Rights and Civil Liberties conduct Civil Rights and Civil Liberties Impact Assessments to determine whether a DHS program, policy, or activity has an impact on the civil rights or civil liberties of individuals.

6 Enhancing Privacy, Civil Rights, and Civil Liberties Protections

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) aims at the broadest possible sharing of information for counterterrorism purposes, while also explicitly recognizing that such sharing must respect privacy, civil rights, and civil liberties (P/CR/CL). Only by zealously protecting these rights and liberties will we continue to secure the confidence and support of the American people for critical information sharing efforts.⁶² The ISE-based community of federal, state, local, and tribal privacy and civil liberties officers works diligently to ensure that privacy protections are identified and addressed with regard to terrorism information sharing activities. A critical factor in the success of the ISE lies in maintaining the trust of the American people that P/CR/CL is protected as information is shared. Accordingly, the Executive Branch is also working with interested privacy advocacy groups to ensure P/CR/CL are appropriately addressed as part of the WikiLeaks mitigation efforts.

The ISE Privacy Guidelines, approved by the White House in 2006, requires agencies to implement policies and processes to protect P/CR/CL.⁶³ The Guidelines also require federal departments and agencies, as well as non-federal partners, to implement protections that are “at least as comprehensive” as the Guidelines. The Privacy and Civil Liberties Sub-Committee of the Information Sharing and Access Interagency Policy Committee (ISA IPC), the successor of the ISE Privacy Guidelines Committee, serves as a resource for information sharing partners for best practices and tools to implement this protection framework. Over the last several years, additional implementation guidance, which provides detailed direction on ISE privacy policy development and white papers on privacy-related topics, has been developed to support the development of P/CR/CL protection policies.

6.1 Privacy, Civil Rights, and Civil Liberties Protection Policies

A critical step in the safeguarding of P/CR/CL during information sharing activities is the development and adoption of a written P/CR/CL policy that meets the standards of the ISE Privacy Guidelines.

As federal mission partners, PM-ISE, the Department of Justice (DOJ), and the Department of Homeland Security (DHS) have supported the development of ISE privacy protection policies by issuing guidance and providing technical assistance to assist ISE participants in implementing their agency or departmental ISE privacy protection policies. These efforts have helped ISE mission partners achieve consistent and uniform implementation of ISE Privacy Guidelines.

62 See page 27 of the 2007 National Strategy for Information Sharing for the Core Privacy Principles for Protecting Privacy and Other Legal Rights in the Sharing of Information: http://www.ise.gov/sites/default/files/nsis_book_0.pdf

63 Section 1016(d)(2)(A) of IRTPA requires the President to issue guidelines to “protect privacy and civil liberties in the development and use of the ISE.” Presidential Guideline 5, ‘Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment,’ implemented this requirement: <http://www.ise.gov/sites/default/files/guideline%205%20-%20privacy%20rights%20and%20legal%20protections.pdf>

Currently, nine out of 14 ISE departments and agencies have reported that they have developed ISE P/CR/CL protection policies. Federal agencies have also made measurable progress toward implementing these policies by modifying business processes and updating sharing agreements to align with the new policies. For example, the DOJ Deputy Attorney General issued a notification memo to all DOJ component heads outlining their responsibilities under the DOJ ISE Privacy Policy. In addition, eight out of 14 departments and agencies report that they have implemented mechanisms to assist senior privacy and civil liberties officers in verifying compliance with P/CR/CL protection policies, including the

As of 31 March 2011, all operational fusion centers have adopted ISE-consistent privacy policies. These privacy policies will ensure strong privacy protections for state and local partners and the public, and address the protection requirements for participation in the Nationwide SAR Initiative.

department or agency's ISE policy. For example, the DHS Privacy Office, the DHS Office for Civil Rights and Civil Liberties, and the DHS Office of the General Counsel now review all DHS agreements for sharing information with external partners to identify P/CR/CL equities, and to ensure that provisions addressing compliance measures and reviews are included.

State, local, and tribal partners have worked to develop ISE P/CR/CL protection policies that are "at least as comprehensive as" the ISE Privacy Guidelines, a standard prescribed by the Guidelines

as a prerequisite for receiving terrorism information from federal entities. For example, all operational fusion centers were determined to have privacy policies that are "at least as comprehensive as" the ISE Privacy Guidelines. All fusion centers have designated privacy and civil liberties officers who have received core training in P/CR/CL protections from the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office. Additionally, from late 2010 to early 2011, 14 fusion centers conducted the first round of peer-to-peer P/CR/CL compliance reviews using a P/CR/CL compliance verification template issued by GLOBAL and the Criminal Intelligence Coordinating Council (CICC).

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office is working diligently with NSI participants to implement all of the elements of the NSI Privacy Framework⁶⁴, including alignment with the privacy protections of the most current ISE-SAR Functional Standard. As part of the NSI expansion to federal agencies, the Department of the Interior (DOI) SAR Policy Working Group met with FBI personnel and with the DOI Chief Privacy Officer for two days in 2010 to develop the DOI policy for SAR.

64 The protection of P/CR/CL is paramount to the success of the NSI. Given this importance, the NSI has worked with key partners—including the American Civil Liberties Union and other advocacy groups—to develop protections that, when consolidated, make up the NSI Privacy Framework, which is derived from the protection requirements of the ISE Privacy Guidelines and has elements specific to NSI operations.

6.2 Privacy Training and Outreach

ISE mission partners have expanded training efforts to re-enforce and institutionalize P/CR/CL protections. All federal agencies reported that personnel receive training with a specialized privacy and civil liberties protection component at least annually. For example, the DOI trained members at all of their bureaus on P/CR/CL protection responsibilities during three sessions in late 2010.

As departments and agencies move forward with adopting P/CR/CL protections, agencies report an increase in P/CR/CL training for personnel with information sharing responsibilities. Currently, half of all responding ISE departments and agencies reported providing this training to ISE personnel on P/CR/CL protection policies, which is a seven percent improvement from 2010.

Under the auspices of the NSI, over 800,000 law enforcement officers nationwide are being provided the NSI Front Line Officer Training, a critical portion of which emphasizes the relevance of P/CR/CL protections in identifying and documenting suspicious activity. Through the full-day NSI Analytic training course, analysts and supervisory analysts receive extensive training in P/CR/CL protections applicable to the specialized SAR vetting process.

Outreach is central to achieving ISE privacy protections. ISE participants at all levels of government engage with external advocacy groups to demonstrate current protections and to solicit input for enhanced protections. Federal ISE participants are engaged in internal outreach among department and agency personnel. For example, the State Department distributed several cables about commercial data privacy to personnel at overseas posts, providing these posts with relevant background about privacy considerations specific to the host country, and increasing consular awareness and understanding of disparate regional approaches to P/CR/CL protection.

The State Department recently announced a mandatory distance learning course for employees. The purpose of this course is to provide employees with the skills and knowledge necessary to comply with laws and regulations by identifying and protecting personally identifiable information.

In addition, all DHS personnel must take the annual "Culture of Privacy" training, which incorporates the elements of the DHS ISE Privacy and Civil Liberties Protection Policy.

6.3 Privacy & Civil Liberties (P/CL) Sub-Committee

The P/CL Sub-Committee was established under the ISA IPC in September 2010. The P/CL Sub-Committee is the successor to the ISE Privacy Guidelines Committee and serves to advise and support the ISA IPC by addressing national security issues (including homeland security issues) that are necessary to facilitate the sharing of information to enhance the national security of the United States while protecting P/CR/CL. The P/CL Sub-Committee consists of senior privacy and civil liberties officials from all departments and agencies who are represented on the ISA IPC and is governed by an Executive Committee consisting of the senior privacy and civil liberties officials of the ODNI, the DHS, and the DOJ.

Over the past year, the P/CL Sub-Committee has established three working groups: the Privacy and Civil Liberties Legal Issues Working Group, the Privacy and Information Technology Working Group, and the Compliance Review Working Group. The Sub-Committee and its working groups are working on the following projects over the next year, including:

- Examining the ISE Privacy Guidelines and the Key Issues Guidance to identify areas in which P/CR/CL protections should be strengthened, clarified, or supplemented as a result of the implementation experience of ISE mission partners.
- Developing tools and processes for automated P/CR/CL practices within federal ISE departments and agencies, to achieve a more standardized application of principles across federal ISE departments and agencies. This effort will include an assessment of automated compliance review solutions currently in use by federal ISE mission partners to identify effective tools for standardizing and strengthening audit, accountability, and oversight capabilities.
- Developing a compliance review and best practices tool to ensure consistency and standardization as federal ISE participants implement the ISE Privacy Guidelines. Through the compliance review process, each federal ISE agency will evaluate its internal operating policies, processes, and procedures to assess its compliance with all applicable constitutional provisions and laws protecting P/CR/CL in the gathering and collection, use, analysis, retention, destruction, sharing, and disclosure of information.
- Developing and delivering P/CR/CL training for ISE mission partners as needed.

These projects reflect the P/CL Sub-Committee's strategic focus on strengthening and regularizing protections for P/CR/CL via compliance or enforcement mechanisms; harmonizing processes, tools, and terms of agreement; and leveraging capabilities. These efforts will support the work of privacy and civil liberties officers going forward.

7 APPENDIX A — Performance Assessment Data

The tables in this appendix contain selected results from the 2011 ISE Performance Assessment as self-reported by the ISE departments and agencies. The 2011 ISE Performance Assessment represents progress against the 2007 National Strategy for Information Sharing and the results are aligned according to the focus areas of this strategy. The “Highlight” box is used to describe successes relative to 2010 to help demonstrate the progress that continues to be made across the ISE. Please note that the Department of Defense (DoD)/Joint Chiefs of Staff (JCS) represents the responses of two ISE members, thus a “yes” response on this line counts as two yeses.

Personnel Appraisals

Measurement Question	Do all employees that support ISE-related priorities have “information sharing and collaboration” as a component of their performance appraisals?			
2011 Metric	14 out of 14 responding ISE departments and agencies have included “information sharing and collaboration” as a component in performance appraisals of employees supporting ISE-related priorities.			
Agency	2011 Response	Agency	2011 Response	
CIA	Yes	DOJ	Yes	
DHS	Yes	DoS	Yes	
ODNI	Yes	DOT	Yes	
DOC	Yes	FBI	Yes	
DoD/JCS	Yes	HHS	Yes	
DOE	No Response	NCTC	Yes	
DOI	Yes	Treasury	Yes	
2011 Highlight	All departments and agencies report having accomplished this activity—up 14% from 2010.			

Measurement Question	How often do personnel <i>without</i> direct ISE responsibilities have “information sharing and collaboration” as a performance objective?			
2011 Metric	10 out of 14 responding ISE departments and agencies have included “information sharing and collaboration” as a component in performance appraisals of employees without direct ISE responsibilities.			
Agency	2011 Response	Agency	2011 Response	
CIA	Always	DOJ	Never	
DHS	Often	DoS	Always	
ODNI	Always	DOT	Never	
DOC	Sometimes	FBI	Never	
DoD/JCS	Sometimes	HHS	Sometimes	
DOE	No Response	NCTC	Always	
DOI	Often	Treasury	NA	
2011 Highlight	71% of responding ISE departments and agencies are carrying out this activity; 30% have shown improvement since 2010.			

ISE Awareness Training

Measurement Question	Have you implemented any mission-specific training that supports information sharing and collaboration?			
2011 Metric	10 out of 14 responding ISE departments and agencies implemented mission-specific training that supports information sharing and collaboration.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	Yes
DOC	No		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	Over the past year, there has been a 7% increase among responding departments and agencies in the development of ISE mission-specific training.			

Incentives for Information Sharing

Measurement Question	Does your agency offer an award that includes information sharing and collaboration directly or indirectly as criteria?			
2011 Metric	12 out of 14 responding ISE departments and agencies offer (or intend to offer) an award that includes information sharing and collaboration directly or indirectly as criteria.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Under Development
ODNI	Yes		DOT	Yes
DOC	No		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	Yes
2011 Highlight	No change from 2010; 86% of responding departments and agencies offer (or intend to offer) an award that includes information sharing and collaboration directly or indirectly as criteria.			

Measurement Question	Has nomination of candidates for information sharing and collaboration awards increased since it was first offered?			
2011 Metric	6 out of 14 responding ISE departments and agencies indicated an increase in the number of nominations for information sharing and collaboration awards.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	NA		DoS	No
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	No		HHS	No
DOE	No Response		NCTC	Yes
DOI	NA		Treasury	NA
2011 Highlight	43% of responding ISE departments and agencies identified an increase in nominations—doubling the number from 2010.			

Systems Security Practices

Measurement Question	Does your agency have documented policies and/or implementing guidelines on IT security reciprocity stating the conditions under which you will accept the security certification and/or accreditation/authorization of another organization?		
2011 Metric	9 out of 14 responding ISE departments and agencies have documented policies and/or implementation guidelines on IT security reciprocity stating the conditions under which they will accept the security certification and/or accreditation of another organization.		
Agency	2011 Response	Agency	2011 Response
CIA	Yes	DOJ	No
DHS	Yes	DoS	No
ODNI	Yes	DOT	Yes
DOC	No	FBI	No
DoD/JCS	Yes	HHS	No
DOE	No Response	NCTC	Yes
DOI	Yes	Treasury	Yes
2011 Highlight	No change from 2010; 64% report having documented policies and/or implementation guidelines on IT security reciprocity stating the conditions under which they will accept the security certification and/or accreditation of another organization.		

ISE Shared Spaces

Measurement Question	Has your agency incorporated Common Information Sharing Technical Standards into your architectures?		
2011 Metric	9 out of 14 responding ISE departments and agencies have incorporated CISS Technical Standards into their architectures.		
Agency	2011 Response	Agency	2011 Response
CIA	Yes	DOJ	Yes
DHS	Yes	DoS	No
ODNI	Yes	DOT	No
DOC	NA	FBI	Yes
DoD/JCS	Yes	HHS	No
DOE	No Response	NCTC	Yes
DOI	Yes	Treasury	No
2011 Highlight	There has been a 7% increase in the number of departments and agencies indicating that they are including CISS standards.		

Measurement Question	Does your agency reference mission segment architectures (e.g. SAR) in implementing ISE mission business processes?		
2011 Metric	9 out of 14 responding ISE departments and agencies reference mission segment architectures (e.g. SAR) in implementing ISE mission business processes.		
Agency	2011 Response	Agency	2011 Response
CIA	Yes	DOJ	Yes
DHS	Yes	DoS	No
ODNI	Yes	DOT	No
DOC	NA	FBI	Yes
DoD/JCS	Yes	HHS	No
DOE	No Response	NCTC	Yes
DOI	Yes	Treasury	NA
2011 Highlight	Over the past year, 7% more of the responding ISE departments and agencies are referencing mission segment architectures.		

2011 ISE Annual Report to the Congress

Measurement Question	Is your agency able to share terrorism and homeland security information following the ISE Shared Spaces concept?			
2011 Metric	11 out of 14 responding ISE departments and agencies are able to share terrorism and homeland security information following the ISE Shared Spaces concept.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	No		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	No
2011 Highlight	No change from 2010; 79% report the capability to share terrorism and homeland security information through ISE Shared Spaces.			

Measurement Question	Do you see an improvement in your terrorism information sharing processes with other ISE partners by implementing an ISE Shared Space in your organization?			
2011 Metric	11 out of 14 responding ISE departments and agencies see an improvement.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	NA
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	No change from 2010.			

Measurement Question	Has access to terrorism information from ISE partners been improved by utilizing their designated ISE Shared Space?			
2011 Metric	9 out of 14 responding ISE departments and agencies are reporting improvement through use of designated ISE Shared Spaces.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	No
DHS	Yes		DoS	Yes
ODNI	Yes		DOT	Yes
DOC	NA		FBI	No
DoD/JCS	Yes		HHS	NA
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	No change from 2010.			

Privacy Policies

Measurement Question	Has your agency submitted an ISE privacy policy to the Privacy and Civil Liberties Sub-Committee?		
2011 Metric	9 out of 14 responding ISE departments and agencies have developed and implemented an ISE Privacy Policy and submitted it to the Privacy and Civil Liberties Sub-Committee.		
Agency	2011 Response	Agency	2011 Response
CIA	Under Development	DOJ	Yes
DHS	Yes	DoS	Yes
ODNI	Yes	DOT	Under Development
DOC	Under Development	FBI	Yes
DoD/JCS	Yes	HHS	No
DOE	No Response	NCTC	Yes
DOI	Yes	Treasury	Under Development
2011 Highlight	No change from 2010 - 64% of responding ISE departments and agencies have developed and implemented an ISE Privacy Policy and submitted it to the Privacy and Civil Liberties Sub-Committee		

Measurement Question	Have personnel with information sharing responsibilities received training on your agency's privacy and civil liberties policies, to include your agency's ISE Privacy Policy?		
2011 Metric	8 out of 14 responding ISE departments and agencies have provided training on privacy and civil liberties policies to personnel with information sharing responsibilities.		
Agency	2011 Response	Agency	2011 Response
CIA	NA	DOJ	Yes
DHS	Yes	DoS	Yes
ODNI	No	DOT	NA
DOC	NA	FBI	Yes
DoD/JCS	Yes	HHS	No
DOE	No Response	NCTC	Yes
DOI	Yes	Treasury	No
2011 Highlight	There has been a 13% increase in the past year in the number of responding ISE departments and agencies who have provided this training.		

Enterprise Architecture – Investments

Measurement Question	Has your agency mapped at least one IT investment to its information sharing segment architectures?		
2011 Metric	11 out of 14 responding ISE departments and agencies have mapped at least one IT investment to its information sharing segment architectures.		
Agency	2011 Response	Agency	2011 Response
CIA	Yes	DOJ	Yes
DHS	Yes	DoS	Yes
ODNI	Yes	DOT	Yes
DOC	NA	FBI	Yes
DoD/JCS	Yes	HHS	No
DOE	No Response	NCTC	Yes
DOI	Yes	Treasury	No
2011 Highlight	There has been a 14% increase in the past year in the number of responding ISE departments and agencies who have mapped at least one investment—now at 79%.		

2011 ISE Annual Report to the Congress

Measurement Question	Has your agency represented all major ISE IT investments in its enterprise transition plans?			
2011 Metric	8 out of 14 responding ISE departments and agencies have represented all major ISE IT investments in its enterprise transition plans.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	Yes
2011 Highlight	There has been a 7% increase in the past year in the number of responding ISE departments and agencies representing all major IT investments—now at 57%.			

Measurement Question	Does your agency have interconnection plans for SBU/CUI networks supporting the ISE?			
2011 Metric	8 out of 14 responding ISE departments and agencies have developed (or are developing) interconnection plans for SBU/CUI networks supporting the ISE.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	No		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	Under Development
2011 Highlight	There has been a 14% increase in the past year in the number of responding ISE departments and agencies who have interconnection plans for SBU/CUI networks supporting the ISE—now standing at 57%.			

Measurement Question	Does your agency have a plan for implementing interconnection capability for sharing terrorism and homeland security information across SBU/ CUI networks?			
2011 Metric	5 out of 14 responding ISE departments and agencies have a plan for implementing interconnection capability for sharing terrorism and homeland security information across SBU/ CUI networks.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	NA		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	Under Development
2011 Highlight	With the IC responding in the negative this year, there is a 21% decrease in positive responses for this question; now standing at 36%.			

Enterprise Architecture - Common Information Sharing Standards (CISS)

Measurement Question	Does your agency have a completed, approved information sharing segment architecture?			
2011 Metric	7 out of 14 responding ISE departments and agencies have a completed, approved information sharing segment architecture.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	NA
2011 Highlight	There has been a 7% increase in the past year in the number of responding ISE departments and agencies completing these architectures.			

Measurement Question	Does your agency reference the Information Sharing Environment section of the Federal Transition Framework (FTF) Catalog in building its segment architectures?			
2011 Metric	7 out of 14 responding ISE departments and agencies reference the Information Sharing Environment section of the Federal Transition Framework (FTF) Catalog in building its segment architectures.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	NA
2011 Highlight	With the IC responding in the negative this year, there is a 21% decrease in positive responses for this question; now at 50%.			

Measurement Question	Has your agency incorporated Common Information Sharing Functional Standards into the management and implementation of its ISE-related mission business processes?			
2011 Metric	10 out of 14 responding ISE departments and agencies have incorporated Common Information Sharing Functional Standards into the management and implementation of its ISE-related mission business processes.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	71% of responding ISE departments and agencies are incorporating the standards, representing a 36% increase over the past year.			

2011 ISE Annual Report to the Congress

Measurement Question	Has your agency incorporated Common Information Sharing Technical Standards into enterprise architectures and IT capability?			
2011 Metric	7 out of 14 responding ISE departments and agencies have incorporated Common Information Sharing Technical Standards into enterprise architectures and IT capability.			
Agency	2011 Response		Agency	2011 Response
CIA	No		DOJ	Yes
DHS	Yes		DoS	No
ODNI	No		DOT	Yes
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	No
DOI	Yes		Treasury	NA
2011 Highlight	50% of responding ISE departments and agencies are incorporating these standards—a 7% increase in the past year in this area.			

Measurement Question	Do you find the Common Information Sharing Functional Standards, such as ISE-SAR, helping your department/agency improve your counterterrorism processes, interfaces to other ISE partners, and structure of your data/information for sharing in the ISE?			
2011 Metric	9 out of 14 responding ISE departments and agencies have noticed improvement over the past year.			
Agency	2011 Response		Agency	2011 Response
CIA	Yes		DOJ	Yes
DHS	Yes		DoS	No
ODNI	Yes		DOT	No
DOC	NA		FBI	Yes
DoD/JCS	Yes		HHS	No
DOE	No Response		NCTC	Yes
DOI	Yes		Treasury	NA
2011 Highlight	There has been a 21% increase in the past year in this area with 64% of responding ISE departments and agencies showing improvement over the past year.			

8 APPENDIX B – Acronyms

ADA	Aviation Security and the Air Domain Awareness
ASCIA	Association of State Criminal Investigative Agencies
ASNI WG	Assured Secret Network Interoperability Working Group
AWW	America’s Waterway Watch
BAE	Backend Attribute Exchange
BCA	Baseline Capabilities Assessment
BCOT	Building Communities of Trust
BIA	Bureau of Indian Affairs (DOI)
BJA	Bureau of Justice Assistance (DOJ)
CAIAC	Civil Aviation Intelligence Analysis Center (DoD)
CBP	U.S. Customs and Border Protection (DHS)
CIA	Central Intelligence Agency
CICC	Criminal Intelligence Coordinating Council
CIKR	Critical Infrastructure and Key Resources
CIKR ISE	Critical Infrastructure and Key Resources Information Sharing Environment
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council (DHS)
CISO	Chief Information Sharing Officer
CISS	Common Information Sharing Standards
CJIS	Criminal Justice Information Services (FBI)
CNSS	Committee on National Security Systems
COC	Critical Operational Capabilities
COI	Community of Interest
CONOPS	Concept of Operations
CT	Counterterrorism
CUI	Controlled Unclassified Information
CUI Office	Controlled Unclassified Information Office (NARA)
CVE	Countering Violent Extremism
DAWG	Data Aggregation Working Group

DD/OS	Deputy Director for Operations Support (NCTC)
DEA	Drug Enforcement Administration (DOJ)
DHE	Domestic Highway Enforcement
DHS	Department of Homeland Security
DI	Directorate of Intelligence (FBI)
DIAP	Drug Interdiction Assistance Program (ONDCP)
DNDO	Domestic Nuclear Detection Office (DHS)
DNI	Director of National Intelligence
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DoS	Department of State
DOT	Department of Transportation
DSAC	Domestic Security Alliance Council (FBI)
DSI MG	DHS SAR Initiative Management Group
DTRA	Defense Threat Reduction Agency (DoD)
EA	Enterprise Architecture or Executive Agent
EO	Executive Order
EOP	Executive Office of the President
EU	European Union
FAA	Federal Aviation Administration (DOT)
FBI	Federal Bureau of Investigation
FBINet	Federal Bureau of Investigation Secret Domain Network
FEA BRM	Federal Enterprise Architecture Business Reference Model
FEMA	Federal Emergency Management Agency (DHS)
FICAM	Federal Identity, Credential, and Access Management
FIGs	Field Intelligence Groups
FIMS	Federated Identity and Management Service
FMCSA	Federal Motor Carrier Safety Administration (DOT)
FSAM	Federal Segment Architecture Methodology

FTF	Federal Transition Framework
FY	Fiscal Year
GAO	Government Accountability Office
GeoCONOPS	Geospatial Concept of Operations
GFIPM	Global Federated Identity and Privilege Management
GLOBAL	Global Justice Information Sharing Initiative
GSA	General Services Administration
HHS	Department of Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center (DHS)
HSDN	Homeland Security Data Network (DHS)
HSEC SINS	Homeland Security Standing Information Needs (DHS)
HSIN	Homeland Security Information Network (DHS)
HSIN-CS	Homeland Security Information Network-Critical Sectors (DHS)
HSIN-EM	Homeland Security Information Network-Emergency Management (DHS)
HSIN-LE	Homeland Security Information Network-Law Enforcement (DHS)
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence and Analysis (DHS)
IA	Intelligence Analyst
IACP	International Association of Chiefs of Police
IC	Intelligence Community
IC ISE	Intelligence Community Information Sharing Executive (ODNI)
ICAM	Identity, Credential, and Access Management
ICAMSC	Identity Credential and Access Management Subcommittee
ICD	Intelligence Community Directive
ICE	Immigration and Customs Enforcement (DHS)
IdAM	Identity and Access Management
IED	Improvised Explosive Device
IEPD	Information Exchange Package Description
IIB	Intelligence Integration Branch (FBI)
IISC	Information Integration Subcommittee
IJIS	Integrated Justice Information System

InCop	Information Collection on Patrol
INTERPOL	International Criminal Police Organization
IO	Intelligence Officer
IP	Office of Infrastructure Protection (DHS) or Identity Provider
IPC	Interagency Policy Committee
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Information Sharing and Access
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISGB	Information Sharing Governance Board (DHS)
ISPE	Information Sharing and Partner Engagement (DoD)
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JABS	Joint Automated Booking System
JCS	Joint Chiefs of Staff (DoD)
JPDO	Joint Planning and Development Office
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
LAPD	Los Angeles Police Department
LEISI	Law Enforcement Information Sharing Initiative
LEO	Law Enforcement Online (FBI)
LOB	Lines of Business
MACE	Multi-Agency Collaboration Environment
MCCA	Major Cities Chiefs Association
MCSA	Major County Sheriffs' Association
MDA	Maritime Domain Awareness
MIST	Multimodal Information Sharing Taskforce
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCIX	National Counterintelligence Executive (ODNI)
NCTC	National Counterterrorism Center (ODNI)

N-DEx	Law Enforcement National Data Exchange (FBI)
NDIC	National Drug Intelligence Center (DOJ)
NextGen	Next Generation Air Transportation System
NFCC	National Fusion Center Conference
NGA	National Geospatial-Intelligence Agency
NGI	Next Generation Identification
NICC	National Infrastructure Coordination Center (DHS)
NIEF	National Information Exchange Federation
NIEM	National Information Exchange Model
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NLE	National Level Exercises
Nlets	National Law Enforcement Telecommunications System
NMIC	National Maritime Intelligence Center
NOC	National Operations Center (DHS)
NPPD	Directorate for National Protection and Programs (DHS)
NSA	National Sheriff's Association or National Security Agency
NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative
NSIS	National Strategy for Information Sharing
NSS	National Security Staff
NSTC	National Science and Technology Council
NSTIC	National Strategy for Trusted Identities in Cyberspace
NTAS	National Terrorism Advisory System
NYC	New York City
NYPD	New York Police Department
NYSIC	New York State Intelligence Center
OASIS	Organization for the Advancement of Structured Information Standards
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OMG	Object Management Group
ONDCP	Office of National Drug Control Policy
OPM	Office of Personnel Management

OSD	Office of the Secretary of Defense (DoD)
P/CL	Privacy and Civil Liberties
P/CR/CL	Privacy, Civil Rights, and Civil Liberties
PAC	Policy Advisory Committee
PCSC	Preventing and Combating Serious Crime
PDA	Portable Digital Assistant
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV-I	Personal Identity Verification – Interoperable
PKI	Public Key Infrastructure
PM-ISE	Program Manager, Information Sharing Environment
PMO	Program Management Office
PRND	Preventive Radiological Nuclear Detection
RAC	Resource Allocation Criteria
RFP	Request for Proposal
RIGs	Regional Intelligence Groups (FBI)
RISC	Repository for Individuals of Special Concern
RISS	Regional Information Sharing System
RISSNET	Regional Information Sharing System Network
SA	Special Agent
SAR	Suspicious Activity Report(ing)
SBU	Sensitive But Unclassified
SDOs	Standards Development Organizations
SIPRNet	Secret Internet Protocol Router Network
SLT	State, Local, and Tribal
SLTPS	State, Local, Tribal and Private Sector
SLTT	State, Local, Tribal and Territorial
SLTPS	State, Local, Tribal, Territorial, and Private Sector
SNCTC	Southern Nevada Counter Terrorism Center
SP	Service Provider or Special Publication
SSO	Simplified Sign On
STC	Securing the Cities

TLOA	Tribal Law & Order Act
TON	Tohono O’odham Nation
TRIPWire	Technical Resource for Incident Prevention (DHS)
TSA	Transportation Security Administration (DHS)
TSC	Terrorist Screening Center (FBI)
TtT	Train the Trainer
TWCG	TRIPWire Community Gateway
UML	Unified Modeling Language
US-VISIT	United States Visitor and Immigration Status Indicator Technology
USCG	U.S. Coast Guard (DHS)
USD(I)	Under Secretary of Defense for Intelligence (DoD)
USIA	Under Secretary for Intelligence and Analysis (DHS)
USSS	U.S. Secret Service (DHS)
VCC	Virtual Command Centers
WITS	Worldwide Incidents Tracking System
WMD	Weapons of Mass Destruction
WSP	Washington State Police
XML	Extensible Markup Language



**PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT
WASHINGTON, D.C. 20511**

202.331.2490

WWW.ISE.GOV



USC



CREATE

HOMELAND SECURITY CENTER

**Foreign Fighters: Terrorist Recruitment and Countering
Violent Extremism (CVE) Programs in Minneapolis-St. Paul**

A Qualitative Field Study

April 2015

Prepared for the Department of Homeland Security Science & Technology
Directorate

By the National Center of Excellence for Risk and Economic Analysis of
Terrorism Events (CREATE), University of Southern California

About the Report

The authors of this report are Dr. Erroll Southers, Director of Transition and Research Deployment and Countering Violent Extremism (CVE) Theme Leader, and Justin Hienz, Subject Matter Expert, both at the Department of Homeland Security National Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California. The report was supported by researcher Dr. Heather Rosoff and USC Sol Price School of Public Policy graduate students Christopher Fox, Corinna Jiang, Sandy Lo, and Young Park. Questions about this report should be directed to Erroll Southers at southers@usc.edu.

This report is sponsored by the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, in support of the CVE program. The goal of this program is to sponsor research that will support the Administration's strategy to advance the understanding of the foreign fighter recruitment dynamic and the cultural, socioeconomic, and community factors that coalesce to create vulnerability to terrorist recruitment in the Somali-American community in Minneapolis-St. Paul, Minnesota.

This research was supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Cooperative Agreement No. 2010-ST-061-RE0001. Any opinions, findings, conclusions or recommendations in this document are those of the authors and do not necessarily reflect the views of the United States Department of Homeland Security or the University of Southern California.

About CREATE

The National Center of Excellence for Risk and Economic Analysis of Terrorism Events (CREATE) is an interdisciplinary national research center based at the University of Southern California. CREATE's mission is to improve national security through the development of advanced models and tools for the evaluation of the risks, costs and consequences of terrorism and to guide economically viable investments in homeland security. The Center serves national interests by providing tools and guidance to the Department of Homeland Security, as well as local, regional, and state decision-makers, for the prioritization of countermeasures to terrorism, identifying areas where investments are likely to be most effective, computing relative risks among potential terrorist events, and estimating the societal consequences of terrorism.

TABLE OF CONTENTS

Executive Summary	1
Introduction.....	2
Methodology	4
Minneapolis-St. Paul Somali Immigrant Community Context.....	6
Terrorist Recruitment in Minneapolis-St. Paul.....	12
Countering Violent Extremism Programs in Minneapolis	21
Conducting Fieldwork in an Immigrant Community.....	33
Conclusions.....	39
References.....	41

Executive Summary

The threat of foreign fighter recruitment is greater today than it has ever been. The Islamic State in Iraq and the Levant (ISIL) is proving lethally effective in drawing extremists from around the world to their ranks, and in the United States, ISIL is targeting the Somali-American community in Minneapolis-St. Paul, Minnesota.

There are more than 40,000 Somali-Americans and immigrants in Minnesota. This growing immigrant community is facing substantial challenges, including weak family structures, lack of education, racism and violent crime. In this mix of chronic community challenges, young people can be unsure of their personal identity, leaving them vulnerable to terrorist recruiters.

The research and fieldwork conducted for this study reveals an evident relationship between the Somali terrorist group al Shabaab and ISIL. Indeed, ISIL has appropriated the al Shabaab recruiting network, indicating some collaboration between the two groups and suggesting a future direct alliance between them.

The study also reveals that two common assumptions about foreign fighter recruitment do not consistently apply in Minneapolis-St. Paul. First, it has been suggested that poverty and a lack of social mobility are primary causes for radicalization and departure. In the Twin Cities, this is untrue. The second assumption is that social media is ISIL's primary method of recruitment; in the Twin Cities, recruitment was reported to always include face-to-face interaction with a recruiter. Social media enhances recruitment but is not necessarily the primary tool for it.

There are several programs in the Twin Cities that are positively influencing the lives of young people. At the same time, there are numerous organizations that secure government funding but do not achieve any measurable impact on the threat from terrorist recruiters, nor do they reduce community crime and related concerns. These organizations are exceedingly effective in passing government reviews, making it difficult to validate which programs are having a real impact based on a clearly articulated strategy. Included in this study are the community's recommendations for what is needed to address challenges and halt the threat from terrorist recruiters.

During fieldwork, the report authors identified several best practices for conducting research in an immigrant community. These practices allowed the report authors to rapidly gain trust, build relationships and gather unprecedented insight into the Somali-American community in Minneapolis-St. Paul.

We are proud to present this important study and contribute to the national effort to protect our nation, our young people and reduce the risk of recruitment to ISIL's deadly ideology.

Introduction

The emergence of the Islamic State in Syria and the Levant (ISIL) presents a new and dangerous threat to regional stability and global security. ISIL has proven successful in luring young people to its ranks with polished propaganda, sophisticated online messaging and an increasingly complex network of terrorist group alliances. Thousands of young people from around the world have traveled to Syria and Iraq to join ISIL's campaign to establish a caliphate in the Middle East, committing atrocities with a vicious inhumanity that has left the world both horrified and resolved to stem this growing threat.

One important component of this effort is halting the flow of foreign fighters to ISIL's ranks. There are an estimated 100 Americans¹ currently fighting with ISIL, and some of these individuals came from the Somali community in Minneapolis-St. Paul, Minnesota. Unfortunately, the phenomenon of foreign fighter recruitment is not new to the Twin Cities. For years, the Somali al Qaeda affiliate al Shabaab has preyed upon the Somali immigrant community in Minnesota, luring young people with a message of nationalism and ultra-strict, violent religious belief.

Given a variety of factors (including community awareness and rejection of violent extremism), al Shabaab recruiting steadily declined since its peak in 2008-2009. In 2014, however, foreign fighter recruiting and departure increased dramatically, except now, young people are traveling to Syria. The question that prompted this study was: *what is the cause of this sudden increase in Somali foreign fighters and the abrupt shift in destination?* After months of research, fieldwork and community interviews, this report presents an answer.

ISIL's recruiting strategy in Minnesota leverages a collage of demographic factors, religious ideas, identity uncertainty, ineffective application of government funding, and the challenges all immigrant communities face when assimilating to a new society. Within this complex web of cultural, economic, sociological, religious and civic elements, there are clear correlations revealing why ISIL has been successful in recruiting foreign fighters, and more importantly, what can be done to frustrate the group's efforts.

¹ Peter R. Neumann, "Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s," *International Centre for the Study of Radicalization*, January 26, 2015.

This study also reviews the Countering Violent Extremism (CVE) initiatives in Minneapolis-St. Paul. There are individuals and organizations developing innovative, community-led methods for stemming recruitment and addressing community needs. Unfortunately, other ineffective (and often unscrupulous) organizations in Minneapolis-St. Paul are highly effective at securing government funding without following through on the efforts for which the funding was given. Study findings suggest that local, state, and federal monies and support are going to the wrong groups. Thus, the challenge of reducing and stopping recruitment in the Twin Cities is not just a result of increased ISIL activity but also a lack of *effective* programs available to counter it.

Despite these substantial challenges, solutions are available. The threat from ISIL can be overcome. Engaging with the community, more strategically applying funding, and empowering families and young people to resist predatory recruitment efforts will have an impact on ISIL's efforts. Presented here are the research, data, fieldwork findings, and community recommendations that collectively reveal important insights for the ongoing effort to, in the words of President Obama, "degrade and ultimately destroy ISIL."

Methodology

The report authors spent 10 days in Minneapolis-St. Paul over the course of three visits. During these visits, the report authors spoke with more than 30 sources, conducting 20 structured interviews, as well as 10 unstructured interviews. The report authors also spent substantial time within the Somali-American community, visiting areas and establishments with a largely Somali demographic and engaging in impromptu conversations with a diverse cross-section of community members.

The study was submitted to University of Southern California's Institutional Review Board (IRB) for an exempt status review. Exempt review indicates that the research involves the use of educational tests that (1) do not collect identifier information from participants, and (2) do not collect any information that would put the participant at risk. The study was approved for exemption in February 2015.

In line with the IRB exempt status, sources' identifier information was not collected. Each source was assigned a number, and the only identifying characteristics that were recorded were the sources' age and gender. Structured interviews were digitally recorded with the sources' permission.² The audio from these interviews was transcribed, yielding 440 pages of transcripts and hundreds of pages of handwritten notes.

This study used a grounded theory approach to qualitative data analysis, which is designed to assess intensive field research with qualitative data.³ This research uses an iterative analysis strategy that codes patterns in qualitative data to describe categories and typologies, leading to the creation of various model outputs. In this study, the researchers used MAXQDA 11 software to manage the large amounts of interview transcript data through the application of grounded theory methods.

² Only one source declined to be recorded.

³ See, K. Charmaz, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis* (London: Sage, 2006); M.Q. Patton, *Qualitative Research and Evaluation Methods* (Thousand Oaks, CA: Sage, 2002); and, A. Strauss and J. Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 3rd ed. (Thousand Oaks, CA: Sage, 2007).

The data analysis began with a complete reading of interview transcripts by the research team. The initial reading produced a set of categories that corresponded with the initial set of research questions: *why is foreign fighter recruitment occurring and what programs are proving effective in halting it?* In addition, categories were developed from the experiential items shared by the interviewees during interview discussions. The complete set of categories contributed to the development of a coding scheme with a total of 73 codes. As a result of source demographic and identifier information not being collected, the moderating effects of these factors were not explored in this study.

A critical component of the analysis process was the establishment of intercoder reliability. Multiple reviewers were involved in assessing the 73 codes. The percent agreement between reviewers was calculated and adjustments made (primarily through consensus changes) until all coders achieved 85% agreement. The coders also met to discuss emerging topics, resolve challenges, and to refine coding strategies by consensus to ensure optimality. Finally, through pattern coding, the analysis formed typologies (e.g., of different types of community program validation) and delineated the components of the models developed in this study. The findings were reviewed by the entire team to allow for discussion of potential additional analyses, to check for contrary evidence, and to ultimately lay the groundwork for reporting.

Concurrent with fieldwork and content analysis, researchers conducted a literature review of academic and media sources examining the Somali-American community in Minnesota and the threat of radicalization and recruitment. Information from this research effort is paired with the fieldwork findings and qualitative data analysis, yielding a multifaceted picture of the foreign fighter recruitment activity in the Twin Cities and how community stakeholders are responding.

Minneapolis-St. Paul Somali Immigrant Community Context

In 2013, Minnesota was home to 38,873 Somali immigrants and Somali-Americans, the largest Somali population in the United States, according to the 2013 American Community Survey.⁴ This number has grown since then, and in any case is artificially small because, as sources indicated, many Somali immigrants (particularly those recently arrived from abroad) fear that responding to census questions and engaging any government initiative could put their legal status and personal wellbeing in jeopardy. This is a consequence of emigrating from a background where government services and law enforcement have engaged in aggressive, sometimes inhumane treatment of its civilians, as well as a misunderstanding of how the U.S. government system works and the civil rights and liberties guaranteed to every citizen and resident of the United States.

More specifically, Riverside Plaza, a public and affordable housing complex in the Cedar-Riverside neighborhood, is often the first place of residence for a new Somali immigrant. While the number of Plaza residents is around 4,000 individuals (the building capacity), community members and law enforcement estimated that the actual number of residents is closer to 10,000. Thus, the current overall number of Somalis living in Minnesota is unknown.

Nearly 56% of Somalis living in Minnesota are 24 years old or younger, with the median age being 21.3 years old. Nationwide, 57.3% of Somalis are 24 years old or younger, with a median age of 21.2 years old.⁵ Troublingly, for the foreign fighters investigated for this study, the average age at the first instance of extremist activity was 22.73 years old.

Of Somali households in Minnesota, 34.6% are single parent, with an average family size of 4.37 people. For Somali-Americans in Minnesota younger than 25, 39% do not have a high school diploma. And of the state's 16-and-older age cohort, 31.9% of the Minnesota Somali population is not part of the state's labor force, yielding a 55.1% poverty rate for Minnesota Somali-Americans and immigrants, 3.5 times greater than the overall U.S. population.

⁴ U.S. Census Bureau, "2013 American Community Survey of Somalis 3-yr Estimate," U.S. Department of Commerce, 2013.

⁵ Ibid.

Nearly 60% of the Twin Cities Somali population was born in the United States, significantly more than the nationwide percentage, where only 37.29% are born in the United States. Thus, there are upwards of 20,000 Minnesota Somalis under the age of 25 who encounter substantial social and economic challenges, though, as shown in this report, poverty is less pertinent to recruitment vulnerability than other factors impacting the community. Young Somali-Americans seek to overcome these challenges in the face of targeted, sophisticated and ongoing recruitment efforts by terrorist organizations.

The densest Somali communities in Minnesota are in the Cedar-Riverside neighborhood in south Minneapolis (also called the “West Bank”) and the University Avenue area between Rice and Hamline Streets in St. Paul.⁶ There are also other sizable Somali communities throughout the greater Minneapolis-St. Paul area. While Cedar-Riverside is commonly a first stop for new Somali immigrants, sources reported that the goal for many residents is not to remain in the neighborhood but to establish themselves in their new society and move on to other areas in Minnesota. This is in part because the Cedar-Riverside area has historically been impoverished with significant crime rates. One source noted an occasion when a charitable organization began distributing second-hand clothes in the Cedar-Riverside area. West Bank residents lined up to receive the donations, leading one to comment, “It’s like we’re still in the refugee camp.”

Immigration to the United States

All sources for this report were originally born in Somalia or a neighboring country harboring Somali refugees. A first wave of immigration commenced in the 1990s and at the turn of the century, as famine and warfare pushed more Somalis into refugee camps in neighboring countries. Most sources for this report immigrated during this time period, 80% first immigrating to a city other than Minneapolis-St. Paul, including Atlanta, Louisville, Los Angeles, New York City, San Diego, Seattle, and northern Virginia cities.

Sources reported that during this first wave of immigration, the Twin Cities offered a wealth of jobs in the cities’ manufacturing and food industries, as well as a perceived absence of racial and ethnic prejudice that some sources experienced in other U.S. cities. The local and state government and religious institutions also offer important social programs and benefits. Today, sources reported that the draw to Minneapolis-St. Paul is less about employment opportunity and social services than it is about a cultural and familial infrastructure built over years of immigration.

⁶ Fartun Dirie, “Mental Maps: Gaining Insight into the Diverse Somali Perceptions of Residential Desirability in the Twin Cities,” *Midwestern Undergraduate Geography Symposium, Macalester College*, April 27, 2013.

There is currently a second wave of Somali immigrants arriving in the United States. In 2014, 1,050 Somali immigrants arrived in Minnesota (nationwide, 9,000). The growing Somali immigrant population is yielding a corresponding increase in the social needs of the Minneapolis-St. Paul community. For example, Somali student enrollment in the Minneapolis School District has increased 70% since 2011, and Somali use of Minnesota food assistance has doubled in the last five years.⁷

Ongoing immigration also continues a trend of clan allegiances being transplanted to the United States. The Minnesota Somali community is made up of numerous confederations of *qabil*, or clans, the most prevalent being the Darod, Dir, Hawiye and Isaaq. These groups are composed of sub-clans, with lineage that can often be traced back hundreds of years. While these clan affiliations were central to the civil war that long-ravaged Somalia, in Minnesota, sources described clans as a form of insurance. For example, if a clan member were in a car accident but could not afford to pay the damages, clan members may contribute money to satisfy the debt or need.

This traditional form of community support does sometimes conflict with U.S. laws. As it was related to the report authors, a challenge for law enforcement is that clans often resolve conflict internally rather than turning to the U.S. justice system. Law enforcement sources discussed violent crimes, including homicide, within the Somali community that are resolved through *xeer*, a traditional method of conflict resolution driven by clan elders. In a case of violent conflict (such as a shooting), a clan may pay “blood money” as reparation for the violence. Once a clan-to-clan agreement has been reached, clan members are forbidden from discussing the crime with officials. This is a source of frustration for local law enforcement, as it leaves murders and other crimes unsolved for want of witnesses, sometimes including the victim themselves.⁸

Immigration inherently challenges one’s identity, forcing one to reconcile “old world” tradition and culture with the social, ethical, legal and economic realities of a new country. While there are many differences between Somali and American culture, these do not necessarily prohibit evident patriotism and a deep appreciation for the United States’ guaranteed freedoms and readiness to accept refugees fleeing war and famine. Structured interviews yielded 119 positive statements about the United States, including sentiments about freedom, safety and the rule of

⁷ Mila Koumpilova, “New Somali Refugee Arrivals in Minnesota Are Increasing,” *Minneapolis Star-Tribune*, Nov. 1, 2014.

⁸ One law enforcement source described an instance where a shooting victim lied under oath rather than identify the defendant as his attacker. In that case, the jury saw through the victim’s false testimony and found the defendant guilty. This was described as an exception rather than the norm for violent crime within the Somali community.

law. Yet, there were negative sentiments about the Somali immigrant experience, including challenges to assimilation, racial tensions and a distrust of authority (notably, the FBI). There were also repeated references to a perceived sense of American animosity towards Islam, often in reference to airport screening.

Religion in the Minneapolis-St. Paul Somali Community

Islamic belief and tradition permeate every aspect of Somali society, guiding dress, relationships, education, diet, recreation, and a host of factors that make Somali society unique. Islam has a long history in Somalia. Historically, Islamic belief in Somalia was of the Sufi variety, which is a mystical interpretation of Islam that employs repetitive sayings and other devotional actions (*dhikr*) to reach a greater insight, connection, and worship of Allah. These longstanding religious traditions have changed in the face of regional and global conflict, and a brief review of Somali political history reveals how civil war and famine has impacted the country's religious landscape.

For the last century, Somalia has been a battleground for competing geopolitical interests. Colonialism and two world wars brought modern weaponry to the country, and in 1969, the military dictator General Mohamed Barre took power in a bloodless coup d'état.⁹ As Barre revealed his dictatorial approach to rule, he formed the Somali Revolutionary Socialist Party, aligning the country with the Soviet Union during the Cold War. Barre nationalized industries, forbade clanism (even as he favored his own clan), and sought to supplant local and genealogical allegiance with loyalty to the state. Barre's totalitarian regime and the violence it wrought prompted Somalis to begin leaving the country, a trend that would only increase in the decades ahead.

Barre invaded neighboring Ethiopia in 1977, and the Soviet Union sided with the communist regime in Ethiopia. Barre changed his allegiance to the United States, making Somalia an even more violent Cold War proxy battle, injecting substantial amounts of weapons into the country. When the Cold War ended and western aid evaporated, Somali government and society, plagued by decades of conflict, collapsed. Barre was forced from power in a coup and clan-based warfare erupted around the heavily armed country.

⁹ Jama Mohamed Ghalib, *The Cost of Dictatorship: The Somali Experience* (New York: Lilian Barber Press, 1995).

In 1991 and 1992, 25,000 people were killed in the capital city of Mogadishu, with 1.5 million people fleeing to neighboring countries and another 2 million people displaced internally.¹⁰ Widespread, persistent fighting and the breakdown of a centralized government authority contributed to famine that struck Somalia in the 1990s. While many Somali refugees have received residency and citizenship in other countries, and some have returned home, the United Nations Human Rights Council reports that there remain nearly 1 million Somali refugees, most harbored in Kenya, Ethiopia and Yemen, with smaller numbers in Uganda, Djibouti, Egypt and other nearby countries.

With clan structures deteriorating, elders and religious leaders killed in fighting, and the evaporation of longstanding social structures, a window of opportunity emerged for Islamic influence from other Muslim-majority countries, notably, the Wahhabist Saudi Arabia. Factions of Sunni Islam began to grow and influence the ravaged Somali society, one of these being Salafism. A segment of Sunni Islam, Salafism calls for a strict interpretation of religious literature, absolute adherence to Islamic law (*shari'a*) and an overall return to the theocracy reflected in writings about seventh- and eighth-century Muslim society. Indeed, in Arabic, *salaf* means “ancient one,” a reference to the first followers of the Prophet. This form of Islamic belief cannot accommodate the culture- and tradition-based, exploratory religious practice that is Somali Sufism. This is one reason why, even today, the Salafi-grounded al Shabaab systematically destroys Sufi shrines and other traditional religious infrastructure that deviates from the unforgiving Salafi theology.

Today, Sunni Islam is the dominant Islamic interpretation in the Minnesota Somali community. Only one source noted an awareness and understanding of Sufi belief and practice. This limited reference to Sufism in Minneapolis-St. Paul is perhaps less a reflection of religious preference than it is a consequence of civil war that has left many learned religious leaders and elders dead, unable to pass on their religious knowledge.

There are more than 20 mosques in the greater Minneapolis-St. Paul area. These mosques are not exclusively attended by Somali-Americans, though some congregations are predominantly Somali. Mosques and other Islamic centers are the locations for daily prayer, but there are also religious study groups and functions for a Muslim community. For example, Minneapolis-St. Paul is home to several Somali Islamic schools (*dugsis*), which simultaneously offer a Western academic curriculum and teachings drawn from Somali culture and tradition. Overall, sources

¹⁰ Mark Bradbury and Sally Healy, “Endless War: A Brief History of the Somali Conflict,” *Whose peace is it anyway? Connecting Somali and International Peacemaking*, 2010.

indicated there are a plethora of opportunities in Minneapolis-St. Paul for a Muslim to garner religious knowledge and guidance, including Sufism.

Al Shabaab in Minnesota

In 2008, al Shabaab seized control of the Somali capital, Mogadishu, and the southern half of the country. Following an extremist Salafi theological interpretation, al Shabaab (Arabic, meaning “the youth”) initially garnered support among the Somali diaspora because they claimed to represent an Islamic nationalistic movement opposed to the interventions of neighboring countries and seeking to rebuild a nation. For a people lamenting the destruction of their motherland, elements of al Shabaab’s message resonated worldwide. While only during unrecorded, unstructured interviews, multiple sources said that they initially supported al Shabaab because they believed they were pursuing a reconstruction of a failed state.

After al Shabaab began aggressively recruiting Somali immigrants in Minneapolis-St. Paul, the community perception of the terrorist group began to change. Somalis who joined the group relayed stories of the atrocities they saw al Shabaab commit. Sources reported stories of young people who attempted to leave al Shabaab and return to their families in the United States but were executed by al Shabaab before that was possible. Word spread that the group was not the nationalistic movement it claimed to be, and one primary reason al Shabaab recruiting decreased after 2009 was that the community became more aware of al Shabaab’s true, terrorist nature and rejected it.

Today, recruiters are again pulling young Somali immigrants to foreign terrorist groups, except now, young people are traveling to Syria.

Terrorist Recruitment in Minneapolis-St. Paul

Since 2014, numerous Minneapolis Somali residents have left the United States to travel to Syria to join ISIL. This is an abrupt shift in destination, as previous departing residents went to Somalia to join al Shabaab. Clearly, something changed, not the people vulnerable to recruitment but the benefactors of the recruiters. Presented here are details of recent foreign fighter recruitment efforts that resulted in Somali-Americans joining or attempting to join ISIL and what it reveals about the risk of terrorist recruitment in Minneapolis.

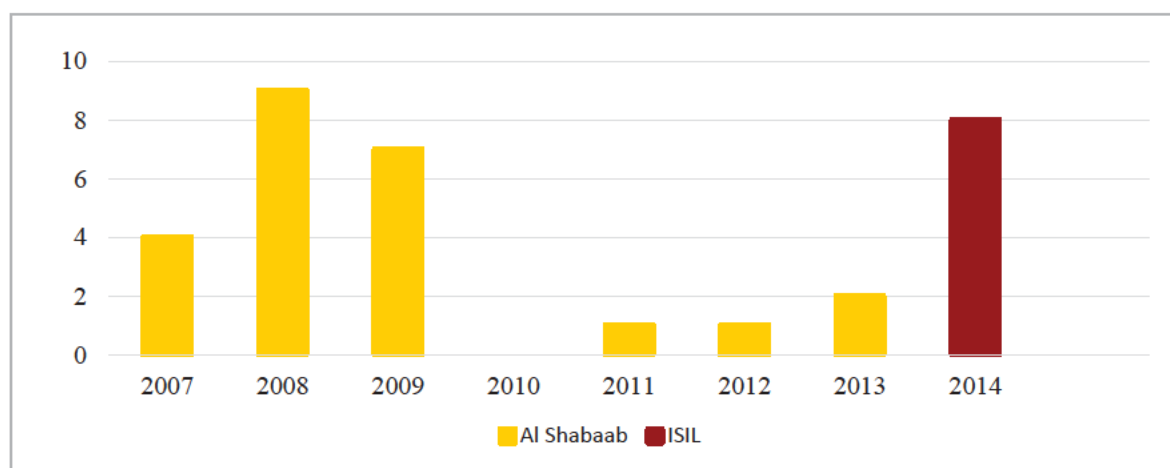


Figure 1 - Foreign Fighter Departures

Cases of Recruitment and Departure

In November 2014, we conducted an interview with the family of a young woman who surreptitiously fled to Syria. The family described a jubilant, sociable, articulate person. Recently graduated from high school, the 19-year-old told family she wanted to become a nurse and planned to register for college in January 2015. She had shown no interest in marriage, though it would not be uncommon for her to marry at that age.

In mid-2014, she became involved with a young man and changed her place of worship. Meanwhile, her family noticed a distinct shift in her manner and social interaction. Her mother said that she stopped speaking to friends and acquaintances. She spent much of her time alone in her room, reading the Qur'an, and she reportedly said she wanted to live in an Islamic country and desired more Islamic education.

On a Friday, she told family she was going to a friend's bridal shower and called later to say she would be spending the night away from home, returning on Saturday. On Sunday, she sent a text message to her mother, saying that she was in Syria.

The story of this young woman closely mirrors that of other young people who have journeyed to join ISIL. In February 2015, London teenagers Amira Abase, Shamima Begum and Kadiza Sultana traveled to Syria via Istanbul to join ISIL. Abase's excuse to her father for leaving was that she was going to a wedding, a curious (if not suggestive) similarity to the excuse offered by the young Somali woman.¹¹

Another example is that of Abdi Nur, who left Minneapolis in May 2014 to join ISIL in Raqqa, the so-called capital of the Islamic State. Nur was attending community college with aspirations of studying law before he became more religious and began proclaiming extremist, pro-ISIL statements.¹²

One might assume that a newfound, strict religious belief is a warning sign that a young Muslim is on a path towards extremism and vulnerability to recruitment; however, in an Islamic family or social group, increased religious activity is not necessarily seen in a negative light. The young Somali woman's family characterized themselves as religious, able to recite the Qur'an from memory. Her increased religious activity was not a troubling sign but a fuller embrace of the family's beliefs, which, from the family's perspective, was inherently good, as it would be for any family holding religion as a core value.

This is one of the principal challenges of empowering families and communities to recognize and disrupt the radicalization and recruitment process. At what point does increased religious activity cross a line from a healthy embrace of belief to a negative, extreme interpretation of religious tenets? It is because of this uncertainty that families may not initially see their young people progressing through the radicalization pathway. Terrorist recruiters can capitalize on this to place an extreme worldview on their targets' developing beliefs. One example is that of Amir Meshal.

¹¹ Holly Yan and Nima Elbagir, "Authorities Scramble to Find Teen Girls Before They Join ISIS," *CNN*, Feb. 23, 2015.

¹² Scott Shane, "From Minneapolis to ISIS: An American's Path to Jihad," *The New York Times*, March 21, 2015.

Amir Meshal is an American of Egyptian descent, originally from New Jersey. In 2014, he began frequenting Minnesota mosques. Leaders of the Al-Farooq Youth and Family Center in Bloomington, a suburb of Minneapolis-St. Paul, filed a no-trespass order against Meshal, citing concerns about his interaction with the community's Muslim youth.¹³ Not long after, religious leaders at the Al-Tawba mosque in Eden Prairie called police when a worshipper relayed that Meshal, who was attending, made extremist statements contrary to the imam's lecture.¹⁴ Meshal has not been seen in Minnesota since.

One source for this report was intimately familiar with the story of Meshal, as he is commonly asked to help Twin Cities Somali families facing legal problems (including terrorism charges). The source narrated what he had gathered about Meshal's radicalization and recruitment process, having spoken directly with the young people who met with Meshal.

The process was described to take place over several months. It began with an offer from Meshal to a Somali young man for a free haircut or a free lunch. In an impoverished community with a background of extreme need, such an offer is not flippant. This evolved into a group of four young men meeting weekly to discuss Islam. They deliberately avoided meeting at mosques or in a religious setting. Instead, they met somewhere different each week, sometimes at the family homes of the young men, with family members looking on. There was no obvious reason for concern at first, as the meetings were benign, simply opportunities to discuss the tenets of Islam with young people.

As the conversation shifted from beliefs and practice to the role of jihad in a Muslim's life, the four young men were instructed not to tell anyone about their meetings, enhancing the relationship and trust between members of the group via the element of confidentiality. Meshal talked about how jihad has been used in the past, in the time of the Prophet and in the growth of the faith afterwards. Having carefully brought his students to a *cognitive opening*, a point at which one can accept and internalize violent extremist ideas, Meshal asked the question, "Looking at the world today, is there a need for jihad?" To be sure, he constructed a view of the world where his recruits would answer in the affirmative.

¹³ Paul McEnroe and Allie Shah, "Federal Grand Jury Targets Local Terrorist Pipeline," *Minneapolis Star-Tribune*, Sept. 20, 2014.

¹⁴ Laura Yuen, "Suspicious, Speculation Grow as FBI's Minn. Terror Probe Churns," *MPR News*, Nov. 13, 2014.

This radicalization process ended with direction for Meshal's recruits to travel to Syria. In July, the FBI stopped an 18-year-old man before he boarded a plane for Istanbul, Turkey. He was destined for Syria, and press reports state that during interrogation, the man identified Meshal as his recruiter.¹⁵

Reports of how many people have departed the Twin Cities to join ISIL often conflict and lack specificity. What is more, due to the open-source nature of this study, there are limits on the kinds of information the report authors accessed during research; publically available FBI figures are often vague and not easily aggregated. That said, the report authors confirmed that at least eight Somali-Americans have left Minneapolis for Syria since the end of 2013, and there are others who have left who have not been reported to authorities (according to sources). Meshal was identified and rejected by the community but not before he radicalized at least one Minneapolis resident. Logic, as well as source statements, suggests there are more recruiters in the community.

Collaboration between Al Shabaab and ISIL

Some sources for this report said they were confused by Twin Cities Somali youths traveling to Syria. Al Shabaab's recruiting message had been based on nationalism and genealogy, as well as religion, and multiple sources said they could understand the enduring desire to see their mother country stabilize and improve, even as they disagreed with the extremist interpretation of Islam that al Shabaab espouses. In Syria, however, that nationalistic zeal does not apply, meaning recruiters are attracting young people not based on their country of origin but by appealing to the notion of a global Muslim community and ISIL's vision of a caliphate and apocalypse.¹⁶

Sources reported that the recruiters who sent young people to Somalia are the same recruiters now sending young people to Syria. One Cedar-Riverside source, who has known several young people who departed the United States to join a terrorist group, said: "*A kid who left [for Somalia] sent a text message to say the new order is to go to Syria. They are using old friends as the messengers.*"

¹⁵ Tom Lyden, "EXCLUSIVE: Man booted from Minn. mosque an ISIS recruiter or FBI mole?" *Fox 9 KMSP-TV*, Oct. 05, 2014.

¹⁶ Jessica Stern, "ISIS's Apocalyptic Vision," Hoover Institution, Stanford University, Feb. 25, 2015. *Also see*, Graeme Wood, "What ISIS Really Wants," *The Atlantic*, March 2015.

U.S. Attorney Andrew Luger concurred with our findings that ISIL has appropriated the al Shabaab recruiting network. What is not yet clear is the nature of the relationship between the two terrorist groups. There are reports that ISIL, via its media outlets, has offered a public invitation for al Shabaab to pledge allegiance to the Islamic State, in the same way that the Nigerian terrorist group Boko Haram did in March 2015.¹⁷ The message also encouraged Abu Ubaidah, the leader of al Shabaab in Somalia, to conduct attacks in neighboring countries. While circumstantial, the fact that al Shabaab recruiters are sending people to Syria and that al Shabaab recently attacked Garissa University in neighboring Kenya suggests that the Somali terror group is edging its way towards a direct alliance with ISIL.¹⁸

Immigration, Identity and Vulnerability

The Somali diaspora following the civil war and famine has thrust a unique Islamic culture and tradition into secular societies. On the one hand, sources overwhelmingly spoke about the United States as a place of opportunity, and there is a deep appreciation for the refuge the United States offered Somalis fleeing their homeland. Yet, there is a significant mistrust of government at all levels, stemming from a perception that social benefits and support are not accessible to the Somali community in Minneapolis-St. Paul.

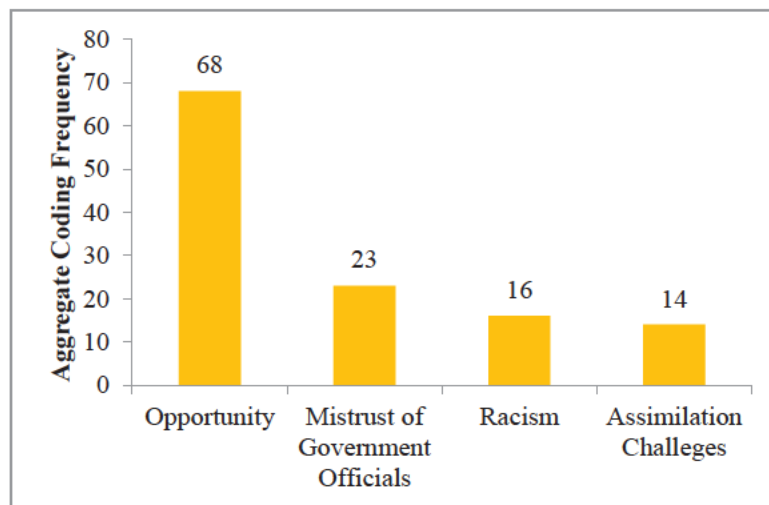


Figure 2 – Somali-American Perceptions of the United States

Sources expressed insult and anger that, due to their traditional dress and names, they receive undue scrutiny at airports and other public places. Frequent and reportedly invasive police and FBI activity has compounded a sense of opposition with government (broadly speaking). Beyond this, sources reported that the first time they encountered the phenomenon of race relations was when they arrived in the United States. The history of racial discrimination and

tension in the United States, experienced particularly by African Americans, is not one shared by Somalis, and immigration to the United States forces an amendment to one's identity to accommodate racism and xenophobia among the varied ethnic communities in the Twin Cities.

¹⁷ Caroline Hellyer, "ISIL courts al-Shabab as al-Qaeda ties fade away," *al Jazeera*, Mar. 23, 2015.

¹⁸ "Kenya attack: 147 dead in Garissa University assault," *BBC News*, Apr. 3, 2015.

These sentiments are encapsulated in a saying several sources offered: “I’ve got five strikes against me, and I just got here. I’m an immigrant. I’m East African. I’m Somali. I’m black. I’m Muslim.” Some female sources added a sixth strike, their gender.

Each of those points contributes to a shared sense of cultural isolation. In this mix of socio-economic challenges and culture clash, young people struggle to define their identity. A third of Minnesota Somali households are single-parent with children,¹⁹ and while the children adopt English and begin to learn U.S. customs from school, the parents often remain isolated, lacking language skills and knowledge of public services. Young people are left to grapple with the inherent conflict between the lifestyle and worship taught by their elders and practiced at home and the secular, American culture they inevitably share by virtue of growing up in the United States. One source said: “There’s a lot of competing threats to a person’s sense of self-worth. And then, within that chaos of ‘who am I,’ it creates an opening for someone else to come in and kind of say, ‘This is who you are.’”

In this challenging environment, there can be a craving for structure and acceptance, one that is commonly found in America’s urban street gangs. Some young Somali men join Somali gangs, which *all* sources said present the greatest safety threat to the Minneapolis-St. Paul community. The Somali Outlaws and Madibon With Attitude (MWA), the two primary Somali gangs in Minneapolis-St. Paul, provide a social structure and identity compatible with U.S. culture (though not necessarily its laws). The Somali gang structure is not hierarchical like many U.S. and international urban gangs, though the groups do resemble American gangs in terms of fraternal structure. Seeking relationships and recognition they are unable to find at home, at school, and in the community, these young men are not unlike other ethnicities and nationalities that join gangs to replace critical social elements. In this regard, the attraction to gangs is universal, as they offer understanding and acceptance, becoming the members’ “real” family, the one they can always count on and who will never judge them.

Other young people, however, find structure in an increasingly rigid view of their faith, which may become incompatible with U.S. customs and laws. An increasingly absolute Muslim identity can be encouraged or exploited by a skilled recruiter. Studies show that immigrant adaptation to a new society is best achieved by embracing both an ethnic identity and the new national identity.²⁰ Foreign fighter recruiters strive to dispel the latter, disrupting an individual’s

¹⁹ U.S. Census, “American Community Survey.”

²⁰ See, Jean Phinney, et al. “Ethnic Identity, Immigration, and Well-Being: An Interactional Perspective,” *Journal of Social Issues*, 57, no. 3 (2001): 493-510; Francis Fukuyama, “Identity, Immigration, and Liberal Democracy,”

opportunity to assimilate and embrace the benefits of their new country. Thus, young people in Minneapolis are vulnerable not simply because they have opportunity to congregate in unsupervised spaces but, more fundamentally, because they are young people in a complex environment with limited familial guidance, conflicted and developing identities, and predatory terrorist recruiters.

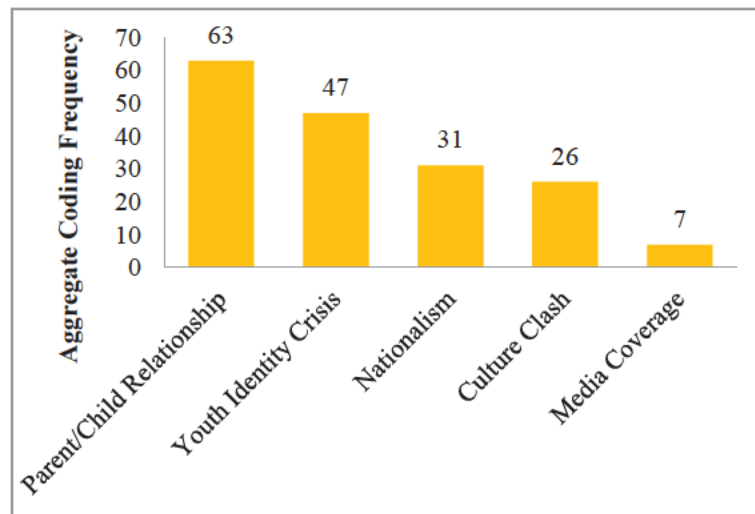


Figure 3 - Risk Factors for Recruitment

To be sure, there is no single factor responsible for causing an individual to become a violent extremist. There is no terrorist profile, though there are risk variables. In source interviews, the most commonly mentioned risk factor for recruitment in the Somali community is the difficult relationship between parent and child.²¹ Obstacles include language barriers between parent and child, long hours for working parents, and a child's abuse of

parental trust. The second most commonly mentioned risk factor was a youth identity crisis. The desire for structure and identity, coupled with a weak parent-child relationship, can make young people susceptible to a recruiter's message, particularly if they seek the approval of a surrogate family member (in the case of Amir Meshal) or a romantic interest (in the case of the aforementioned young woman). A nationalistic zeal²² for rebuilding Somalia and immigrant cultural conflict, inflamed by sensationalistic media coverage of terrorist threats, may also make a young person susceptible to a compelling terrorist narrative that leverages these themes.

Correcting Assumptions

There are two common assumptions made about extremist recruiting that our research revealed to be inaccurate in Minnesota. First, recruits from Minneapolis are not necessarily (or even primarily) lacking in opportunities for a successful future in the United States. Take the example

Journal of Democracy, 17, no. 2 (2006): 5-20; and Salman Akhtar, *Immigration and Identity: Turmoil, Treatment, and Transformation* (Jason Aronson: 1999).

²¹ This factor has been noted in studies of other communities and violent extremists, such as Tamerlan and Dzhokhar Tsarnaev, who attacked the 2013 Boston Marathon. See, Masha Gessen, *The Brothers: The Road to an American Tragedy* (New York: Riverhead Books, 2015), 73.

²² Sources indicated this risk factor with regard to previous al Shabaab recruiting and not with ISIL.

of Zakaria Maruf, relayed to us by one of his childhood friends who knew him before he left for Somalia in 2008.

Maruf was socially popular, athletic and succeeding in school. He was also affiliated with a Somali gang, which at the time called itself the “Somali Hot Boyz.”²³ After graduating from high school, Maruf separated from the gang and became increasingly religious, eventually becoming a teacher at a dugsi in the Cedar-Riverside neighborhood. Maruf swapped his gang-centered social structure for one founded on an ultra-strict interpretation of Islam. Based on the findings from this study, it seems clear Maruf did not travel to Somalia because he was poverty-stricken and hopeless but because his identity, based on a narrow interpretation of Islamic beliefs and a vague sense of nationalism, required it of him. As Maruf himself said in a 2009 statement broadcast over a Somali radio station:

“They want to make it appear as if the people who left or want to leave, those who migrated for the sake of Allah, were people who did not have a life, and they simply want to wrong their name. These are lies and propaganda. It is not possible to brainwash or coerce a conscious, grown man. And where we come from is not a place where people are coerced or brainwashed.”²⁴

The report authors did not find any direct link between Minnesota Somali gangs and terrorist recruitment, a view supported by law enforcement sources who monitor Somali gangs and engage the Somali-American community. A law enforcement gang officer said of gang members: *“They don't want that structure of trying to join ISIS or al Shabaab where they have someone telling them what to do. They want to be out there on the block, doing whatever they want to do.”*

Sources said that some of the individuals recruited by terrorist organizations may have been rejected from gang membership and thus open to other social networks and beliefs. One source suggested recruiters target gang members, their message being that gang affiliation and action is sinful and the target should conform to Islamic morals; however, no other source mentioned this phenomenon and the report authors were unable to find any evidence of it.

²³ Today, the gang calls itself the Somali Outlaws.

²⁴ “Radio Interview with Zakaria Maruf,” transcript, *The New York Times*, July 11, 2009.

The second inaccurate assumption is that social media has been the primary vehicle for ISIL recruitment efforts in the Twin Cities. In every incident reported during fieldwork, face-to-face interaction was a critical element of the recruitment process. Social media interaction and links to extremist online content reinforce the messages that recruiters offer in person. To be sure, digital communication plays a role in recruitment, but at least in the Somali community in Minneapolis-St. Paul, in-person interaction is irreplaceable.

There are chronic socio-economic challenges in Minneapolis-St. Paul among the Somali-American community. Even as terrorist recruiters hide in the population and seek vulnerable targets, the community is struggling with gang violence, poverty, racism, unemployment, and an ongoing need to assimilate to a new culture and country. While the challenges are great, there are a range of programs and organizations in Minnesota that are geared towards improving the welfare and quality of life of the Somali residents and countering the violent messages of ISIL and al Shabaab.

Countering Violent Extremism Programs in Minneapolis

In the Twin Cities, growing in tandem with the threat from ISIL recruitment are multiple programs that seek to dispel terrorist narratives, engage young people, and improve community engagement and quality of life. As a part of its August 2011 Countering Violent Extremism (CVE) strategy, the Obama Administration's "Strategic Implementation Plan (SIP) for Empowering Local Partners to Prevent Violent Extremism in the United States" focuses on three primary objectives: enhancing federal CVE community engagement; cultivating public sector expertise in CVE; and countering extremist messaging.

This initiative resulted in the development of a CVE pilot program in Minneapolis, led by U.S. Attorney Andrew Luger. The pilot focuses on stemming recruitment efforts by cultivating and funding youth programs, job training, and expanded after-school programs intended to facilitate mentorship. Working with community representatives, the pilot takes a holistic approach to improving the welfare and support for Somali-American young people in Minnesota. The pilot is also the basis for community-led intervention programs, making it easier for families to request help from mental health professionals, religious leaders, teachers, and others if their children are suspected of associating with, or being recruited by, terrorist organizations. This creates a safe way for the community to address threats and concerns without drawing undue attention from law enforcement, which is a pervasive fear throughout the community.

This government-supported, community-based strategy exists alongside independent, grassroots CVE efforts in Minneapolis-St. Paul. There are currently two types of programs that may have an impact on the thinking and actions of young people in Minneapolis: CVE-focused organizations; and community-improvement-focused organizations. Efforts in each area are yielding important advances in how the Minneapolis-St. Paul Somali community nurtures its younger populations and guards against extremist recruitment.

CVE Organizations in Minneapolis-St. Paul

Mohamed Ahmed is a husband and father, a manager at a convenience store, and the creator of *Average Mohamed*, a website (averagemohamed.com) presenting counter-radicalization messaging geared towards young people (ages 8 to 16). The project uses cartoons to present Islamic messages that counter the radical ideology preached by ISIL, al Shabaab, and other terror groups, approaching youth in a media format with which they are familiar and interested. Ahmed collaborates with local religious leaders to craft the messages in a way that relays Islamic ideas

while dispelling ISIL's ideology. Ongoing for nearly a decade, the project has been entirely conceived, funded and managed by Ahmed. He said of his project:

*"It takes an idea to defeat an idea. Extremist ideology must be competed against. It only takes an average man to radicalize and recruit vulnerable young people, and it only takes an average man to offer a different, peaceful narrative. Average Mohamed is the answer to the ongoing efforts to mislead our children."*²⁵

While Ahmed's efforts clearly align with the administration's SIP objectives, Ahmed and his project have no affiliation with government efforts, his work and successes existing outside the realm of government-driven initiatives. It is perhaps for this reason that Ahmed has been able to spread his message to the Minneapolis-St. Paul Somali youth without much community suspicion with regard to his motives, unlike other Minneapolis programs that the community widely believes to be pawns of Federal counterterrorism efforts.²⁶ Indeed, other studies have discovered that government sponsorship inevitably undermines the legitimacy of any program that counters extremist messaging from a theological perspective.²⁷

The cost of developing and operating *Average Mohamed* is significant for Ahmed, and while he says funding would be welcome, the report authors found opportunities to advance his effort without direct monetary support. For example, Dr. Erroll Southers was asked to speak to CNN's *New Day* in January about U.S. CVE efforts.²⁸ By sharing a University of Southern California article (also written by the report authors) with CNN, we were able to secure a joint interview on *New Day* with Southers and Ahmed. We also worked with Ahmed in his media relations with other news outlets. Finally, as global public awareness of Ahmed's project grew, we worked with him to plan a growth strategy, discussing a project transition into a non-profit and connecting Ahmed with experts in that field to advise him. Ahmed founded a non-profit in April 2015, asking Southers and Hienz to serve on the board of directors.

²⁵ "USC's CREATE Works with 'Average Mohamed,' a Grassroots Effort to Counter Foreign Fighters," *Sol Price School of Public Policy, University of Southern California*, Jan. 29, 2015.

²⁶ Specifically, some members of the community indicated they see the CVE organization Ka Joog as working for the FBI, a product of the organization accepting an FBI award. Further research is needed to enumerate the degree to which this perception is held in the community. See, "Somali-American Ka Joog Organization Honored for Community Leadership," *FBI Minneapolis Press Release*, Oct. 25, 2012.

²⁷ Todd C. Helmus, Erin York and Peter Chalk, "Promoting Online Voices for Countering Violent Extremism," RAND Corporation, 2013.

²⁸ New Day, "Group Works to Counter Radicalization," *CNN*, January 20, 2015
<<http://transcripts.cnn.com/TRANSCRIPTS/150120/nday.03.html>>.

There are other community-driven programs in Minneapolis that seek to prevent young people from embracing the extremist narrative. Examples include:

The Islamic Civic Society of America (ICSA): Based in Minneapolis, the ICSA strives to relay a view that Islamic tenets and civic principles in a democratic society are compatible. Importantly, given research findings on recruitment in Minneapolis, ICSA is focused on helping Muslims develop a personal identity that can safely accommodate both Islamic and secular principles. ICSA is affiliated with the Minneapolis Dar Al-Hijrah Mosque.

Somali Citizens League: A grassroots organization, the Somali Citizens League works with the Minneapolis community and law enforcement to advance the welfare of the local population through education, services and funding.

Ka Joog – A non-profit founded in 2007, the purpose of the organization is to provide “positive elements of education, mentorship, employment and the arts” to Somali youth in Minneapolis.²⁹ While the group is not only focused on preventing radicalization and recruitment, the genesis of Ka Joog can be traced to al Shabaab’s earlier success recruiting in the Twin Cities. The organization tracks academic grades, school attendance and “behavior changes,” while also working with parents. Data is collected every 90 days throughout a young person’s time in high school, and according to Executive Director Mohamed Farah, since 2007, no Ka Joog participants have been involved in recruitment or gangs. This is not proof of success, but it is “evidence of absence.”

Minneapolis Law Enforcement and Community Engagement

Multiple sources reported that the community relationship with local law enforcement has improved dramatically in recent years. One reason for this is a focused effort to hire Somali-Americans as sworn law enforcement officers and community liaisons. Somali-American police officers enforce the notion of community participation in public safety, and their work and insights profit local law enforcement a deeper cultural understanding of the communities they serve. This aligns with findings in previous research, indicating that when authorities are seen as

²⁹ Mohamed Farah, "Press Conference Statement," *Somali Current*, Jan. 20, 2015.

legitimate, “their rules and decisions are more likely to be accepted. Community engagement is—in part—an effort to make law enforcement authority more accepted within localities.”³⁰

In St. Paul, the city has created a council of Somali elders that advise the police department. The city’s Police Athletic League attracts hundreds of Somali young people, and the St. Paul Police Department has also hosted halal³¹ cookouts.³² Meanwhile, the Minneapolis Police Department (MPD) conducts ongoing programs to engage the community. The Somali Women and Women in Law Enforcement gatherings provide MPD an opportunity to interact directly with the mothers and other relatives of young people, building relationships that could lead to closer collaboration between law enforcement and the community when it comes to preventing radicalization and recruitment. An existing relationship increases the likelihood that a parent or other community member will report troubling changes in behavior and belief, or worse, a departure to join a foreign terrorist group. Al Shabaab has intimidated members of the community into silence, warning that if family members speak to authorities, they will never see their child again. For a parent, the smallest glimmer of hope that a child will come home is more palatable than any benefit that might be gained by working with authorities.

The MPD also operates a Youth Safety Camp where one primary goal is to engage Somali youth and create an environment where they can interact with the other community cultures in Minneapolis. This program is offered for middle school students so that when they reach high school, they have formed cross-cultural friendships, thus reducing the risk of culture-based conflict. The MPD is also planning to launch a new program, Conversations with Cops in Coffee Shops. With this program, police officers will frequent cafes where Somali-Americans congregate, particularly the Starbucks on Nicollet Ave. and Franklin St. in Minneapolis, where the clientele is largely Somali men from the community.³³ The goal is to increase communication with the Somali community and offer regular opportunities for citizens to have positive interactions with MPD.

³⁰ Jerome P Bjelopera, “Countering Violent Extremism in the United States,” *Congressional Research Service*, Feb. 19, 2014.

³¹ Food that is prepared in accordance with Islamic rules.

³² Executive Staff, FBI National Security Branch, “A New Approach to Countering Violent Extremism: Sharing Expertise and Empowering Local Communities,” *FBI Law Enforcement Bulletin*, October 2014.

³³ The report authors found that the patrons of this establishment can be an excellent source of information regarding the landscape of the community and its concerns.

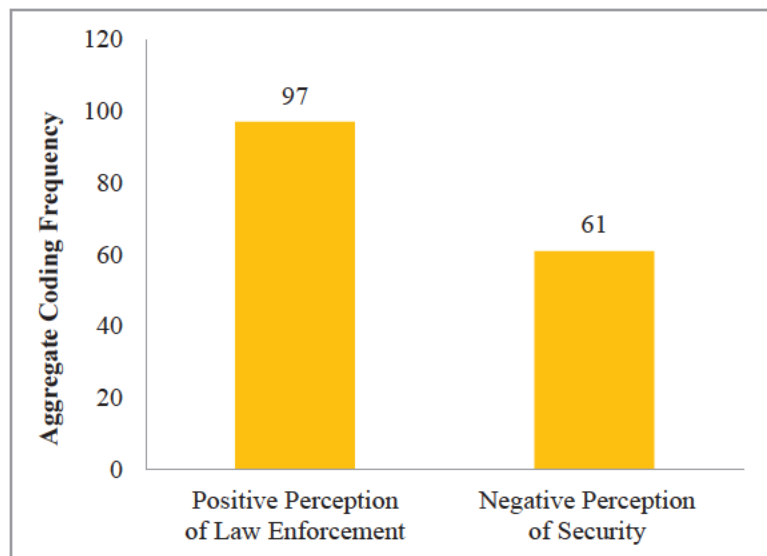


Figure 4 - Perceptions of Law Enforcement

These efforts by local police to engage the community are having an important, positive effect on perceptions of local law enforcement. In interviews, there were 97 instances of a positive perception of law enforcement, and of these, 66% were specifically in reference to MPD, the department's value, and how their presence in the community is yielding positive outcomes. This positive view leads to greater trust between the community and law enforcement, which can yield

more effective collaboration in addressing community concerns and identifying bad actors in Minneapolis-St. Paul. Even as the community-police relationship is improving, there remains a reticence to proactively inform police about a case of radicalization and recruitment. During the first meeting with a community engagement officer in Minneapolis, the report authors were told, "You found out more in two days than I've found out in two years."

While local police efforts have improved relationships, the community's positive sentiment towards law enforcement does not extend to the federal level. There were 61 instances of a negative perception of law enforcement, and 65.5% were specifically in reference to the FBI. The Bureau has been working with local law enforcement to engage the community; for example, attending community meetings and participating in Somali Independence Day celebrations.³⁴ Yet, the FBI remains in a perceived adversarial role vis-à-vis the Somali-American community in the Twin Cities.

Community Organizations and CVE

There are 35 nonprofit organizations in Minnesota that serve the Somali-American community, and 23 of these are in Minneapolis-St. Paul, according to ChairtyNavigator.org. In addition, there are organizations and programs that exist outside the nonprofit arena. One of the most widely known and respected of these is the West Bank Athletic Club (WBAC), run by a man known throughout the community simply as "Coach."

³⁴ FBI, "A New Approach to Countering Violent Extremism."

Coach Ahmed is the founder and leader of the WBAC soccer teams. Founded in 2012, WBAC works with Minneapolis young people year-round. Interest and participation has steadily grown over the last three years. There are currently 45 young people (14-19 years old) playing for WBAC, split into three teams of 15 players. However, there are 150 young people on a waiting list, indicating the massive interest in the club, as well as the consequences of severely limited funding. WBAC is working to secure funds for practice space and equipment and aspires to have 10 to 12 teams catering to players 5 to 18 years old.

As a part of our fieldwork, the report authors attended soccer practices and team gatherings. One of the club's 19-year-old members spoke about how Coach Ahmed plays an active role in young Somali-Americans' lives that stretches beyond the soccer field. He said:

"My coach is really good. He takes me home most of the time. He gives us rides when I don't have one because my mom doesn't drive...he waits for me until I get in the house. Then he'll call, 'Are you safe?' I'm like, 'Yes, Coach.'"

"Coach always tells us, 'Stay away from bad things and bring in grade reports. Stay good in the school. I'm not coaching you guys because you are the best players. I'm coaching you guys so you can be something later on. I want you guys to play for colleges. I want to see you getting good grades.' He's getting us a tutor so he can help us with math, so our GPA can go up and our soccer will be good and then we'll be good enough."

This focus on personal and academic development is similar to other organizations in Minneapolis-St. Paul, but critically, Coach Ahmed is not paid for his work, the costs of practice areas and equipment funded by family and community donations. Far from the million-dollar-grant aspirations of other organizations, Coach Ahmed is focused entirely on the wellbeing of his soccer players. In structured interviews, there were 135 statements championing Coach Ahmed and his program, and multiple sources reported, "Coach is doing the real work."

This common refrain was not simply an acknowledgement of Coach Ahmed's impressive work but also an implicit criticism of other individuals and organizations that claim to help Somali-American youth in Minnesota but ultimately are motivated to increase personal wealth and prestige through grant money intended for the community's young people. The community calls these people and organizations "The Pretenders."

The Pretenders

There are competing interests among the community-based organizations in the Twin Cities. There is some rivalry between organizations vying for grant money, and there are enduring clan allegiances that have carried over from Somalia. Thus, a criticism of a specific group must be assessed not just for its validity but also for whether it is a self-serving criticism intended to tilt perception in favor of the criticizer. That said, there is a persistent view throughout the community that there are individuals and organizations that have become adept at securing government funding, though that funding is not directed to the intended recipients of the aid (i.e., Somali-American young people). This sentiment, mentioned 72 times during interviews, is pervasive in Minneapolis-St. Paul. Anecdotally:

A Somali Law Enforcement Officer said:

There are a lot of community organizations who get money in the name of the community and never come back...So-called Somali community leaders have been receiving money from the city or the state or local but the community never benefit. They benefit only that little group. And the community is pissed off.

One of Coach Ahmed's soccer players said:

"Most of the leaders in the community, most of them tell us, 'We'll do something for you guys,' but they never have done anything. The coach is like, 'We'll help you guys. We'll come everywhere. I'll call the kids.' But [the Pretenders] make a promise and then they never make it up."

Another source was even blunter:

"[The Pretenders] are bloodsuckers. All they need is the paycheck. They don't care about the ills and the problems."

And during a protest in the Cedar-Riverside neighborhood, Mubashir Jeilani, co-founder of Cedar Riverside Youth Council, told the *Twin Cities Daily Planet*:

“Our real problems are community development. We have so many different organizations claiming that they help our youth, but...they don’t help us.”³⁵

How are leaders able to secure funding when they are not effecting change in the community? In the words of another source, “The community leader programs always pass. I’m sure they’ve been vetted. They just pass. They know the loopholes and what they need to do.”

Sources recounted a troubling anecdote that evidences this ability to pass official assessments. During DHS Secretary Jeh Johnson’s 2014 visit to Minneapolis to meet with community leaders, he sat with individuals who claimed to be CVE advocates but, according to sources, were previously proponents of al Shabaab *and* its extremist message.

The Pretenders are skilled at manipulating information and imagery to secure funding. Coach Ahmed recounted instances where organizations asked him to bring some of his soccer players to an event or meeting, so the organization could claim they help a given number of young people. Yet, time and again, Coach Ahmed said, these organizations do not use their funding to help the young people as they claimed they would.

It is this phenomenon of a Pretender that makes program validation difficult, inconsistent and potentially misleading. A rigorous vetting process does not necessarily reveal a Pretender, as sources reported they are good at being vetted.

CVE Program Recommendations

It is not possible to prove a negative. No organization can claim with certainty that their work directly prevented or reduced the risk of radicalization and recruitment because it is impossible to identify who would have become an extremist without the organization. Perhaps the most that can be hoped for is “evidence of absence:” a lack of recruitment for a given group *suggests* that the group is successful in preventing recruitment. Yet, even this is a challenge for many Minnesota organizations, as metrics tracking appears to be a secondary priority to the work of

³⁵ Parker Lemke, “In Cedar-Riverside protest, youth link terrorist recruitment to lack of resources,” *Twin Cities Daily Planet*, Oct. 1, 2014.

the program. This is somewhat understandable, particularly for the community organizations that are run with virtually no budget and limited staff.

There are numerous Minneapolis-St. Paul organizations focused on helping young people resist recruitment, but Somali-American youths continue to depart to join foreign terrorist groups. On each visit to Minneapolis, the report authors were informed that more young people had left, and on each occasion, at least one of these missing young people was not reported to police.³⁶ Clearly, current programs are insufficient to stem the flow of fighters to ISIL. More needs to be done. This does not necessarily mean increased funding, but instead, a smarter, more strategic application of funds to programs that reflect the stated needs of the community and are continually delivering evidence that funds are spent on real, immediate efforts and not used as a way to increase personal income and prestige.

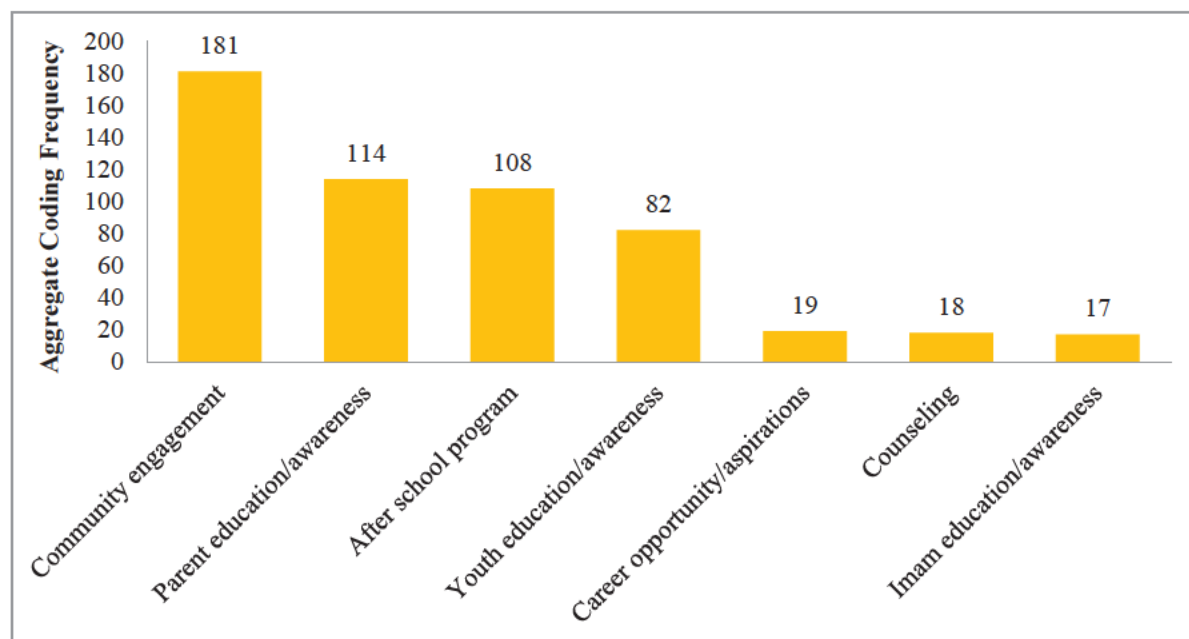


Figure 5 - Community Program Recommendations

Sources were asked to recommend important elements in a CVE program. The community's recommendations focused on a holistic, integrated approach to supporting young people and their families. "Community engagement" was by far the most commonly mentioned element.

³⁶ The report authors provided this information to Minneapolis police without compromising the anonymity of our sources.

The community wants to be a part of the effort to stem violent extremism, and the efforts by local law enforcement to work with the community are having an important effect.

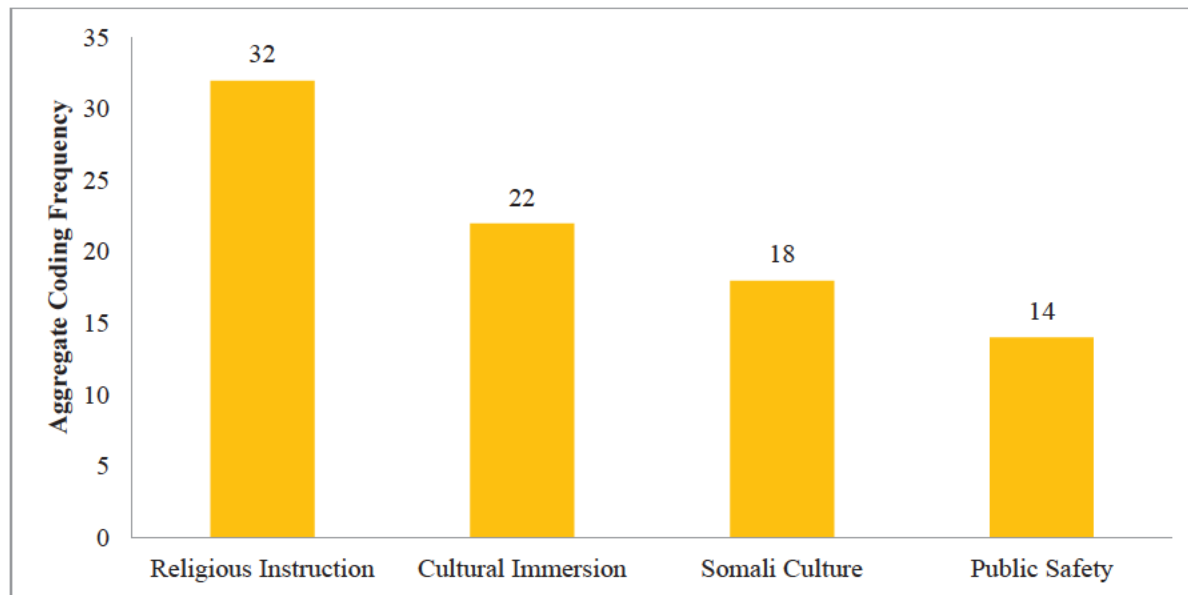


Figure 6 - Youth Program Recommendations

The involvement of schools and teachers in parental and youth education and afterschool programs was also widely cited. For youth programs, religious instruction was identified as the most important element. A clearer understanding of religious texts and beliefs can undercut the violent theological message of terrorist recruiters, and it can also support healthy identity formation, as young people understand, via legitimate community-led education, that Islamic beliefs and a secular society can safely exist simultaneously in one's view of themselves. Likewise, the importance of cultural instruction was emphasized with regard to Somali tradition, history and language, *as well as* U.S. culture, civic principles, and pluralism.

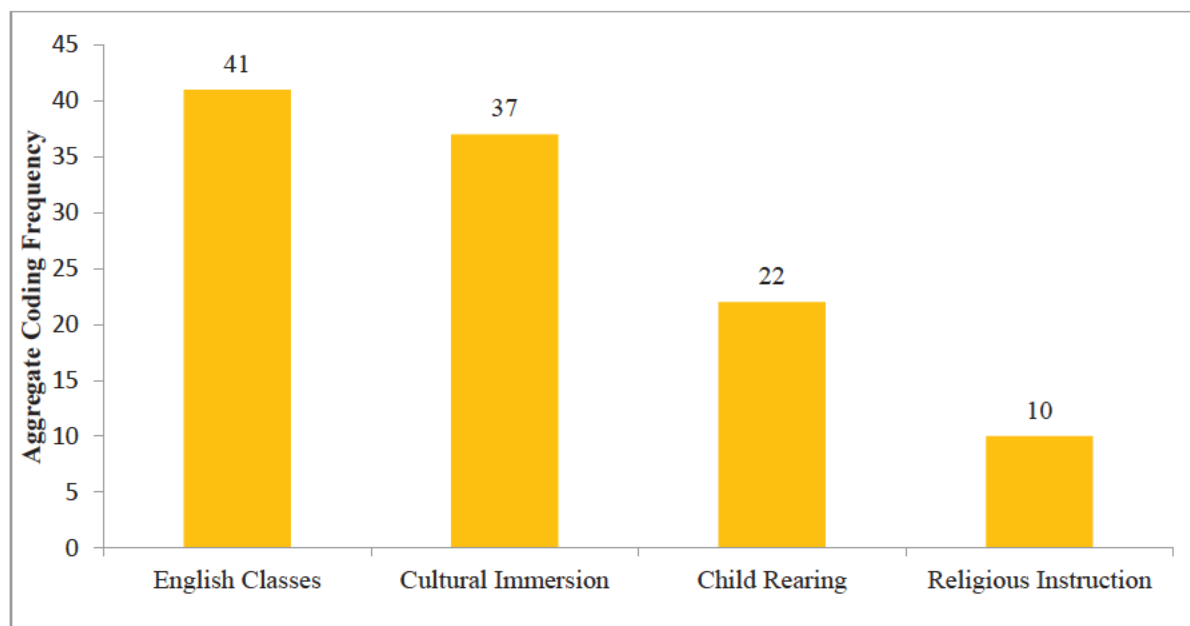


Figure 7 - Parental Program Recommendations

For both parental and youth programs, guidance on cultural immersion was cited as an important element, indicating a community-wide recognition that after immigration, new residents require further support to fully embrace their new home. For parental education programs, sources more commonly noted practical topics: learning to speak and read English; and advice for child rearing. The latter is particularly important because 34.6% of Minnesota Somali households are single parent, a challenge for any family that is exacerbated in Minneapolis-St. Paul by the challenge of assimilating to a new country.

There are cascading benefits that can be realized by engaging parents in the Minneapolis-St. Paul school systems, including the Somali charter schools. The director of a Minneapolis dugsi said that his school serves as a hub for the community, helping parents navigate a new culture and country while also supporting their children’s education. The director said that the three primary challenges for families are “translation, transportation and connectivity.”

Language barriers can preclude parents from fully engaging a new society. At the same time, parents might have limited mobility. Particularly in the sub-zero temperatures of a Minnesota winter, the inability to drive and navigate the city isolates parents and challenges assimilation. With language and transportation barriers, parents can find it difficult to access the social, medical and legal services available in the United States.

The dugsi director explained how his organization is working to engage parents more fully in the education of their children, using it as an opportunity to address the core community challenges.

Conducting Fieldwork in an Immigrant Community

The first interview the report authors conducted in Minneapolis was held in the evening, in a back office of a brick two-story building in the Cedar-Riverside neighborhood, the epicenter of Somali immigration to the United States. We were led into a small room where we found several Somali men and women with uncertain gazes. They closed the door, and the eldest figure in the room leaned forward and asked, “What do you want?”

As the conversation evolved, it was clear they had researched us, though we knew very little about them. Each of the people in that room ultimately became an essential source for the findings in this report. Indeed, this group came to refer to the report authors as “family.” We ate dinner together, went to Somali Islamic schools, and watched young people play soccer. We learned about their families, their backgrounds, and their admirable embrace of American society. Over the course of three trips, these connections opened the Somali-American community to us in a way that is not often reflected in previous studies of the Twin Cities communities. The question is, why were we successful in eliciting so much information, in a matter of months, when previous researchers found the community to be closed and unwilling to talk?

Based on this research experience, there are several evident best practices for conducting research in the Minneapolis-St. Paul Somali community, and potentially, in immigrant communities across the country.

Leveraging Backgrounds

The report authors recognized early on that there were two critical attributes that allowed us to quickly establish common ground with our sources, the basis for trust and collaboration. Dr. Erroll Southers is African American. The advantage of his ethnicity was most clearly seen during our first visit, when a resident said, “*I am African. You are African-American. You know exactly what we go through in America.*”

The individual was explaining the consequences of profiling, exacerbated by immigration and the ongoing homeland security threats. While infrequently mentioned directly, sources exhibited comfort and familiarity during interviews and subtly acknowledged that Souther's race made a difference to them.

Justin Hienz is a scholar of religion with years of academic and professional study of Islam, including time spent living and traveling throughout the Middle East. Hienz's deep familiarity with Islamic texts, terms, history and other religious ideas allowed the report authors to immediately evidence our appreciation for and understanding of our sources' belief system. Several sources remarked, "*You know more about my religion than I do.*"

These two qualities—Souther's ethnicity and Hienz's understanding of Islam—allowed the report authors to connect with sources on the two parts of their identity that create the most concern in Minneapolis-St. Paul. Racial tensions in Minneapolis create a sense of isolation for the Somali-American community, and Souther's ethnicity inherently implied to sources that he could understand their concerns and experiences on a personal level. Meanwhile, given the noted perception of government animosity towards Islam, Hienz's ready knowledge of the faith implied to sources that they could speak openly without fear of being misinterpreted, including frank conversations on the concept of jihad, which, while a dangerous motivation for violent extremism, is also a legitimate, sacred-text-based Islamic concept.

Future researchers would do well to consider their own backgrounds and whether they can be leveraged to establish common ground and trust. One critical question every researcher should ask themselves *before* commencing fieldwork is, *Am I the right researcher for this project?* Intellect and professional accomplishments are not always sufficient to yield valid, deep insights in a community cautious of outsiders.

Honesty and Transparency

While the report authors were aware of the benefits of their respective backgrounds, they were also keenly aware of the drawbacks. Dr. Souther is a former FBI Special Agent and a career law enforcement officer. Given the animosity towards federal law enforcement, this professional background could have presented an impediment to trust and openness. The report authors were aware of this potential conflict before arriving, and from the initial meeting with community leaders through the final interview conducted for this report, Dr. Souther purposefully informed each source that he formerly worked for the FBI. This forthrightness yielded candid, often-

negative statements about the Bureau's CVE efforts, though comments were offered in a way that acknowledged Southers had no responsibility for the FBI's perceived missteps.

This transparency cultivated trust in part because many of the sources had researched Dr. Southers and were already aware of his previous work with the FBI. His readiness to admit his work for the Federal government evidenced honesty. Had he concealed any part of his background, most sources would have recognized deceit and reciprocated with less-than-truthful responses during interviews.

Likewise, the report authors did not hesitate to tell sources that this project has been funded by the Department of Homeland Security Science and Technology Directorate. Nor did we conceal that our primary interest was in the foreign fighter recruitment occurring in Minneapolis-St. Paul, a sensitive topic in the community that has attracted significant attention—and generated significant resentment of federally funded research efforts.

Overcoming Preconceived Notions

One of the first and most frequent criticisms the report authors heard from sources about other research efforts was that the community feels like an experiment under observation, like “lab rats.” After years of researchers, journalists, government offices, and other organizations coming to Minneapolis-St. Paul to study radicalization and recruitment, many in the community feel that all promises of help are hollow, all declarations of support self-serving.

Particular grievance was expressed regarding a study in which the researchers reportedly paid individuals for interviews. The principal investigator was characterized as aggressive and insulting, and the injection of money created tension within the community. This evidenced, in the eyes of our sources, a distinct absence of respect and appreciation for the community. As a result of this blunt approach, sources said they were less than forthcoming with interviewers, withholding critical information that by consequence made the study incomplete and in some cases, inaccurate.

Sources used this example of a poorly conducted study to highlight why we were being given so much information and access to the community. Sources mentioned the value of relationship building 42 times, indicating it is a widely shared sentiment. The community is willing to work with people who take time to build trust. On our first visit to Minneapolis, we spent more time

listening than asking questions. We did not conduct structured interviews and did not record any discussions. During most conversations on the first visit, there was little or no talk about terrorism or terrorist organizations, foreign fighters, or CVE. This gave sources time to assess the motivations and forthrightness of the report authors, allowing trust to develop naturally, a tactic that proved vastly more productive than offering money for interviews.

Encouraging Community Collaboration

Sources also indicated that because the report authors showed genuine interest in the community, its challenges *and* its accomplishments, they were more willing to discuss the primary research interest—terrorist recruitment and methods for countering it. Despite the focus of this report, interviews always began with questions about where the sources had lived in the United States, their path to Minneapolis and the primary public safety concerns for their community. With few exceptions, it was not until midway through interviews that the topic of extremism and recruitment was raised. Sources were consistently aware of the report authors’ primary research interest, but focusing on the source’s personal history and concerns evidenced genuine interest in the source, by consequence building a trust level that allowed sources to feel comfortable discussing a sensitive topic.

Yet, the purpose of the questions regarding community concerns was not simply to engender trust and comfort with the report authors. Potential violent extremists all have families and live in communities that possess the potential to reduce the risk of a deadly attack. With an appreciation of how charismatic figures, group dynamics, and the radicalization pathway contribute to the emergence of violent extremism, it is essential to understand and leverage a community’s identified priorities as a means to enhance public safety (and reduce the risk of foreign fighter recruitment). Doing so requires a more nuanced community-based strategy, a *Mosaic of Engagement*. This is the concept of a “community-based strategy to improve the quality of life by reducing the risk of extremist recruitment, radicalization and related criminal activity. This goal is only feasible through engagement of *tipping point* stakeholders via Neighborhood Alliances, as well as community consensus that [homegrown violent extremism] reduction is the desired by-product of a safe community.”³⁷

Committing to Long-term Engagement

Another frequent criticism of previous research efforts was that interest in the Somali community lasted only as long as the research project. Community members complained that they had not

³⁷ Erroll Southers, *Homegrown Violent Extremism* (Routledge, 2013), 107.

seen positive results from supporting research efforts in the past and felt that despite their readiness to help, researchers consistently abandoned the community when the research funding was exhausted.

Recognizing the enormous public safety and national security concerns in the Twin Cities and the chronic socio-economic challenges to the Somali-American community, the report authors committed early in this research to long-term, ongoing work with the community. During our second visit to Minneapolis, multiple sources reported that they were “shocked” that the report authors returned, surprised because previous researchers (evidently) did not return after the initial visit.

This kind of ongoing research profits not just initial information but instead an invaluable relationship that affords the kind of openness and trust that is essential for understanding the constant evolution of terrorist recruiter tactics and targets in Minneapolis-St. Paul. Put another way, ongoing research yields tremendous assets for future projects and initiatives.

Research Limitations

Even as the report authors successfully accessed a complex community, rapidly building trust and learning critical information, there were aspects of the research effort that presented limitations. There were practical challenges, such as the project’s time constraints, limited timeframes where both report authors could set aside other professional responsibilities and travel to Minnesota to conduct the fieldwork, and the freezing Minnesota weather, which tended to keep residents home, indoors, and overall less mobile and available.

The report authors also faced the challenge of conducting fieldwork while simultaneously growing the network of sources and establishing trust with them. During the first visit, we were dependent on a limited number of individuals to assist in identifying and locating people who might participate in the study. In time, the report authors’ network of sources began to grow independently and exponentially, with people eager to talk, contribute, and offer further introductions to worthwhile sources. What is more, the report authors have mentioned this study during lectures and presentations throughout the country, and that has profited additional contacts from people who know residents in the Cedar-Riverside community. Continued research in Minneapolis-St. Paul will inevitably be more productive as we now have dozens of contacts who have stated a readiness to continue working with the report authors.

Another challenge was ensuring that we interviewed a representative cross-section of the Twin Cities Somali community. Many clan and sub-clan allegiances, carried over from Somalia, perpetuate in the cities, and while clan divisions were characterized as antiquated and fading, it remains a factor in developing relationships and capturing an accurate, comprehensive picture of the community. The report authors were told by sources that future research must purposefully engage more clans or else segments of the community will assume that the report authors are advocates of specific groups, rather than objective researchers interested in the entire community. Yet, achieving this is made difficult by the fact that it is considered inappropriate (if not completely taboo) for people outside the community to inquire about clan affiliation. Thus, future research will demand that the report authors navigate an issue about which they cannot directly ask.

These research tactics proved successful in ingratiating the report authors with the community, rapidly yielding critical information and insights. It is remarkable that simply by listening, showing respect and allowing the community time to assess the report authors, sources shared information that is typically not discussed outside the Somali community. One cannot conduct counterterrorism research from behind a desk, and the results of this project are evidence of that.

Conclusions

While this qualitative field study has ended, the work in Minneapolis-St. Paul is far from over. This study was the first step on a long road to addressing the chronic challenges in the Minnesota Somali community and halting ISIL's recruitment efforts. The findings are critical to the larger global effort to defeating and destroying ISIL. The most essential findings are that:

- ISIL has appropriated the al Shabaab recruiting network in Minneapolis-St. Paul;
- Recruitment in Minnesota includes face-to-face interaction and is not solely a social media-driven effort;
- One of the core factors in vulnerability to recruitment is a young person's crisis of identity; and
- There are individuals and organizations in Minneapolis-St. Paul who are adept at securing government funding without effecting any real change in the community.

Just as important as these findings, however, is that the report authors now hold strong relationships with many members of the Minneapolis-St. Paul Somali community and have opportunities to expand our network of sources and elicit even more critical information. As noted above, the Somali community desires help in preventing their young people from being drawn abroad, provided they are approached as partners in the effort. The report authors evidenced this approach to CVE during the course of this study, and going forward, continued collaboration will yield the greatest benefit to the community, as well as great gains for U.S. national security and the fight against ISIL.

Considering next steps, members of the Hennepin County Sheriff's Office have offered to coordinate a series of roundtable discussions between community religious leaders, law enforcement and the report authors. The information gleaned from these conversations will be invaluable in continuing to understand the nature of the evolving foreign fighter threat and how CVE programs can be developed to address it.

Following on findings in this study, the report authors are preparing to return to Minnesota to speak with a wider sample of the Twin Cities age cohort potentially vulnerable to recruitment so as to more finely understand the nuances and factors that recruiters exploit in the community. In

addition, the report authors will also strive to specifically identify ISIL recruiters in the community.

The incredible access and trust the community has offered will undoubtedly lead to information and insights that can only be gained through collaboration and collective agreement that ISIL recruiters can, will, and must be defeated. The report authors, as well as the sources for this study, are committed to continuing their research, analysis, and support until terrorist recruiters are expelled from Minneapolis-St. Paul.

References

- Akhtar, Salman. *Immigration and Identity: Turmoil, Treatment, and Transformation*. Jason Aronson: 1999.
- Alahdad, Ziad, et al. "Countering Violent Extremism: Scientific Methods & Strategies." *Topical Strategic Multi-Layer Assessment and Air Force Research Laboratory Multi-Disciplinary White Paper in Support of Counter-Terrorism and Counter-WMD*. September 2011.
- Al-Shabaab Appears to Call for Attacks on Minnesota's Mall of America, Other Malls. *CBS News*. February 21, 2015.
- Bjelopera, Jerome P. "Countering Violent Extremism in the United States." *Congressional Research Service*. February 19, 2014.
- Bradbury, Mark and Sally Healy. "Endless War: A Brief History of the Somali Conflict." *Whose peace is it anyway? Connecting Somali and International Peacemaking*. 2010.
- Brown, Christopher. *Countering Radicalization Refocusing Responses to Violent Extremism within the United States*. Master's Thesis, Naval Postgraduate School, 2011.
- Carpenter, J. Scott, et al. "Fighting the Ideological Battle: The Missing Link in U.S. Strategy to Counter Violent Extremism." *The Washington Institute for Near East Policy*. July 2010.
- Charmaz, Kathy. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. London: Sage, 2006.
- Corbin, Juliet and Anselm Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 3rd ed. Thousand Oaks, CA: Sage, 2007.
- Currier, Cora. "Spies Among Us: How Community Outreach Programs to Muslims Blur Lines between Outreach and Intelligence." *The Intercept*. January 21, 2015.
- Dickson, Louise. "Revival of the Civic Spirit: Contradictions in Somali-American Citizenship." *Bildhaan: An International Journal of Somali Studies*. 2011.
- Dirie, Fartun. "Mental Maps: Gaining Insight into the Diverse Somali Perceptions of Residential Desirability in the Twin Cities." *Midwestern Undergraduate Geography Symposium, Macalester College*. April 27, 2013.

Executive Staff, FBI National Security Branch. "A New Approach to Countering Violent Extremism: Sharing Expertise and Empowering Local Communities." *FBI Law Enforcement Bulletin*. October 2014.

Farah, Mohamed. "Press Conference Statement." *Somali Current*. January 20, 2015.

Farid, Mohamed, and Don McMahan. *Accommodating and Educating Somali Students in Minnesota Schools: A Handbook for Teachers and Administrators*. St. Paul, MN: Hamline University Press, 2004.

FBI Minneapolis. "Somali-American Ka Joog Organization Honored for Community Leadership." *Press Release*. October 25, 2012.

Fergusson, James. *The World's Most Dangerous Place: Inside the Outlaw State of Somalia*. Da Capo Press, 2013.

Fukuyama, Francis. "Identity, Immigration, and Liberal Democracy." *Journal of Democracy*. 17, no. 2 (2006): 5-20.

Gerges, Fawaz. *Journey of the Jihadist: Inside Muslim Militancy*. Orlando, Fla.: Harcourt, 2006.

Gessen, Masha. *The Brothers: The Road to an American Tragedy*. New York: Riverhead Books, 2015.

Ghalib, Jama Mohamed. *The Cost of Dictatorship: The Somali Experience*. New York: Lilian Barber Press, 1995.

Goodstein, Laurie. "Police in Los Angeles Step Up Efforts to Gain Muslims Trust." *The New York Times*. March 9, 2011.

Goodstein, Laurie. "U.S. Muslims Take On ISIS Recruiting Machine." *The New York Times*. February 19, 2015.

Hammond, Laura, et al. "Cash and Compassion: The Role of the Somali Diaspora in Relief, Development, and Peace-Building." *UN Development Programme*. 2011.

Hansen, Stig Jarle. *Al-Shabaab in Somalia: The History and Ideology of a Militant Islamist Group, 2005-2012*. New York: Columbia University Press, 2013.

Harper, Mary. *Getting Somalia Wrong?: Faith, War and Hope in a Shattered State*. London: Zed Books, 2012.

Hellyer, Caroline. "ISIL courts al-Shabab as al-Qaeda ties fade away." *al Jazeera*. Mar 23 2015.

Helmus, Todd, Erin York and Peter Chalk. "Promoting Online Voices for Countering Violent Extremism." RAND Corporation. 2013.

Henry, Devin. "U.S. Attorney Luger Pitches Outreach Plan to Fight Terror Recruitment, with a Promise: 'No Surveillance.'" *Minneapolis Post*. February 19, 2015.

Holmer, Georgia. "Countering Violent Extremism: A Peacebuilding Perspective." United States Institute of Peace. August 29, 2013.

Horgan, John. *Walking Away from Terrorism: Accounts of Disengagement from Radical and Extremist Movements*. London: Routledge, 2009.

Husain, Ed. *The Islamist: Why I Joined Radical Islam in Britain, What I Saw inside and Why I Left*. London: Penguin, 2007.

Kapteijns, Lidwien. *Clan Cleansing in Somalia: The Ruinous Legacy of 1991*. Philadelphia: University of Pennsylvania Press, 2013.

Kenya attack: 147 dead in Garissa University assault. *BBC News*. April 3, 2015.

Kerry, John. "Outlining an Action Agenda to Counter Violent Extremism." U.S. Department of State. February 19, 2015.

Khalil, Lydia. "US Counter-radicalisation Strategy: the Ideological Challenge." Australian Strategic Policy Institute. January 11, 2011.

Kosseim, Amin. "Counter-radicalization Best Practices in the United States and Lessons Learned from Abroad." *Thesis*, Naval Postgraduate School, 2011.

Koumpilova, Mila. "New Somali Refugee Arrivals in Minnesota Are Increasing." *Minneapolis Star-Tribune*. November 1, 2014.

Lemke, Parker. "In Cedar-Riverside protest, youth link terrorist recruitment to lack of resources." *Twin Cities Daily Planet*. October 1, 2014.

Leiter, Michael. *Nine Years after 9/11 Confronting the Terrorist Threat to the Homeland: Hearing before the Committee on Homeland Security and Governmental Affairs*. United States Senate. Washington, DC: GPO, 2011.

Levitt, Matthew. "From the Boston Marathon to the Islamic State: Countering Violent Extremism." *The Washington Institute for Near East Policy*. April 1, 2015.

Longstaff, Patricia, Nicholas Armstrong, Keli Perrin, Whitney May Parker, and Matthew Hidek. "Building Resilient Communities: A Preliminary Framework for Assessment." *Homeland Security Affairs*. 6, no. 3 (2010).

Lyden, Tom. "EXCLUSIVE: Man booted from Minn. mosque an ISIS recruiter or FBI mole?" *Fox 9 KMSP-TV*. October 5, 2014.

McEnroe, Paul and Allie Shah. "Federal Grand Jury Targets Local Terrorist Pipeline." *Minneapolis Star-Tribune*. September 20, 2014.

Nelson, Rick and Ben Bodurian. "A Growing Terrorist Threat? Assessing 'Homegrown' Extremism in the United States." *Center for Strategic and International Studies*. March 2010.

Neumann, Peter. "Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s." *International Centre for the Study of Radicalization*. January 26, 2015.

Neumann, Peter. *Preventing Violent Radicalization in America*. Bipartisan Policy Center. June 2011.

New Day. "Group Works to Counter Radicalization." *CNN*. January 20, 2015
<<http://transcripts.cnn.com/TRANSCRIPTS/1501/20/nday.03.html>>.

Obama, Barack. "Remarks by the President at the Summit on Countering Violent Extremism." *The White House*. February 19, 2015.

Office of the Press Secretary. "Statement from the Press Secretary on the White House Summit on Countering Violent Extremism." *The White House*. January 11, 2015.

Olsen, Jennie. "EXTENDED INTERVIEW: U.S. Attorney Discusses Terrorism in Minnesota." *KSTP*. February 18, 2015.

Onyanga-Omara, Jane. "British YouTube Star Keeps Kids off the Extremist Path." *USA Today*. April 6, 2015.

Onyanga-Omara, Jane. "Teens Stopped at Sydney Airport on Suspicion of Trying to Join ISIL." *USA Today*. March 8, 2015.

Patton, Michael Quinn. *Qualitative Research and Evaluation Methods*. Thousand Oaks, CA: Sage, 2002.

Perkins, Samuel J. *Homegrown Terror and American Jihadists: Addressing the Threat*. Hauppauge, NY: Nova Science Publishers, 2011.

Phinney, Jean, et al. "Ethnic Identity, Immigration, and Well-Being: An Interactional Perspective." *Journal of Social Issues*. 57, no. 3 (2001): 493-510.

Radio Interview with Zakaria Maruf. Transcript. *The New York Times*. July 11, 2009.

Rice, Susan. "Remarks by National Security Advisor Susan E. Rice at the White House Summit on Countering Violent Extremism." *The White House*. February 19, 2015.

Ross, Daveed. *My Year Inside Radical Islam: A Memoir*. New York: Penguin, 2007.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-first Century*. Philadelphia: University of Pennsylvania Press, 2008.

Schanzer, David, Charles Kurzman and Ebrahim Moosa. "Anti-Terror Lessons of Muslim-Americans." National Institute of Justice. January 6, 2010.

Shane, Scott. "From Minneapolis to ISIS: An American's Path to Jihad." *The New York Times*. March 21, 2015.

Somanader, Tanya. "President Obama on the Causes and Antidotes to Violent Extremism." *The White House*. February 19, 2015.

Southers, Erroll. *Homegrown Violent Extremism*. Routledge, 2013.

Sol Price School of Public Policy. "USC's CREATE Works with 'Average Mohamed,' a Grassroots Effort to Counter Foreign Fighters." University of Southern California. January 29, 2015.

Stern, Jessica. "ISIS's Apocalyptic Vision." Hoover Institution, Stanford University. February 25, 2015.

Stern, Jessica. *Terror in the Name of God: Why Religious Militants Kill*. New York: Ecco, 2003.

United States Census Bureau. "2013 American Community Survey of Somalis 3-yr Estimate." U.S. Department of Commerce. 2013.

United States Government Accountability Office. "Countering Violent Extremism Additional Actions Could Strengthen Training Efforts: Report to the Committee on Homeland Security and Governmental Affairs." *GAO-13-79*. 2012.

United States Senate. "The Roots of Violent Islamist Extremism and Efforts to Counter It." *Hearing before the Committee on Homeland Security and Governmental Affairs*. Washington, DC: GPO, 2009.

United States Senate. "U.S. Government Efforts to Counter Violent Extremism." *Hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services*. Washington, DC: GPO. 2011.

United States Senate Minority and Majority Staff. *Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat*. Washington, DC: U.S. Senate Committee on Homeland Security and Governmental Affairs. 2008.

Weine, Steven, et al. "Community and Family Approaches to Combating the Radicalization of Somali-American Refugee Youth and Young Adults: A Psychosocial Perspective." *Dynamics of Asymmetric Conflict*. 2 (2009).

Weine, Steven, and Osman Ahmed. "Building Resilience to Violent Extremism Among Somali-Americans in Minneapolis-St. Paul." *National Consortium for the Study of Terrorism and Responses to Terrorism*. August 2012.

White House. "Empowering Local Partners to Prevent Violent Extremism in the United States." August 2011.

Wood, Graeme. "What ISIS Really Wants." *The Atlantic*. March 2015.

Yan, Holly and Nima Elbagir. "Authorities Scramble to Find Teen Girls Before They Join ISIS." *CNN*. February 23, 2015.

Yuen, Laura. "Luger Releases Minnesota Anti-Radicalization Plan." *MPR News*. November 24, 2014.

Yuen, Laura. "Suspensions, Speculation Grow as FBI's Minn. Terror Probe Churns." *MPR News*. November 13, 2014.

Yuen, Laura. "Twin Cities Leaders Take Anti-extremism Efforts to White House." *MPR News*. January 23, 2015.