Forging a New Legacy

Homeland Security Investigations

National Security Investigations Division

Visa Security

Social Media Pilot Program

DNI Open Source Center
Open Source Academy

Social Media for Intelligence Professionals

Site Summary List

Social Networking

Facebook	General network	www.facebook.com
Qzone	General network	www.qq.com
LinkedIn	Business network	www.linkedin.com

Dashboards

Google	Trend tools	www.google.com/trends www.google.com/insights/search
Netvibes	Dashboard	www.netvibes.com/en

Social Bookmarking

Samepoint	Search engine	www.samepoint.com
Socialmention	Search engine	www.socialmention.com
Knowem	Name look-up	knowem.com

Blogs

Technorati	Blog directory	technorati.com
Ice Rocket	Blog search engine	www.icerocket.com

Microblogs

Twitter	Microblog	twitter.com
Tweetdeck	Microblog organizer	www.tweetdeck.com
Trendistic	Trend tracker	www.trendistic.com

File Sharing

YouTube	Video file sharing	www.youtube.com
NicoNicoDuga	Video file sharing	www.nicovideo.jp
Flikr	Photo file sharing	www.flikr.com
Slideshare	Presentation sharing	www.slideshare.net
Ushahidi	Collaboration site	www.ushahidi.com

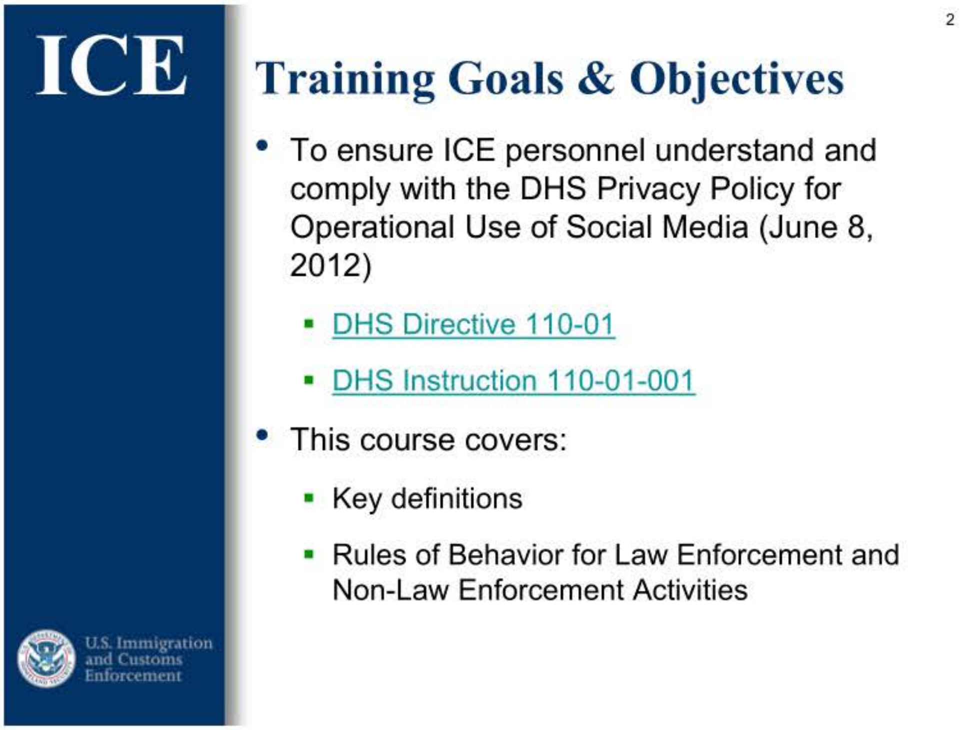
Location-based Services

Foursquare	Mobile service	foursquare.com
Facebook Places	Mobile service	www.facebook.com/places
Gowalla	Mobile service	gowalla.com
Scvngr	Mobile game service	www.scvngr.com

Privacy Requirements for Operational Use of Social Media

November 2013

U.S. Immigration
and Customs
Enforcement



ICE

Training Goals & Objectives

- To ensure ICE personnel understand and comply with the DHS Privacy Policy for Operational Use of Social Media (June 8, 2012)
  - DHS Directive 110-01
  - DHS Instruction 110-01-001
- This course covers:
  - Key definitions
  - Rules of Behavior for Law Enforcement and Non-Law Enforcement Activities

U.S. Immigration
and Customs
Enforcement

3

ICE

What Does This Policy Do?

- Regulates how DHS collects personally identifiable information (PII) from “Social Media” Internet sites for an “Operational Use”
- Requires DHS components and offices to establish Rules of Behavior that personnel must follow
- Requires annual training of all personnel who engage in this type of activity

U.S. Immigration and Customs Enforcement

4

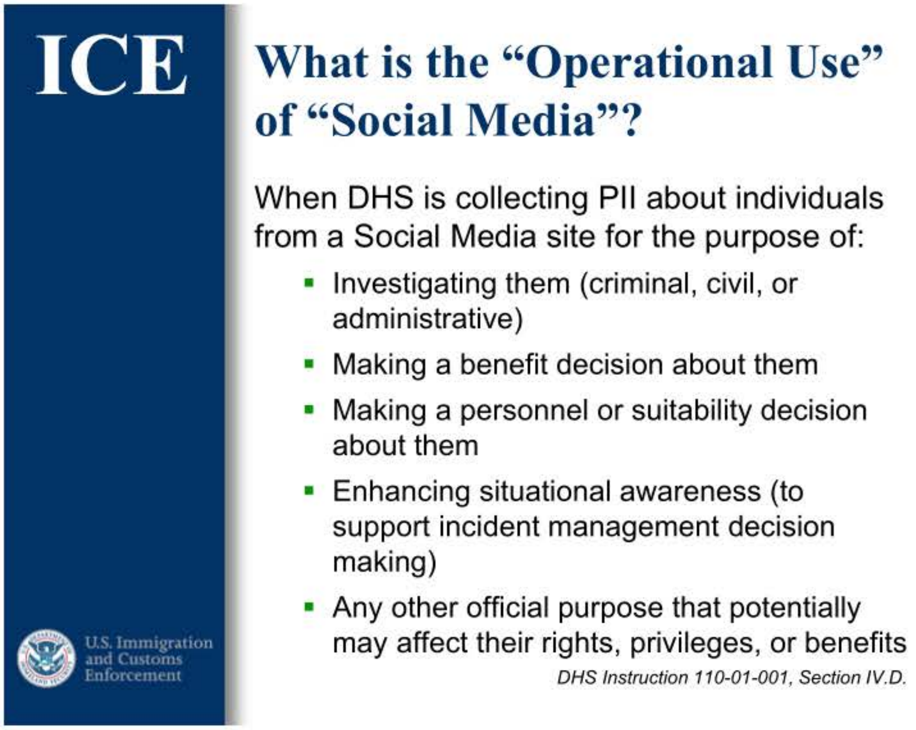
ICE

Why Was This Policy Created?

- To address public and congressional concerns about how DHS collects PII from Social Media sites
- To ensure DHS is not engaging in an unlawful or inappropriate collection of PII from Social Media
- To ensure that there are clear “dos and don’ts” for personnel to follow – these are called the “Rules of Behavior”
- To ensure all DHS personnel are aware of the rules through annual training

U.S. Immigration and Customs Enforcement

5



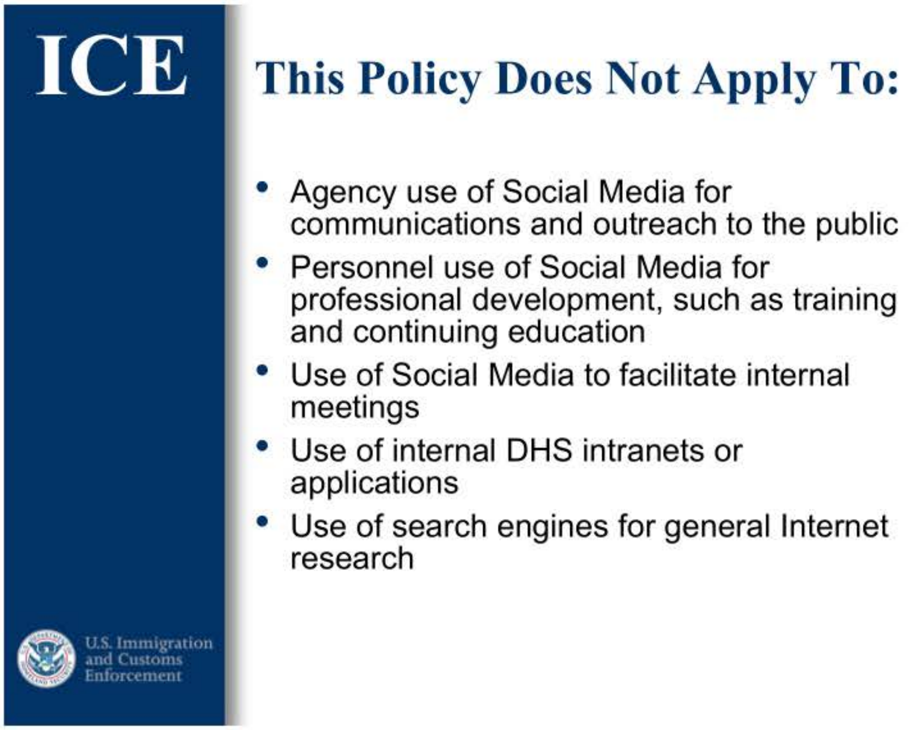
What is the “Operational Use” of “Social Media”?

When DHS is collecting PII about individuals from a Social Media site for the purpose of:

- Investigating them (criminal, civil, or administrative)
- Making a benefit decision about them
- Making a personnel or suitability decision about them
- Enhancing situational awareness (to support incident management decision making)
- Any other official purpose that potentially may affect their rights, privileges, or benefits

DHS Instruction 110-01-001, Section IV.D.

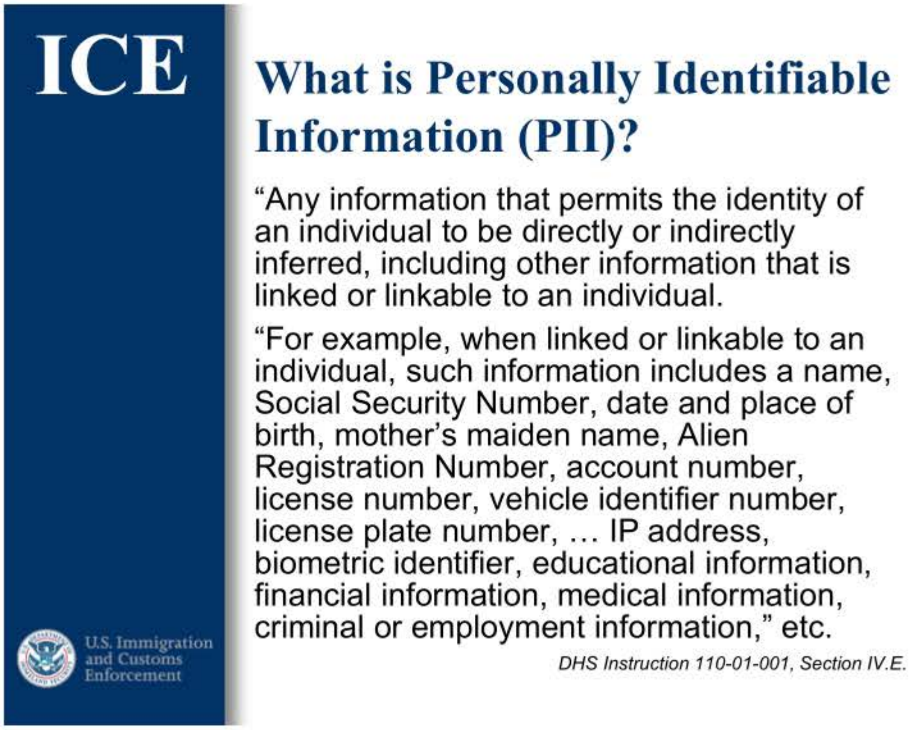
6



This Policy Does Not Apply To:

- Agency use of Social Media for communications and outreach to the public
- Personnel use of Social Media for professional development, such as training and continuing education
- Use of Social Media to facilitate internal meetings
- Use of internal DHS intranets or applications
- Use of search engines for general Internet research

7



ICE

What is Personally Identifiable Information (PII)?

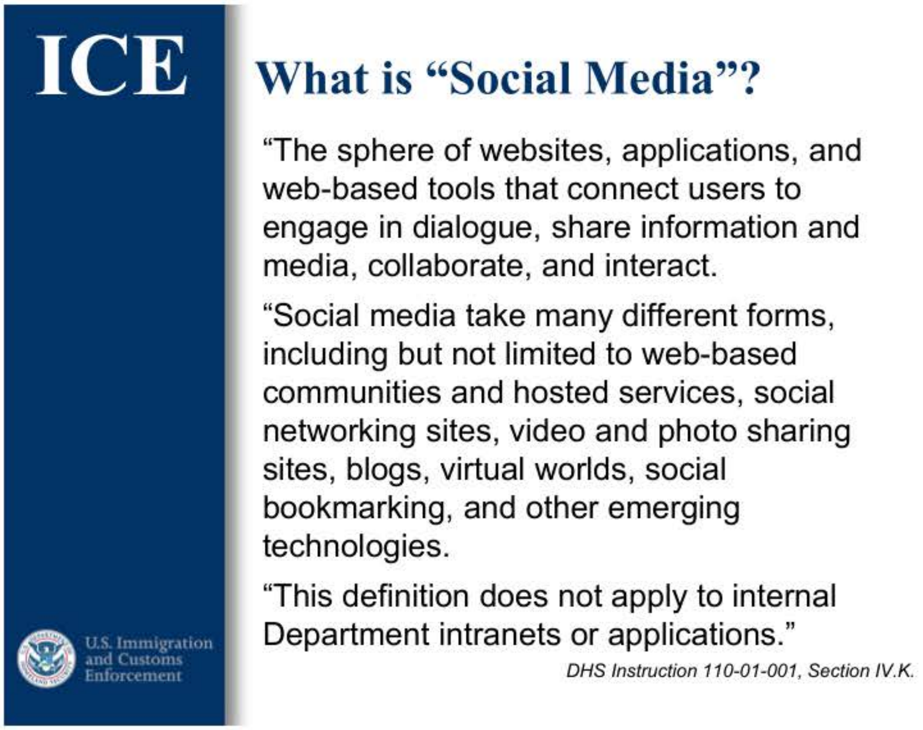
"Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

"For example, when linked or linkable to an individual, such information includes a name, Social Security Number, date and place of birth, mother's maiden name, Alien Registration Number, account number, license number, vehicle identifier number, license plate number, … IP address, biometric identifier, educational information, financial information, medical information, criminal or employment information," etc.

DHS Instruction 110-01-001, Section IV.E.

U.S. Immigration and Customs Enforcement

8



ICE

What is "Social Media"?

"The sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact.

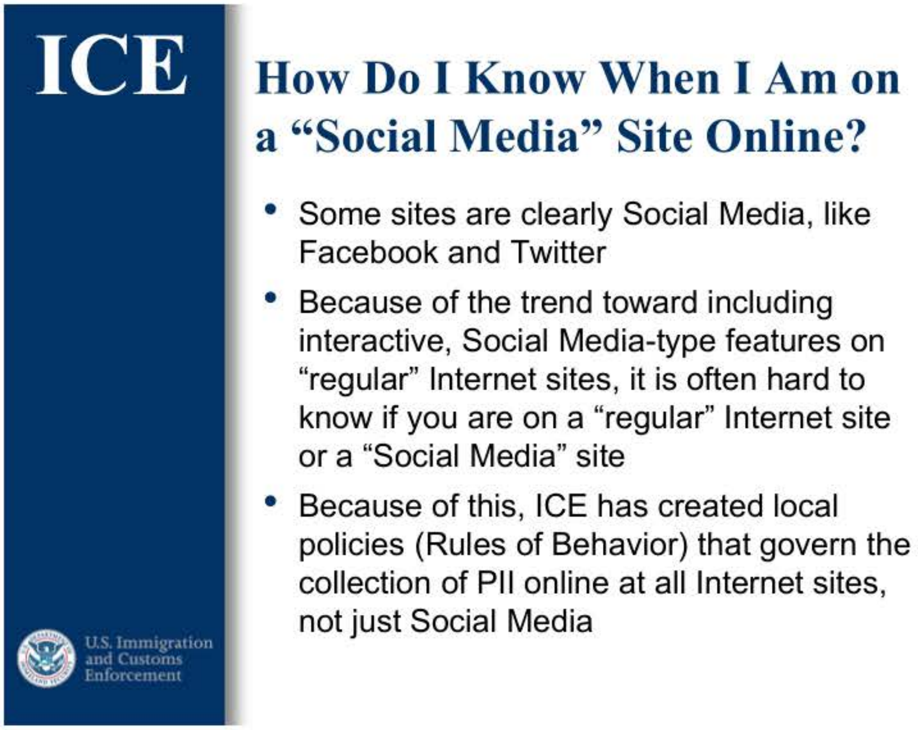
"Social media take many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies.

"This definition does not apply to internal Department intranets or applications."

DHS Instruction 110-01-001, Section IV.K.

U.S. Immigration and Customs Enforcement

9



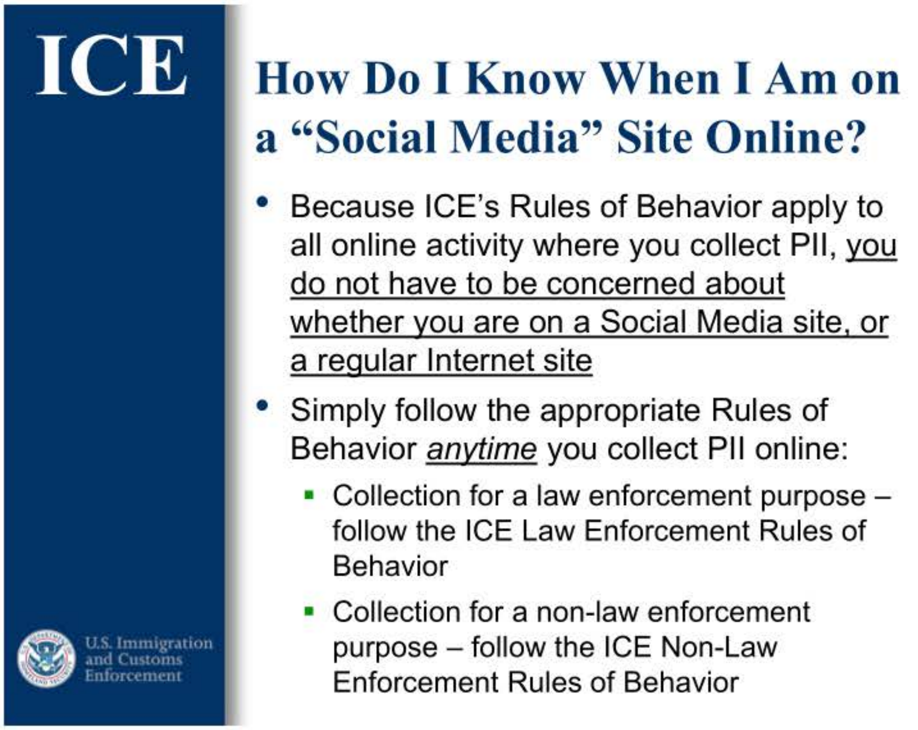
ICE

How Do I Know When I Am on a "Social Media" Site Online?

- Some sites are clearly Social Media, like Facebook and Twitter
- Because of the trend toward including interactive, Social Media-type features on "regular" Internet sites, it is often hard to know if you are on a "regular" Internet site or a "Social Media" site
- Because of this, ICE has created local policies (Rules of Behavior) that govern the collection of PII online at all Internet sites, not just Social Media

U.S. Immigration and Customs Enforcement

10



ICE

How Do I Know When I Am on a "Social Media" Site Online?

- Because ICE's Rules of Behavior apply to all online activity where you collect PII, you do not have to be concerned about whether you are on a Social Media site, or a regular Internet site
- Simply follow the appropriate Rules of Behavior *anytime* you collect PII online:
  - Collection for a law enforcement purpose – follow the ICE Law Enforcement Rules of Behavior
  - Collection for a non-law enforcement purpose – follow the ICE Non-Law Enforcement Rules of Behavior

U.S. Immigration and Customs Enforcement

CTCEU Open Source Team Success Stories

HSI Los Angeles arrest of a Jordanian national in November 2014:

(b)(7)(E);(b)(6);(b)(7)(C) [redacted]

HSI New York AWOL case of a Yemen national in January 2015:

(b)(7)(E);(b)(6);(b)(7)(C) [redacted]

HSI San Diego request for open source intelligence report of Saudi Arabia national in May 2015:

(b)(7)(E);(b)(6);(b)(7)(C) [redacted]

From: (b)(6);(b)(7)(C) [redacted]
To:
Cc:
Subject: DB numbers for August 2017
Date: Friday, September 8, 2017 12:08:45 PM
Attachments: DB August 2017.xlsx

Good afternoon (b)(6);(b)(7)(C) [redacted]

It was nice meeting you this morning. Here are the GOST stats for August, also attached is the spreadsheet, exported from the access DB containing all stats of leads worked by OST in August 2017.
Let me know if you have any questions.

Thanks,

(b)(6);(b)(7)(C) [redacted]

(b)(7)(E) [redacted]

From: (b)(7)(C);(b)(6)
To:
Cc:
Subject: FW: (16-079-ISP-USCIS, ICE) "DHS Capabilities to Screen Social Media Use of Visa and Asylum Seekers" [ICE OAC # 657]
Date: Wednesday, December 14, 2016 3:24:57 PM
Attachments: Visa Overstay Enforcement Investigations.doc
Domestic Mantis White Paper August 2016.docx
Social Media White Paper 03252016.docx
FY16 Social Media Pilot Project NSIC ISL and BRS.DOCX
Importance: High

Sir,

The OIG also failed, or conveniently left out, how we did recommend metrics for measuring success during our social media pilot.

See 2, 3 below for response during our meeting with DHS OIG in September clearly explaining our intent to support once our 1 year pilot was complete in 2017.

(b)(7)(C);(b)(6) | Assoc.DAD | National Security Inv Division | DHS | ICE | HQ - Homeland Security Investigations (b)(7)(C);(b)(6) 500 12th SW | Washington, D.C.| 20536

From (b)(7)(C);(b)(6)
Sent: Monday, September 19, 2016 4:12 PM
(b)(7)(C);(b)(6)
Subject: FW: (16-079-ISP-USCIS, ICE) "DHS Capabilities to Screen Social Media Use of Visa and Asylum Seekers" [ICE OAC # 657]
Importance: High

Coming back down…

(b)(7)(C);(b)(6) Acting Unit Chief
National Security Integration Center - Visa Security Program
(b)(7)(C);(b)(6)

From (b)(7)(C);(b)(6)
Sent: Tuesday, September 13, 2016 3:42 PM
To (b)(7)(C);(b)(6)
Cc
Subject: RE: (16-079-ISP-USCIS, ICE) "DHS Capabilities to Screen Social Media Use of Visa and Asylum Seekers" [ICE OAC # 657]
Importance: High

(b)(7)(C);(b)(6)

This is the cleared response with the four attached documents. Please coordinate with (b)(7)(C);(b)(6) (b)(7)(C);(b)(6) for further questions regarding the stats and let me know when I can proceed. Thank you again for the help.

Due to the nature and differences of the three separate pilot programs, a combined response is not practical. In order to best answer the questions posed by the OIG, the responses from CTCEU are in black and NSIC in blue. The documents referred to in the questions are attached.

(b)(7)(E);(b)(5)

(b)(7)(E);(b)(5)

[redacted]

(b)(7)(E);(b)(5)

V/r,

(b)(6);(b)(7)(C)

Special Agent / SADAD

National Security Investigations Division

Homeland Security Investigations

(b)(6);(b)(7)(C)

From (b)(6);(b)(7)(C)
Sent: Tuesday, August 30, 2016 9:36:36 AM (UTC-05:00) Eastern Time (US & Canada)
To: NSID Tasking
Cc (b)(6);(b)(7)(C) n L
Subject: FW: (16-079-ISP-USCIS, ICE) "DHS Capabilities to Screen Social Media Use of Visa and Asylum Seekers" [ICE OAC # 657]

Good Morning,

Please see below DHS OIG document request reference OIG Audit on "DHS Capabilities to Screen Social Media Use of Visa and Asylum Seekers". Please provide your responses NLT Tuesday September 6, 2016.

Thanks,

(b)(6);(b)(7)(C)

Special Agent (b)(6);(b)(7)(C)

SADAD for Investigative Services Division
OIG Audit Liaison for HSI/SIP & LEOSA PM
Management Oversight Section
Homeland Security Investigations (HSI)

(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Monday, August 29, 2016 12:13 PM
(b)(6);(b)(7)(C)
Subject: (16-079-ISP-USCIS, ICE) "DHS Capabilities to Screen Social Media Use of Visa and Asylum Seekers"

Good Afternoon (b)(6);(b)(7)(C)

I hope this email finds you well. We would like to request the following documents (if available) from ICE in relation to the VSP pilot program:

(b)(6);(b)(7)(C)

Please let me know if you have any questions, comments, or concerns. As always, we greatly appreciate your help!

Thank you,

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Policy Advisor . U.S. Department of Homeland Security . Office of Inspector General . Office of Inspections and Evaluations

From: (b)(7)(C);(b)(6)
To:
Cc:
Subject: FW: Social Media
Date: Tuesday, January 24, 2017 12:44:26 PM
Attachments: (b)(7)(C);(b)(6)
image006.jpg

(b)(7)(E)

Thank you,

(b)(7)(C)

From: (b)(7)(C);(b)(6)
Sent: Tuesday, January 24, 2017 12:02 PM
To: (b)(7)(C);(b)(6)
Subject: FW: Social Media

(b)(7)(

Can you go and look at this. If you were looking this and saw this at the time would he be given a visa?

(b)(7)(C);(b)(6)
Acting Section Chief
Homeland Security Investigations
National Security Integration Center - Visa Security Program
National Security Investigations Division
(b)(7)(C);(b)(6)

From: (b)(7)(C);(b)(6)
Sent: Tuesday, January 24, 2017 9:29 AM
To: (b)(7)(C);(b)(6)
Subject: Social Media

Good morning,

(b)(7)(E)

(b)(7)(C);(b)(6)

I was also wondering, is the email for (b)(7)(C);(b)(6) I found a few of them on Lync. I'll go ahead and send the write-up to him as well.

Please let me know if you have any questions!

v/r,

(b)(7)(C);(b)(6)
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(7)(C);(b)(6)

From: (b)(6);(b)(7)(C)
To:
Subject: FW: Visa pilot anecdotes
Date: Tuesday, November 8, 2016 10:42:17 AM

Giant Oak is the gift that keeps on giving,. We should go ahead and get this scheduled soonest. When are you two available?

Thanks,
(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C), Acting Unit Chief
National Security Integration Center - Visa Security Program
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, November 08, 2016 10:07 AM
To (b)(6);(b)(7)(C)
Subject: FW: Visa pilot anecdotes

(b)(6);(b)(7)(C)

Wanted to shoot a note over checking on the anecdotes from the Visa pilot program. These are very helpful to Giant Oak as a gauge of our performance as well as continued domain building and refinement.

My boss, (b)(6);(b)(7)(C), has asked that I facilitate a meeting between you and he to discuss the pilot program to date. Please let me know some dates and times that are agreeable to you.

Thank you,
(b)(6);(b)(7)(C)

From (b)(6);(b)(7)(C)
Sent: Monday, October 31, 2016 11:45 AM
To (b)(6);(b)(7)(C)
Subject: FW: Visa pilot anecdotes

(b)(6);(b)(7)(C)

The CTCEU is in the process of creating a briefing for (b)(6);(b)(7). I wanted to shoot over an email checking on the status of these anecdotes.

To whom will they be circulated? For situational awareness, I would like to receive a copy.

Thank you,

(b)(6);(b)(7)(C)

From(b)(6);(b)(7)(C)
Sent: Monday, October 31, 2016 9:20 AM
To:(b)(6);(b)(7)(C)
Subject: Fwd: Visa pilot anecdotes

---------- Forwarded message ----------
From: (b)(6);(b)(7)(C)
Date: Thu, Oct 27, 2016 at 11:11 PM
Subject: RE: Visa pilot anecdotes
(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)
I just wrote two of them up this afternoon because, you guessed it, the boss asked us too.
(b)(6);(b) is going to tighten up what I wrote up so I will forward.
We will get you something out soonest.
Thanks for letting me know.
(b)(6);(b)(7)(C)

Sent with Good (www.good.com)

From:(b)(6);(b)(7)(C)
Sent: Thursday, October 27, 2016 11:00:20 PM
(b)(6);(b)(7)(C)
Subject: Visa pilot anecdotes

Mr. (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C);(b)(7)(E)

I have copied my boss,(b)(6);(b)(7)(C) on this email. Please feel free to include(b)(6) in this conversation.

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
To:
Subject: FW: Visa Pilot
Date: Thursday, December 1, 2016 4:16:58 PM

(b)(6);(b)(7)(C)

Good afternoon.

Please see below I think that this may have been intended for you.

Thank you,

(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Thursday, December 01, 2016 2:52 PM
(b)(6);(b)(7)(C)
Subject: Visa Pilot

All,

My team and I continue to spot check the highest ranked cases in the GOST tool. Below are two cases that I think you will find interesting. These are cases that scored in the 50s, very high compared to the size of the daily upload.

(b)(6);(b)(7)(C);(b)(7)(E)

(b)(6);(b)(7)(C);(b)(7)(E)

(b)(6);(b)(7)(C)

4601 N Fairfax Drive
Suite 1200
Arlington, VA 22203

Phone: 703.436.4512
Email: info@giantoak.com
Web: www.giantoak.com

GIANT OAK

Confidence Scores Definitions:

Overview:

As part of our services to the government, Giant Oak provides prioritization and confidence ratings of our search results. These prioritizations allows analysts and decision makers to more effectively and efficiently allocate scarce manpower and resources to the most important tasks. Below are the definitions that comprise Giant Oak's confidence ratings.

(b)(5)

[redacted]

From: (b)(6);(b)(7)(C)
To:
Cc:

Subject: GOST Security Assessment Report
Date: Thursday, May 25, 2017 11:24:38 AM
Attachments: 2017 Giant Oak FISMA SAR.docx
2017 Giant Oak Risk Exposure Table (RET).xlsx

(b)(6);(b)(7)(C)

Attached you will find the GOST Security Assessment Report (SAR) issued by Giant Oak's third party assessors, Coalfire. Please review the SAR, and the Risk Exposure Table (RET), for discussion and inclusion into Giant Oak's GOST Remediation Plan.

(b)(6);(b)(7)(C);(b)(5)

I am eager to learn how the documents provided here will assist in the signing of a Risk Memo and look forward to discussing this afternoon and in the coming weeks.

SECTION B
SF 1449 CONTINUATION

INTENTIONALLY LEFT BLANK

SECTION C
CONTRACT CLAUSES

FEDERAL ACQUISITION REGULATION (FAR) CLAUSES INCORPORATED BY REFERENCE

52.252-2 Clauses Incorporated by Reference (FEB 1998)
52.225-25 Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran—Representation and Certifications (DEC 2012)
52.232-39 Unenforceability of Unauthorized Obligations (JUN 2013)
52.244-6 Subcontracts for Commercial Items (JUL 2014)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: http://acquisition.gov/far/index.html

52.212-4 Contract Terms and Conditions—Commercial Items (MAY 2014)

FEDERAL ACQUISITION REGULATION (FAR) CLAUSES INCORPORATED BY FULL TEXT

52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders—Commercial Items (JUL 2014)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).

__Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004)"(Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

__ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

__ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509)).

__ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (June 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

__ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jul 2013) (Pub. L. 109-282) (31 U.S.C. 6101 note).

__ (5) [Reserved].

_**X**_ (6) 52.204-14, Service Contract Reporting Requirements (Jan 2014) (Pub. L. 111-117, section 743 of Div. C).

__ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Jan 2014) (Pub. L. 111-117, section 743 of Div. C).

_**X**_ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Aug 2013) (31 U.S.C. 6101 note).

_**X**_ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

__ (10) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (May 2012) (section 738 of Division C of Pub. L. 112-74, section 740 of Division C of Pub. L. 111-117, section 743 of Division D of Pub. L. 111-8, and section 745 of Division D of Pub. L. 110-161).

__ (11) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).

__ (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

__ (13) [Reserved]

_ **X** _ (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (Nov 2011) (15 U.S.C. 644).

__ (ii) Alternate I (Nov 2011).

__ (iii) Alternate II (Nov 2011).

__ (15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

__ (ii) Alternate I (Oct 1995) of 52.219-7.

__ (iii) Alternate II (Mar 2004) of 52.219-7.

_ **X** _ (16) 52.219-8, Utilization of Small Business Concerns (May 2014) (15 U.S.C. 637(d)(2) and (3)).

__ (17)(i) 52.219-9, Small Business Subcontracting Plan (Jul 2013) (15 U.S.C. 637(d)(4)).

__ (ii) Alternate I (Oct 2001) of 52.219-9.

__ (iii) Alternate II (Oct 2001) of 52.219-9.

__ (iv) Alternate III (Jul 2010) of 52.219-9.

__ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011)(15 U.S.C. 644(r)).

__ (19) 52.219-14, Limitations on Subcontracting (Nov 2011) (15 U.S.C. 637(a)(14)).

__ (20) 52.219-16, Liquidated Damages—Subcon-tracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

__ (21)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).

__ (ii) Alternate I (June 2003) of 52.219-23.

__ (22) 52.219-25, Small Disadvantaged Business Participation Program—Disadvantaged Status and Reporting (Jul 2013) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

__ (23) 52.219-26, Small Disadvantaged Business Participation Program—Incentive Subcontracting (Oct 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

__ (24) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657 f).

__ (25) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).

__ (26) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (Jul 2013) (15 U.S.C. 637(m)).

__ (27) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (Jul 2013) (15 U.S.C. 637(m)).

_ **X** _ (28) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

_ **X** _ (29) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2014) (E.O. 13126).

_ **X** _ (30) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

_ **X** _ (31) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

_ **X** _ (32) 52.222-35, Equal Opportunity for Veterans (Sep 2010)(38 U.S.C. 4212).

_ **X** _ (33) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

_ **X** _ (34) 52.222-37, Employment Reports on Veterans (SEP 2010) (38 U.S.C. 4212).

_ **X** _ (35) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

__ (36) 52.222-54, Employment Eligibility Verification (AUG 2013). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

__ (37)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

__ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

__ (38) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

__ (39)(i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (Dec 2007) (E.O. 13423).

__ (ii) Alternate I (Dec 2007) of 52.223-16.

_ **X** _ (40) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Aug 2011) (E.O. 13513).

__ (41) 52.225-1, Buy American—Supplies (May 2014) (41 U.S.C. chapter 83).

__ (42)(i) 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43.

__ (ii) Alternate I (May 2014) of 52.225-3.

__ (iii) Alternate II (May 2014) of 52.225-3.

__ (iv) Alternate III (May 2014) of 52.225-3.

__ (43) 52.225-5, Trade Agreements (Nov 2013) (19 U.S.C. 2501, *et seq*., 19 U.S.C. 3301 note).

_**X**_ (44) 52.225-13, Restrictions on Certain Foreign Purchases (June 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

__ (45) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

__ (46) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

__ (47) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

__ (48) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

__ (49) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

_ **X** _ (50) 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013) (31 U.S.C. 3332).

__ (51) 52.232-34, Payment by Electronic Funds Transfer—Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

__ (52) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

_ **X** _ (53) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

__ (54)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

__ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate.*]

__ (1) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

__ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (May 2014) (41 U.S.C. chapter 67).

__ (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (May 2014) (41 U.S.C. chapter 67).

__ (7) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O.13495).

__ (8) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792).

__ (9) 52.237-11, Accepting and Dispensing of $1 Coin (Sept 2008) (31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record.* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after

any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509).

(ii) 52.219-8, Utilization of Small Business Concerns (May 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Veterans (Sep 2010) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(viii) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

(ix) 52.222-50, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).

___Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(xi) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(xii) 52.222-54, Employment Eligibility Verification (AUG 2013).

(xiii) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xiv) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

52.217-8 Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days of contract completion.

(End of Clause)

52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **30** days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

(End of Clause)

52.224-1 Privacy Act Notification (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

52.224-2 Privacy Act (APR 1984)

(a) The Contractor agrees to—
(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—
(i) The systems of records; and
(ii) The design, development, or operation work that the contractor is to perform;
(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and
(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.
(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.
(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of clause)

52.227-14 RIGHTS IN DATA—GENERAL (MAY 2014)

(a) *Definitions*. As used in this clause—

"Computer database" or "database means" a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"—

(1) Means

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

"Restricted computer software" means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

"Restricted rights," as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

"Technical data" means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 116).

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in—

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to—

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) Copyright—

(1) Data first produced in the performance of this contract.

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) Unauthorized marking of data.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g) (4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense. The Contracting Officer may agree to do so if the Contractor—

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) Protection of limited rights data and restricted computer software.

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall—

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) [Reserved]

(h) *Subcontracting*. The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of clause)

52.239-1 Privacy or Security Safeguards (AUG 1996)

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.
(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.
(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(End of clause)

HOMELAND SECURITY ACQUISITION REGULATIONS (HSAR) INCORPORATED BY REFERENCE

3052.242-72 Contracting officer's technical representative (DEC 2003)

HOMELAND SECURITY ACQUISITION REGULATIONS (HSAR) CLAUSES INCORPORATED BY FULL TEXT

3052.204-71 Contractor employee access

(a) *Sensitive Information,* as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

(b)(7)(E) [redacted]

HSAR Class Deviation 15-01 -SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions.* As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate.* The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements.*

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

HSAR Class Deviation 15-01 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise

specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

SECTION D
CONTRACT DOCUMENTS, EXHIBITS OR ATTACHMENTS

STATEMENT OF WORK (SOW)
U.S. Department of Homeland Security
U.S. Immigration and Customs Enforcement (ICE)
Homeland Security Investigations (HSI)
Counterterrorism and Criminal Exploitation Unit (CTCEU)

1.0 EXECUTIVE SUMMARY

U.S. Immigration and Customs Enforcement is the principal investigative arm of the U.S. Department of Homeland Security (DHS) and the second largest investigative agency in the federal government. Created in 2003 through a merger of the investigative and interior enforcement elements of the U.S. Customs Service and the Immigration and Naturalization Service, ICE has approximately 19,000 employees in offices in all 50 states and 47 foreign countries.

ICE has three main components: Homeland Security Investigation (HSI), the largest criminal investigative agency within DHS; Enforcement and Removal Operations (ERO), which identifies, apprehends, and administratively removes illegal aliens from within the United States; and Management and Administration, which supports HSI and ERO by providing sound agency management.

HSI conducts criminal investigations against terrorist and other criminal organizations who threaten national security. HSI combats worldwide criminal enterprises who seek to exploit America's legitimate trade, travel and financial systems and enforces America's customs and immigration laws at and beyond the nation's borders. HSI is comprised of more than 9,000 employees, which includes approximately 7,000 special agents who are assigned to 26 Special Agent in Charge (SAC) offices in major cities, 185 other field offices throughout the United States, and 71 overseas locations in 47 countries.

2.0 BACKGROUND

Within ICE, the Counterterrorism and Criminal Exploitation Unit (CTCEU) falls within the National Security Investigations Division (NSID). The CTCEU is the first and only law enforcement entity entrusted with the enforcement of nonimmigrant visa violations. Today, through the CTCEU, ICE proactively develops cases for investigation from the Student Exchange Visitor Information System (SEVIS) and the Arrival and Departure Information System (ADIS) datasets–which house the records of millions of students, tourists, and temporary workers present in the United States at any given time; to include flight schools and foreign students attending those schools—or those who have overstayed or otherwise violated the terms and conditions of their admission.

Each year, the CTCEU analyzes records of potential status violators, based on data received from SEVIS, ADIS, and other sources. These records are resolved by further establishing potential violations that would warrant field investigations, establishing compliance, or establishing departure dates from the United States. Since the creation of the CTCEU in 2003, analysts have resolved more than 2 million such records using automated and manual review techniques. The CTCEU drew upon various government databases to gather and analyze the identifiable national security leads on foreign students, exchange visitors, and other nonimmigrant visitors.

In order to identify those that pose the greatest threat to national security, the CTCEU employs various targeting and prioritization rules to detect and identify individuals exhibiting specific risk factors based on intelligence reporting, including international travel from specific geographic locations to the U.S., and in-depth criminal research and analysis of dynamic social networks. The targeting and prioritization rules employed by CTCEU are not static and evolve with time, relying on emerging intelligence from inside the Homeland as well as from the intelligence community and theaters overseas. Many of the highest threat leads identified by CTCEU are worked in collaboration with many Federal Agencies.

CTCEU requires analytics based upon the application of social and behavioral sciences to disparate data sets to locate these dangerous individuals who pose an eminent threat to the United States. The solution must be off the shelf and able to be customized on an ongoing basis.

In 2009, the CTCEU entered into a contract for similar alert services with Lexis/Nexis. This system allows all potential leads with an unknown address or other locator to be constantly updated through multiple database checks and when a hit on the subject occurs with a verifiable locator, a lead can then be sent to the field. Additional data sources like social media are needed to enhance CTCEU's overstay enforcement mission to be in stride with evolving technology.

3.0 **OBJECTIVES**

The purpose of this task order is to obtain mission critical subject monitoring data and custom alert services to allow the CTCEU to proactively investigate national security leads that have incomplete address information or those that have been returned from field investigations without a resolution.

The contractor shall use a wide range of proprietary, commercial, and public information data sources to ensure optimal search capability for the most difficult to find individuals. Publicly available data searches include credit bureau information, utilities, real estate, criminal databases and more. Searches on social media profiles on a variety of social media sites including Facebook, LinkedIn, Twitter and others are expected. This will enable CTCEU to leverage data sources in powerful ways to search for persons of interest in both large batches and individual cases. Any proposed solutions to the data analytics and custom alert services requirement must be able to address the following objectives:

- CTCEU requires data and analytic services that integrate areas of expertise in law enforcement and social science to meet increasing demands for efficiency in accomplishing CTCEU's unique mission.

- CTCEU requires that analytics have significant social media and internet searching capabilities.

- CTCEU requires analytics based upon the application of social and behavioral sciences to disparate data sets to locate these dangerous individuals who pose an eminent threat to the United States.

The contractor shall use a wide range of proprietary, commercial, and public information data sources to ensure optimal search capability for the most difficult to find individuals. Publicly available data searches include credit bureau information, utilities, real estate, criminal databases and more. Searches on social media profiles on a variety of social media sites including Facebook, LinkedIn, Twitter and others are expected. For social media searches, the contractor shall search only publicly-accessible social media profiles. This will enable CTCEU to leverage data sources in powerful ways to search for persons of interest in both large batches and individual cases.

The contractor shall track daily address changes and credit activity of individuals (i.e. new aliases, DOB changes, SSNs, etc.) to hundreds of thousands of updates from their data sources and compare them to the subjects provided to them on a weekly basis. Source listings for this information shall include but is not limited to the following: Insurance/Auto, Insurance/Property, Pizza/Phones, Employment, Renter, Credit Check, Accidents, Check Cashing and Death Registry. The contractor shall not search, reference, or use as a source any license plate reader databases. Any relevant changes are then sent out to ICE personnel to review and determine if the information identifies a viable location of the subject. The provider must be able to conduct rapid electronic batch searches for information relating to nonimmigrants who pose a danger to national security or a risk to public safety who are fugitives or otherwise obstruct immigration controls. The contractor shall not maintain any data, including the list of individuals provided by ICE and search results provided to ICE after the analysis is complete, nor shall the contractor maintain any data on behalf of ICE after the data is no longer in a state of analysis.

Return of Information from Non-Social Media Sources:
The contractor shall return to ICE from publicly available or proprietary sources available to the contractor, any information that tracks address changes and changes in identifiers of individuals; i.e. new aliases, date of birth changes, SSN changes, Utility changes, Credit checks, Death Registry, Employment changes, Insurance.

Return of Information from Social Media Sources:
The contractor shall return to ICE any publicly available information that identifies the possible location of the target; contact information such as phone numbers, email addresses, or user names; affiliated organizations by which a location can be derived; and employers. This initial

search and return of information (i.e., tier 1) is limited to information directly connected to the target and may be conducted using sources including, but not limited to, Facebook, Google+, LinkedIn, Pinterest, Tumblr, Instagram, VK, Flickr, Myspace, or Twitter. This may include the collection of any public messages (e.g., Tweets), postings, and media (photos, documents such as resumes, and geocached information). Search results directly connected to the target that also contain information related to the target's associates shall be included with all tier 1 information returned to ICE.

Upon exhaustion of tier 1 information, ICE may request that the contractor conduct a follow-up search and return of information (i.e., tier 2) that includes any publicly available information about the target's associates, such as family members, friends, or co-workers, through which a location of the target may be derived. Tier 2 searches may be conducted using the aforementioned social media sources.

Visa Security Proof of Concept: Social Locator with Giant Oak Search Technology (GOST)™ provides a behavioral analytical approach to understanding online information about human behavior. We aggregate information from across the web and proprietary sources (such as Social Media, forums, IP addresses, other non-Google/Bing indexed sources) and combine them in a domain specific index to provide priority rankings and standardized dossiers that aid in the fact-finding process.

Social Locator's GOST™ provides efficient triage that can search through entities in real time in bulk or on an ad hoc basis, and can sort entities into groups. For the purposes of conducting a Proof of Concept for the application of the Social Locator's GOST™ to the visa security mission, Giant Oak will conduct the following steps:

4.0 SERVICE PROVIDER – NON PERSONAL SERVICES

DHS/ICE retains the authority to make all decisions regarding the DHS/ICE mission, and the execution or interpretation of laws of the United States. Contractor services defined are not considered to be inherently Governmental in nature, as defined by Federal Acquisition Regulation (FAR) Subpart 7.5. This is a Non-Personal services contract as defined by FAR Subpart 37.101. Contractor personnel rendering services under this order are not subject to supervision or control by Government personnel.

5.0 SPECIFIC TASKS

Task 1: The contractor shall provide person-specific, customized data and analysis to include rapid electronic batch searches/reports for 120,000 individuals using a wide variety of data sources such as: Non-social media sourced information including credit bureau information, utilities, real estate, criminal databases, etc. and social media information that includes profiles and media sites such as Facebook, LinkedIn, Twitter, etc. Social media sites including the internet will be mined for possible leads.

Task 2: The contractor shall provide continuous monitoring and alert systems to track certain information for new activities with mapping capabilities.

Task 3: Ad Hoc Data: The contractor shall provide Ad Hoc Batches of up to a cumulative of 1.3 million records per year.

Task 4: The contractor shall provide NSID with an additional 650,000 ad hoc entity queries with the ability to place an additional 60,000 individuals into continuous monitoring and alert systems for twelve months in support of a visa security proof of concept.

5.1 COLLECTION OF SOCIAL MEDIA INFORMATION

The contractor and contractor personnel must adhere to the following requirements when obtaining information from social media sources in fulfillment of their duties under the contract:

1. Obtaining Information from Unrestricted Sources. When conducting social media searches, the contractor may obtain information from publicly-accessible online sources and facilities under the same conditions they may obtain information from other sources generally open to the public. This principle applies to publicly-accessible sources located in foreign jurisdictions as well as those in the United States.

2. Accessing Restricted Sources. When conducting social media searches, the contractor may not access restricted online sources or facilities.

3. Obtaining Identifying Information about Users or Networks. The contractor may not use software tools, even those generally available as standard operating system software, to circumvent restrictions placed on system users.

4. Public Interaction. The contractor may access publicly-available information only by reviewing posted information and may not interact with the individuals who posted the information.

5. Appropriating Online Identity. "Appropriating online identity" occurs when an entity electronically communicates with others by deliberately assuming the known online identity (such as the username) of a real person, without obtaining that person's consent. The contractor may not use this technique to access information about individuals.

6. PII Safeguards. The contractor will protect personally identifiable information (PII) as required by the Privacy Act and DHS privacy policy.

7. International Issues. Unless gathering information from online facilities configured for public access, law enforcement personnel conducting investigations should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a

foreign jurisdiction. Whenever an item or person is located abroad, law enforcement personnel should follow ICE's policies and procedures for international investigations.

6.0 POSITIONS/POSITION DESCRIPTIONS

Giant Oak's obligation is to provide monitoring data and custom alert capabilities. The following sections provide a summary of which Giant Oak personnel may need access to Classified Information.

6.1 SOCIAL SCIENTIST Access to Classified Information

Position Description: The Social Scientist assists CTCEU analysts in analyzing the trails of data left by people in social media, public records, and other data sources resulting from human behaviors and decisions. The Social Scientist tweaks the algorithms behind the Social Locator ™ and works with CTCEU analysts and the Giant Oak software development team to identify and integrate new sources of data in the system. The Social Scientist also improves the transliteration and name matching tools built into Social Locator ™ to be further specialized for certain ethnic groups, non-roman languages and alphabets, or countries of origin. To be truly proficient and knowledgeable, the Social Scientist will, on occasion, require access to classified facilities in order to engage in meaningful conversations related to homeland security missions, and obtain awareness of emerging relevant technologies in the Intelligence and Law Enforcement communities, for the benefit of Social Locator's continued useful deployment within the CTCEU.

Classification Level: This position requires access to classified information at the TS/SCI level

PROGRAM MANAGEMENT/DATA SCIENTIST Access to Classified Information

Position Description: In order to implement a successful deployment of Social Locator within the CTCEU, it is required that the company offers the program management and data science expertise. The program management responsibilities will include contract oversight, including programmatic and financial functions. The Data Scientist function is highly important to Social Locator's success within CTCEU, as this role is responsible for executing experiments pertaining to major components of the system (i.e. data comparisons, reliability and relevance scoring, algorithm accuracy, etc.) and subsequently assessing the statistical significance of all experiment outcomes. To be truly proficient and knowledgeable, the Program Manager/Data Scientist will, on occasion, require access to classified facilities in order to engage in meaningful conversations related to homeland security missions, and obtain awareness of emerging relevant technologies in the Intelligence and Law Enforcement communities, for the benefit of Social Locator's continued useful deployment within the CTCEU.

Classification Level: This position requires access to classified information at the TS/SCI level

7.0 GENERAL REQUIREMENTS

7.1 PERIOD OF PERFORMANCE

The estimated duration of this task is from September 4, 2014, through August 31, 2019, and is inclusive of (1) one, one-year base period, and four (4), one-year option periods, totaling five years as follows:

Base Period:	September 4, 2014 – August 31, 2015
Option Period 1:	September 1, 2015 – August 31, 2016
Option Period 2:	September 1, 2016 – August 31, 2017
Option Period 3:	September 1, 2017 – August 31, 2018
Option Period 4:	September 1, 2018 – August 31, 2019

Actual performance dates will be dependent upon date of award.

7.2 PLACE OF PERFORMANCE

HSI Division 1 CTCEU
1525 Wilson Blvd suite #425
Arlington, VA 22209

7.3 CONTRACT TYPE

This contract will be a firm-fixed price contract.

7.4 CONTRACT PROGRESS – MEETINGS AND TELECONFERENCES

The CO, COR and Government Program Manager as appropriate will meet periodically or participate in teleconferences with the Contractor to review contract performance, progress, and resolve technical issues. Minutes of the meetings/teleconferences, with action items identified, shall be documented by the Contractor and provided to the COR no later than 72 hours after meeting.

7.5 RELEASE OF INFORMATION

Contractor access to proprietary and Privacy Act-protected information (covered by DHS/ICE-009 External Investigations System of Records Notice (SORN)) is required under the PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the Privacy Act of 1974, and the *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS*. Contractor and subcontractors shall not hold any discussions or release any information relating to this contract to anyone not having a direct interest in performance of this contract, without written consent of the CO. This restriction applies to all news releases of information to the public, industry or Government agencies, except as follows: Information for actual or potential subcontractors or other individuals necessary for Contractor's performance of this contract. Contractor and subcontractors shall not issue advertisements about projects performed under this task without government review and approval. For the purposes of this paragraph, advertisement is considered to be Contractor-funded promotional brochures, posters, tradeshow handouts, world-wide-web pages, magazines, or any other similar type promotions.

7.6 NON-DISCLOSURE STATEMENTS

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of these tasks and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of these tasks. Contractor personnel are required to sign Non-Disclosure statements (DHS Form 11000-6).

8.0 DELIVERABLES

The Contractor shall provide the following deliverables:

The list below reflects the deliverables considered by the CTCEU to be most important for the successful performance of this task order. The Government will establish a Quality Assurance Surveillance plan that is not part of this task order in order to monitor performance requirements summary items described in the list below.

DELIVERABLES SCHEDULE:

Deliverable	Type of Report	Frequency	Due Date
Post-award Orientation (SOW 9.0)	N/A	Once	Within 10 days after contract award
Progress Meetings (SOW 6.3)	Electronic delivery as agreed; format	As required	As required
Invoice Courtesy Copy	Electronic; .pdf file	Monthly	No later than the 10th calendar day of the preceding month
Batch Reports (SOW 5.0, Task 1)	Electronic delivery as agreed; format	Daily	As coordinated with the COR
Ad Hoc Reports (SOW 5.0, Task 3)	Electronic delivery as agreed; format	As required	As required

9.0 INSPECTION AND ACCEPTANCE:

All periodic reports and task deliverables shall be inspected, tested (where applicable), reviewed, and accepted by the Government within a reasonable period of time, but in no case more than 20 business days. If found unacceptable, the Government shall notify the Contractor in writing or by email of the non-acceptance and detail why the deliverable was not accepted. The Contractor shall then have 10 business days to discuss, correct, or arrive at an acceptable solution with the Government.

9.1 ACCEPTANCE CRITERIA:

The deliverables are prepared/packaged to meet the following quality criterion:

a. All information is accurate and verifiable
b. Where appropriate, inclusion of all required steps
c. Prepared/presented all required and necessary information in an easy to follow logical, sequential manner
d. Feasibility fits into the parameters identified
e. Written in succinct, simple, straightforward language
f. Written requirements are at a consistent level of detail throughout the deliverables

Only the Contracting Officer's Representative (COR) or the Contracting Officer (CO) has the authority to inspect, accept, or reject all deliverables. Final acceptance of all deliverables will be provided in writing, or in electronic format, by the COR or CO within 30 days from the end of the task order.

Performance by the Contractor to correct defects found by the Government as a result of quality assurance surveillance and by the Contractor as a result of quality control, shall be in accordance with FAR 52.246-4, Inspection of Services – Firm Fixed Price (AUG 1996). The COR will monitor compliance and report to the Contracting Officer.

10.0 POST AWARD ORIENTATION CONFERENCE:

The contractor shall participate in a post-award conference for the purposes of making introductions, coordinating security requirements, discussing schedules, prioritizing SOW requirements.

The contractor shall commence work on the first day of the period of performance. The Post Award Orientation Conference shall be coordinated with the Contracting Officer and held no later than 10 days after award.

11.0 PRIVACY ACT:

Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

12.0 REPORTING SUSPECTED LOSS OF SENSITIVE PII

Contractors must report the suspected loss or compromise of Sensitive PII (as defined in the *Guide to Safeguarding Sensitive PII at DHS*) to ICE in a timely manner and cooperate with ICE's Inquiry into the incident and efforts to remediate any harm to potential victims.

1. Contractor must report the suspected loss or compromise of Sensitive PII by its employees or sub-Contractors to the ICE Contracting Officer's Representative (COR) or Contracting Officer within one (1) hour of the initial discovery.

2. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and sub-Contractors are trained to identify and report potential loss or compromise of Sensitive PII.

3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of Sensitive PII containing the following information:

a. Narrative, detailed description of the events surrounding the suspected loss/compromise.
b. Date, time, and location of the incident.
c. Type of information lost or compromised.
d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
e. Names of person(s) involved, including victim, Contractor employee/sub-Contractor and any witnesses.
f. Cause of the incident and whether the company's security plan was followed or not, and which specific provisions were not followed.
g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

4. The Contractor must cooperate with ICE or other government agency inquiries into the suspected loss or compromise of Sensitive PII.

5. At the government's discretion, Contractor employees or sub-Contractor employees may be identified as no longer eligible to access Sensitive PII or to work on that contract based on their actions related to the loss or compromise of Sensitive PII.

13.0 SECURITY REQUIREMENTS

GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the task as described in **HSCEMD-14-C-00002** requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) may access classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

52.204-2 Security Clause Requirements.

This clause applies to the extent that this contract involves access to information classified **TS/SCI level.**

The Contractor shall comply with:
(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DOD 5220.22-M); and
(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(a) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.
(b) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (b) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the *National Industrial Security Program Operating Manual (NISPOM)* for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at an ICE or other Government Facility, it will abide by the requirements set by the agency.

In conjunction with acquisition **HSCEMD-14-C-00002** the contractor shall ensure all investigative, reinvestigate, and adjudicative requirements are met in accordance with *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 2-1.

No person shall be allowed to begin work on contract **HSCEMD-14-C-00002** and/or access sensitive information related to the contract without ICE receiving clearance verification from the FSO. ICE further retains the right to deem an applicant as ineligible due to an insufficient background investigation or when derogatory information is received and evaluated under a

Continuous Evaluation Program. Any action taken by ICE does not relieve the Contractor from required reporting of derogatory information as outlined under the NISPOM.

The FSO will submit a Visitors Authorization Letter (VAL) through the Contracting Officer's Representative (COR) to psu-industrial-security@ice.dhs.gov for processing personnel onto the contract. The clearance verification process will be provided to the COR during Post-Award. Note: *Interim TS is not accepted by DHS for access to Top Secret information. The contract employee will only have access to SECRET level information until DoD CAF has granted a full TS.*

For processing any personnel on a classified contract who will not require access to classified information see BACKGROUND INVESTIGATIONS (Process for personnel do not require access to classified information).

PRELIMINARY DETERMINATION

ICE may, as it deems appropriate, authorize and make a favorable preliminary fitness to support decision based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment fitness determination or a full employment fitness determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment fitness determination or final fitness determination by the OPR-PSU.

BACKGROUND INVESTIGATIONS (Process for personnel do not require access to classified information):

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the OPR-PSU. Prospective Contractor employees without adequate security clearances issued by DoD CAF shall submit the following completed forms to the OPR-PSU through the Contracting Offices Representative (COR), no less than 35 days before the starting date of the contract or 35 days prior to the expected entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P "Questionnaire for Public Trust Positions" Form will be submitted via e-QIP (electronic Questionnaires for Investigation Processing) (Original and One Copy)

2. Three signed eQip Signature forms: Signature Page, Release of Information and Release of Medical Information (Originals and One Copy)

3. Two FD Form 258, "Fingerprint Card"

4. Foreign National Relatives or Associates Statement (Original and One Copy)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (Original and One Copy)

6. Optional Form 306 Declaration for Federal Employment (applies to contractors as well) (Original and One Copy)

If the contract authorizes positions which do not require access to classified information:
In those instances where a Prospective Contractor employee will not require access to classified information, areas or classified systems the Vendor will add to and the COR will insure the following statement is added to the eQip Worksheet prior to submitting it to OPR PSU: "Employee will not require NSI Access to Classified Information or Classified Systems at any level".

Required forms will be provided by ICE at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, ICE retains the right to deem an applicant as ineligible due to insufficient background information.

EMPLOYMENT ELIGIBILITY

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

The contractor will agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represent the best means currently available for employers to verify the work authorization of their employees.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

FACILITY ACCESS:

ICE shall have and exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation.

Contract employees assigned to the contract not needing access to sensitive ICE information, recurring access to ICE facilities or access to DHS/ICE IT systems, to include email, will not be subject to security contractor fitness screening.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to Government facilities or information, the COR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU will conduct reinvestigations every 5 years, or when derogatory information is received, to evaluate continued eligibility.

ICE reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

REQUIRED REPORTS:

The contractor/COR will notify OPR-PSU of all terminations / resignations, etc., within five days of occurrence. The Contractor will return any expired ICE issued identification cards/ credentials and building passes, or those of terminated employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU through the COR as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation) . The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

The contractor is required to report certain events that have an impact on the status of the facility clearance (FCL) and/ or the status of the contract employee's personnel security clearance as outlined by *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter1-3, Reporting Requirements. Contractors shall establish internal procedures as are necessary to ensure that cleared personnel are aware of their responsibilities for reporting pertinent information to the FSO and other federal authorities as required.

Submit reports to the email address psu-industrial-security@ice.dhs.gov

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

Contractors shall provide all employees supporting contract **HSCEMD-14-C-00002** proper initial and annual refresher security training and briefings commensurate with their clearance level, to include security awareness, defensive security briefings.(*National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 3-1. The contractor shall forward a roster of the completed training to the COR on a quarterly bases.

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former

Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

INFORMATION TECHNOLOGY

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS MD 140-01 - Information Technology Systems Security and DHS MD 4300 Sensitive Systems Policy.* Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

All contractor employees using Department automated systems or processing Department sensitive data will be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

Contractors, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security
Responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

(b)(7)(E)

[redacted]

(b)(7)(E)

[redacted]

(b)(7)(E)

[redacted]

(b)(7)(E)

[redacted]

From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Domestic Mantis/Visa Life Cycle
Date: Tuesday, October 3, 2017 11:24:00 AM
Attachments: Team Hotel Operations.docx

Good Morning,

I apologize I am just getting back to you on this. Last week was pretty busy. However, I've attached Team Hotel's Operations document with updated information, which also contains info on how we use the GOST tool. The below paragraph is a summary of visa lifecycle. (b)(7)(E)

(b)(7)(E)

(b)(7)(E) Let me know if you have any more questions.

(b)(7)(E)

From: (b)(7)(C);(b)(6)
Sent: Wednesday, September 27, 2017 11:36 AM
(b)(7)(C);(b)(6)
Subject: Domestic Mantis/Visa Life Cycle

(b)(7)(

Can you provide a write up on how or what drives the prioritizing of the leads worked in Domestic Mantis and Visa Life Cycle? Is the GOST the driving factor to Hotel's prioritizing? Additionally how is GOST used daily in working these programs?

(b)(7)(

Sent with BlackBerry Work
(www.blackberry.com)

From: (b)(7)(C);(b)(6)
To:
Subject: RE: Giant Oak meeting notes
Date: Friday, July 7, 2017 1:51:41 PM

You're welcome, sounds great! Yes I'm looking forward to the next hopeful monthly meeting as well, in agreement that we need some improvements.
The breakdown of GOST results vs. analysts has been extremely time consuming, but in instances like these I think it's worth it to showcase.

I'd love to also come by, maybe sometime next week, and sit with you for a few minutes to see what you all do too. I keep getting pulled into these overview meetings about social media exploitation, and I'd like to keep your team in mind more for these innovations they keep talking about.

From: (b)(7)(C);(b)(6)
Sent: Friday, July 7, 2017 1:48 PM
(b)(7)(C);(b)(6)
Subject: RE: Giant Oak meeting notes

Thanks (b)(7)(C I will sit down with my team and look over this and come up with some terms. Thanks for sharing your notes with us yesterday, you guys were way better prepared than we were! I think having monthly meetings with (b)(7 and all the OS teams will be really helpful. (b)(7)(E)
(b)(7)(E)

From (b)(7)(C);(b)(6)
Sent: Friday, July 07, 2017 11:21 AM
(b)(7)(C);(b)(6)
Subject: Giant Oak meeting notes

Hey (b)(7 and (b)(7)(C);(b

(b)(7 added his questions in red to the GO meeting notes, attached. I highlighted one that I thought you would want to discuss or think about since it deals with finding derog for your subjects. Right now I know GO just uses a huge list of terms that are represented as derogatory.

(b)(7)(

From: (b)(6);(b)(7)(C)
To:
Subject: RE: Ground Truths
Date: Thursday, December 29, 2016 10:14:16 AM

(b)(6

FYI, for the criteria below I get an estimate of about 13,000 subjects.

Thanks,

(b)(6)

(b)(6);(b)(7)(C)
WTS, Inc. | Technical Architect
Solutions Delivery Division (SDD)
Office of the Chief Information Officer
U.S. Immigration & Customs Enforcement (ICE)
Department of Homeland Security
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Wednesday, December 28, 2016 3:15 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: Ground Truths

(b)(6);

We would like to send more ground truths to GO.

(b)(7)(E)

Thank you,

(b)(6);(b)(7)(C)
Visa Security Program Manager
ICE-HSI, National Security Investigations
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Historical Applications - Ground Truth
Date: Wednesday, December 7, 2016 3:40:03 AM

(b)(6);

(b)(7)(E)

From (b)(6);(b)(7)(C)
Sent: Tuesday, December 06, 2016 9:57 PM
To (b)(6);(b)(7)(C)
Cc
Subject: RE: Historical Applications - Ground Truth

I agree. This request falls outside the current approval we have from ICE Privacy office. Adding these data elements would require us to update the Privacy Threshold Assessment (PTA) and re-submit to the ICE Privacy office for approval.

(b)(6);(b)(7)(C)

Project Manager, Solutions Delivery Division
Office of the Chief Information Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, December 6, 2016 3:20 PM
To (b)(6);(b)(7)(C)
Cc
Subject: FW: Historical Applications - Ground Truth

(b)(7)(E)

If I'm wrong please just delete.

From (b)(6);(b)(7)(C)
Sent: Tuesday, December 06, 2016 3:14 PM
(b)(6);(b)(7)(C)
Subject: Re: Historical Applications - Ground Truth

(b)(6);(

Thank you for the clarification on the call today. We discussed and determined the more data that can be provided, the better. (b)(7)(E)

(b)(7)(E)

Thanks,

(b)(6);

(b)(6);(b)(7)(C)

wrote:

(b)(6) All,

(b)(7)(E)

Thoughts?

Thanks,

(b)(6)

(b)(6);(b)(7)(C)

WTS, Inc. | Technical Architect
Solutions Delivery Division (SDD)
Office of the Chief Information Officer
U.S. Immigration & Customs Enforcement (ICE)
Department of Homeland Security

(b)(6);(b)(7)(C)

From (b)(6);(b)(7)(C)
Sent: Tuesday, December 6, 2016 12:21 PM

(b)(6);(b)(7)(C)

Subject: Re: Historical Applications - Ground Truth

This is great news. Thank you (b)(6);(

(b)(6);(b)(7)(C)

Hello (b)(6)

(b)(7)(E)
(b)(7)(E) It's on our task list for this week. We should have it to you by Friday.

Thanks,

(b)(6)

(b)(6);(b)(7)(C)
WTS, Inc. | Technical Architect
Solutions Delivery Division (SDD)
Office of the Chief Information Officer
U.S. Immigration & Customs Enforcement (ICE)
Department of Homeland Security
(b)(6);(b)(7)(C)

From (b)(6);(b)(7)(C)
Sent: Tuesday, December 6, 2016 11:55 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: Historical Applications - Ground Truth

(b)(6);(b)(7)(

(b)(7)(E)

Please let me know if I can help with anything.

(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
To:
Subject: RE: (b)(7)(E) - Open Source/ Social Media Data Analytics - Award Notification
Date: Friday, June 9, 2017 10:38:07 AM

Good morning (b)(6);(b

I am preparing a requisition right now. We just received our funds last night.

From: (b)(6);(b)(7)(C)
Sent: Friday, June 09, 2017 10:32 AM
To: (b)(6);(b)(7)(C)
Subject: FW: (b)(7)(E) - Open Source/ Social Media Data Analytics - Award Notification

(b)(6);(b)(7)(C)

Is there any update on funding for VSP???

(b)(6);(b)(7)(C)
Investigations & Operations Support Dallas | Contracting Officer
DHS | ICE | Office of Acquisition Management (OAQ)
Phone: (b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, June 06, 2017 9:27 AM
(b)(6);(b)(7)(C)
Subject: (b)(7)(E) - Open Source/ Social Media Data Analytics - Award Notification

Dear Vendor,

Congratulations!

You have received the attached award for Open Source/ Social Media Data Analytics from the Department of Homeland Security/ Immigration and Customs Enforcement.

The attached award has a limit of 30 million queries over a five year period of performance.

The award ceiling is estimated at $37,008,960.64.

We look forward to your continued support of our mission.

If there are any questions please do not hesitate to contact myself or the Contracting Officer Representative, (b)(6);((b)(6);(b)(7)(

Respectfully,

(b)(6);(b)(7)(C)
Investigations & Operations Support Dallas | Contracting Officer

(b)(6);(b)(7)(C)

From: (b)(7)(C);(b)(6)
To:
Subject: Re: Relevance/Reliability
Date: Tuesday, July 25, 2017 12:24:26 PM
Attachments: image001.jpg

(b)(

Sorry for the delay on this. We are working through an issue with one of our data providers. It is almost fixed and should be up and running in the next day. We are going to reprocess all cases since the errors with the Relevance score started.

In the meantime, best practice is to relay on the Reliability scores of '5', sort the ranking column from high to low, then work your way through the cases as your resources allow.

Thank you and sorry for the inconvenience.

(b)(7)(C);(b)(6)

> Hi Nick,
>
> I just wanted to give you a heads up that we are no longer receiving scores for relevance…only reliability:
>
> Thanks,
>
> (b)(

From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Social Media
Date: Wednesday, January 25, 2017 3:49:31 PM
Attachments: image001.jpg
image002.jpg

I'd like to commend (b (b)(6) for his outstanding work on this and prompt attention to the matter and the follow on requests from Islamabad.

Thank you!

(b)(

From: (b)(6);(b)(7)(C)
Sent: Wednesday, January 25, 2017 6:20 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: Social Media

Good morning,

(b)(7)(E);(b)(6);(b)(7)(C)

Please let me know if you have any questions!

v/r,

(b)(6);(b)(7)(C
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Wednesday, January 25, 2017 5:58 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: Social Media

FYSA

From: (b)(6);(b)(7)(
Sent: Wednesday, January 25, 2017 5:22:20 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: Social Media

Gentlemen,

(b)(7)(E);(b)(5)

If there is anything useful on high side, please send that over to (b)(6);(b)(7)(C)

Thank you!

(b)(6);(b)(7)(C)
DHS Representative
Embassy of the United States
Islamabad, Pakistan

Office Direct (b)(6);(b)(7)(C)
Cell Phone:
DHS E Mail:

State E Mail: (b)(6);(b)(7)(C)
ClassNet:
JWICS:

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 11:53 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: Social Media

(b)(6);(b)(

(b)(5);(b)(6);(b)(7)(C)

Let me know if we can be any help here.

(b)(

(b)(6);(b)(7)(C)
Special Agent/Program Manager, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 1:09 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: Social Media

(b)(6);(b)(

Please take a look at the attached discovered as part of NSID's social media pilot. Please contact Islamabad and continue to track this.

(b)(6);

(b)(6);(b)(7)(C)
Section Chief, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 12:32 PM
To: (b)(6);(b)(7)(C)
Subject: FW: Social Media

FYI on something we found on our social media pilot for this applicant. Let's talk soon.

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 9:29 AM
To: (b)(6);(b)(7)(C)
Subject: Social Media

Good morning,

(b)(7)(E);(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

I was also wondering, is the email for (b)(6);(b)(7)(C)? I found a few of them on Lync. I'll go ahead and send the write-up to him as well.

Please let me know if you have any questions!

v/r,

(b)(6);(b)(7)(C
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Social Media
Date: Wednesday, January 25, 2017 1:52:38 PM
Attachments: image003.png
image004.jpg
image005.jpg

[redacted]

(b)(7)(E)

From: (b)(6);(b)(7
Sent: Wednesday, January 25, 2017 9:37 AM
To:
Cc: (b)(6);(b)(7)(C)
Subject: RE: Social Media

[redacted]

(b)(7)(E)

Thanks

From: [redacted]
Sent: Wednesday, January 25, 2017 5:58 AM
To: [redacted]
Cc: (b)(6);(b)(7)(
Subject: FW: Social Media

FYSA

From: [redacted]
Sent: Wednesday, January 25, 2017 5:22:20 AM
To:
Cc: (b)(6);(b)(7)(C)
Subject: RE: Social Media

Gentlemen,

(b)(5)

The following would be helpful, if we can have these sent to us:

(b)(7)(E)

If there is anything useful on high side, please send that over to (b)(6);(b)(7)(C)

Thank you!

(b)(6);(b)(7)(C)
DHS Representative
Embassy of the United States
Islamabad, Pakistan

Office Direct: (b)(6);(b)(7)(C)
Cell Phone:
DHS E Mail:
State E Mail:
ClassNet:
JWICS:

From: (b)(6);(b)(
Sent: [redacted] 24, 2017 11:53 PM
To:
Cc: (b)(6);(b)(7)(C)
Subject: RE: Social Media

(b)(6);

(b)(5)

Let me know if we can be any help here.

[redacted]

[redacted]
Special Agent/Program Manager, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
(b)(6);(b)(7)(C)

From: [redacted]
Sent: Tuesday, January 24, 2017 1:09 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: Social Media

[redacted]

Please take a look at the attached discovered as part of NSID's social media pilot. Please contact Islamabad and continue to track this.

[redacted]

[redacted]
Section Chief, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
[redacted]

From: [redacted]
Sent: Tuesday, January 24, 2017 12:32 PM
To: [redacted]
Subject: FW: Social Media

FYI on something we found on our social media pilot for this applicant. Let's talk soon.

From: [redacted]
Sent: Tuesday, January 24, 2017 9:29 AM
To: [redacted]
Subject: Social Media

Good morning,

I went ahead and attached the write-up that I sent [redacted] along with screenshots of the website for the U.S. company. Also, here is the contact information for the TECS record [redacted]

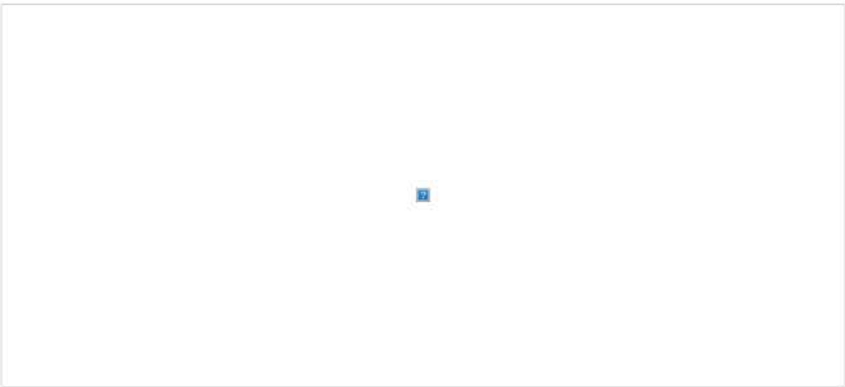
(b)(6);(b)(7)(C)

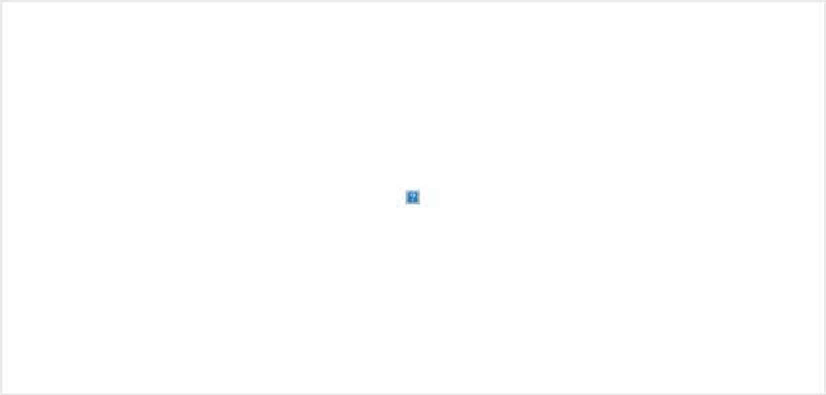
I was also wondering, is the email for [redacted] I found a few of them on Lync. I'll go ahead and send the write-up to him as well.

Please let me know if you have any questions!

v/r,

[redacted]
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(6);(b)(7)(C)





From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Social Media
Date: Wednesday, January 25, 2017 9:37:01 AM
Attachments: image001.jpg
image002.jpg

(b)(6);(b)

(b)(5)

Thanks

From: (b)(6);(b)(7)(C)
Sent: Wednesday, January 25, 2017 5:58 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: Social Media

FYSA

From: (b)(6);(b)(7)(C
Sent: Wednesday, January 25, 2017 5:22:20 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: Social Media

Gentlemen,

(b)(5);(b)(6);(b)(7)(C)

The following would be helpful, if we can have these sent to us:

(b)(7)(E)

If there is anything useful on high side, please send that over to (b)(6);(b)(7)(C)

Thank you!

(b)(6);(b)(7)(C)
DHS Representative
Embassy of the United States
Islamabad, Pakistan

Office Direct: (b)(6);(b)(7)(C)
Cell Phone:
DHS E Mail:
State E Mail:
ClassNet:
JWICS:

From: (b)(6);(b)(7)(
Sent: Tuesday, January 24, 2017 11:53 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: Social Media

(b)(6);(b)

(b)(5)

(b)(5)

Let me know if we can be any help here.

(b)(

(b)(6);(b)(7)(C)
Special Agent/Program Manager, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 1:09 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: Social Media

(b)(6);(b)(7)(

Please take a look at the attached discovered as part of NSID's social media pilot. Please contact Islamabad and continue to track this.

(b)(6);

(b)(6);(b)(7)(C)
Section Chief, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 12:32 PM
To: (b)(6);(b)(7)(C)
Subject: FW: Social Media

FYI on something we found on our social media pilot for this applicant. Let's talk soon.

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 9:29 AM
To: (b)(6);(b)(7)(C)
Subject: Social Media

Good morning,

(b)(7)(E);(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

I was also wondering, is the email for (b)(6);(b)(7)(C)? I found a few of them on Lync. I'll go ahead and send the write-up to him as well.

Please let me know if you have any questions!

v/r,

(b)(6);(b)(7)(C
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Social Media
Date: Tuesday, January 24, 2017 12:51:08 PM
Attachments: image001.png
image002.jpg
image003.jpg

From: (b)(6);(b)(7)(C
Sent: Tuesday, January 24, 2017 12:44 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: Social Media

(b)(5)

Thank you,

[redacted]

From: (b)(6);(b)(7
Sent: Tuesday, January 24, 2017 12:02 PM
To: (b)(6);(b)(7)(
Subject: FW: Social Media

[redacted]

Can you go and look at this. If you were looking this and saw this at the time would he be given a visa?

(b)(6);(b)(7)(C)
Acting Section Chief
Homeland Security Investigations
National Security Integration Center - Visa Security Program
National Security Investigations Division
(b)(6);(b)(7)(

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 9:29 AM
To: [redacted]
Subject: Social Media

Good morning,

I went ahead and attached the write-up that I sent to [redacted] along with screenshots of the website for the U.S. company. Also, here is the contact information for the TECS record (b)(7)(E)

(b)(6);(b)(7)(C)

I was also wondering, is the email fo(b)(6);(b)(7)(C) I found a few of them on Lync. I'll go ahead and send the write-up to him as well.

Please let me know if you have any questions!

v/r,

(b)(6);(b)(7)
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Social Media
Date: Wednesday, January 25, 2017 3:50:10 PM
Attachments: image001.jpg
image002.jpg

I will second that- great work

From: (b)(6);(b)(7)(C)
Sent: Wednesday, January 25, 2017 3:50 PM
To (b)(6);(b)(7)(C)
Cc
Subject: RE: Social Media

I'd like to commend (b)(6);(b)(7)(C) for his outstanding work on this and prompt attention to the matter and the follow on requests from Islamabad.

Thank you!

[redacted]

From: (b)(6);(b)(7)(C)
Sent: Wednesday, January 25, 2017 6:20 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: Social Media

Good morning,

Attached are the printouts from the Virginia State Corporation Commission and the Volera website. It appears that the company was registered in the brother-in-law's name, but it states on the website that both of them operate the business in the U.S.

Please let me know if you have any questions!

v/r,

(b)(6);(b)(7)(C)
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Wednesday, January 25, 2017 5:58 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: Social Media

FYSA

From: (b)(6);(b)(7)(C)
Sent: Wednesday, January 25, 2017 5:22:20 AM
To (b)(6);(b)(7)(C)
Cc
Subject: RE: Social Media

Gentlemen,

(b)(5)

The following would be helpful, if we can have these sent to us:

(b)(7)(E)

If there is anything useful on high side, please send that over to (b)(6);(b)(7)(C)

Thank you!

(b)(6);(b)(7)(C)
DHS Representative
Embassy of the United States
Islamabad, Pakistan

Office Direc (b)(6);(b)(7)(C)
Cell Phone:
DHS E Mail
State E Mail
ClassNet:
JWICS:

From (b)(6);(b)(7)(
Sent: Tuesday, January 24, 2017 11:53 PM
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: Social Media

(b)(6);(b

(b)(5)

Let me know if we can be any help here.

(b)(

(b)(6);(b)(7)(C)
Special Agent/Program Manager, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 1:09 PM
To (b)(6);(b)(7)(C)
Cc
Subject: FW: Social Media

(b)(6);(b)(7)(

Please take a look at the attached discovered as part of NSID's social media pilot. Please contact Islamabad and continue to track this.

(b)(6);

(b)(6);(b)(7)(C)
Section Chief, Visa Security Program
International Operations
ICE | Homeland Security Investigations
Washington, DC
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C
Sent: Tuesday, January 24, 2017 12:32 PM
To: (b)(6);(b)(7)(C)
Subject: FW: Social Media

FYI on something we found on our social media pilot for this applicant. Let's talk soon.

From: (b)(6);(b)(7)(C)
Sent: Tuesday, January 24, 2017 9:29 AM
To (b)(6);(b)(7)(
Subject: Social Media

Good morning,

I went ahead and attached the write-up that I sent to (b along with screenshots of the website for the U.S. company. Also, here is the contact information for the TECS record (b)(7)(E)

(b)(6);(b)(7)(C)

I was also wondering, is the email for (b)(6);(b)(7)(C) ? I found a few of them on Lync. I'll go ahead and send the write-up to him as well.

Please let me know if you have any questions!

v/r,

(b)(6);(b)(7)(C)
Intelligence Analyst
ICE/HSI/Visa Security Program
(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
To:
Cc:
Subject: RE: Social Media
Date: Friday, May 29, 2015 10:48:24 AM

Thanks.

From (b)(6);(b)(7)(C)
Sent: Friday, May 29, 2015 10:39 AM
To (b)(6);(b)(7)(C)
Cc
Subject: RE: Social Media

(b)(6);(

(b)(7)(E)

Please let me know if you have any more questions.
Thank you,

(b)(6);(

From: (b)(6);(b)(7)(C)
Sent: Friday, May 29, 2015 10:20 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: Social Media

To date: How many Open Source leads have we sent domestically and internationally? How many arrests resulted from this?

Thanks. (b)(6);(

Background:

The Homeland Security Investigations (HSI) National Security Investigations Division (NSID) Counterterrorism and Criminal Exploitation Unit (CTCEU) combats national security vulnerabilities and prevents terrorists and other criminals from exploiting the nation's immigration system. The pursuit of these violators provides significant support to the "disrupt and deter" counterterrorism strategy of the U.S. CTCEU accomplishes its mission by reviewing the immigration status of known and suspected terrorists, by combating criminal exploitations of the Student and Exchange Visitor Program (SEVP), and by leveraging HSI's expertise with partnering agencies in identifying national security threats. CTCEU is the only national program dedicated to the enforcement of nonimmigrant visa violations.

CTCEU focuses its efforts on identifying and prioritizing, for enforcement action, foreign nationals who overstayed their period of admission or otherwise violated the terms or conditions of their admission to the U.S. CTCEU receives nonimmigrant compliance information from various investigative databases and Department of Homeland Security (DHS) entry/exit registration systems. The information identifies nonimmigrants who have entered the U.S. through an established immigration entry process and may have failed to comply with immigration regulations. Using a comprehensive prioritization scheme, CTCEU identifies nonimmigrant overstays, conducts in-depth analyses, locates targets, and initiates field investigations by referring high priority information to HSI Special Agents nationwide. CTCEU reviews over 1,000,000 violator leads for derogatory information annually and sends approximately 8,400 cases to HSI field offices for investigation.

DESCRIPTION OF REQUIREMENTS

The objective of this task order is to collect, research, analyze, and populate data in various law enforcement databases, as well as work with other government agencies at off-site locations. The Contractor shall be expected to meet operational demands and ensure timely responses to projects, daily requirements such as lead development and completion of weekly lead imports to ensure no backlogs develop, support operational components and timely submissions of deliverables.

The Government anticipates requiring continuation of the following tasks:

Task 1: Vetting and Screening.

The Contractor shall conduct searches of designated ICE systems, other government agency computer systems, and open source sites in order to identify violations and lead viability. The Contractor shall ensure that Contractor employees have or develop knowledge in the following:

- Terrorist organizations, history, operations, and tactics to include an understanding of how the various terrorist organizations operate.
- Illicit cross-border movement of people, cargo, vehicles, drugs, etc. and/or trade industry, to include identifying suspect trends and patterns.
- International criminal organizations (or international smuggling) and how the organizations operate and their areas of operation.

The Contractor shall perform analytical research and data analysis that includes, but is not limited to:

- Performing assessments on individuals, groups, financial institutions, commodities, and travel patterns on targets of interest.
- Having the ability to ingest and screen large volumes of Visa electronic applications efficiently and at high speed in regard DHS holdings in development of pre-adjudication information, derogatory and threat information assessment, adjudication recommendation to the Department of State and notification to other government equites when warranted.
- Providing case identification and tracking of IV and NIV applications at post through the application and adjudication process and provide electronic mechanism to push information to relevant partner programs systems and subsystems.
- Provide mechanism for scraping Visa issuance information to records and provide electronic mechanism to push information to relevant partner programs systems and subsystems.
- Provide multiple Metric solution capabilities in regard visa applicant, applications, VSPTS cases, ICM cases and trend analyses functions; provide external mechanism to validate the same information remotely. Provide electronic mechanism to push information to relevant partner programs systems and subsystems.

Task 2: Lead Generation.

The Contractor shall establish a team of highly trained analysts to perform case initiations, case reroutes, and case closures. These analysts shall be responsible for ensuring that each lead to the field is accurate and thorough. Additionally, these analysts shall provide investigative support to the field as needed. The Contractor shall generate a minimum of 10,000 investigative leads annually to the appropriate HSI field offices. To accomplish this, the Contractor shall provide:

- Automated lead review to determine lead viability.
- Process leads timely to ensure no backlogs occur on a monthly basis.
- Append viable leads daily to the case management database for further processing.
- Close non-viable leads daily in the LeadTrac Mod database management system.
- Develop strategies to exploit the various internal and external data sources to refine the intelligence analysis process.
- Implement process improvements and reengineer methodologies for modernization of systems and projects.
- Conduct bulk data extractions and insertions as required in LeadTrac Mod and Mongodb environment or other systems.

Task 3: Social Media Exploitation.

The Contractor shall leverage open source/social media to expand upon CTCEU's established abilities to utilize government and law enforcement databases in the investigation of national security and public safety concerns that exploit vulnerabilities in the U.S. immigration system by applying social media analytic capabilities, *derived only from free and publicly available sources through unattributed computers,* in numerous ways, including:

3.1 The Contractor shall use the open source information to identify actionable intelligence in addition to enhancing investigative findings, which includes, but is not limited to:

- Identification of recent valid addresses

- Investigation of cold cases
- Enhancement of subject identification
- Performing trend analysis
- Identification of criminal activity and derogatory information
- Identification of terrorist links and recruitment efforts displayed online

The Contractor shall analyze and apply techniques to exploit publically available information, such as media, blogs, public hearings, conferences, academic websites, social media websites such as Twitter, Facebook, and LinkedIn, radio, television, press, geospatial sources, internet sites, and specialized publications with intent to extract pertinent information regarding targets, including criminals, fugitives, nonimmigrant violators, and targeted national security threats and their location.

3.2 The National Security Investigations Division (NSID) seeks to develop a system to encompass the entire lifecycle of visa applicants from application through visa issuance, entry, departure, overstay or otherwise violation of the terms of admission into the United States.

Through the Visa Overstay Lifecycle pilot program, launched in August 2016, NSID visa screening operations are currently bifurcated and supported by two systems: the Visa Security Program's (VSP) Pre-Adjudicated Threat Recognition and Intelligence Operations Team (PATRIOT), and CTCEU's overstay enforcement system. PATRIOT identifies national security, public safety, and other visa eligibility concerns at the earliest point of an individual's visa application lifecycle. Upon entry to the United States, CTCEU then tracks the visa for the remaining validity and lifecycle.

The pilot project is designed to track the online activity of nonimmigrant visa holders that were issued in particular countries of concern from the time of application, through visa issuance, and entry into the United States. The project will conduct initial screening for social media presence and ongoing monitoring of social media activity, to continue during travel in the United States, until subsequent departure. This ongoing monitoring is focused on certain key indicators of emergent concerns, such as threats to public safety or affiliation with known or suspected terrorists or terror groups. Any derogatory information developed is then evaluated and referred for investigation and other actions as appropriate. In the event that the individual violates the terms and conditions of their admission to the United States or overstays their period of admission, the system allows HSI to leverage social media activity to locate and detain the individual. To enhance the Visa Overstay Lifecycle pilot program, the Contractor shall:

- Have the ability to ingest and screen against large volumes of visa electronic applications efficiently and at high speed in regard worldwide social media and open source holdings and domains relevant to person centric derogatory and threat information assessment information, adjudication recommendation to the Department of State and notification to other government equites when warranted. And, provide electronic mechanism to push information to relevant partner programs systems and subsystems.
- Develop a robust, overarching vetting process that would streamline the process to encompass the entire lifecycle of visa applicants from application through visa issuance, entry, departure, overstay, or otherwise violation of their terms of admission.

- Identify ways to more fully leverage social media as a tool to identify the whereabouts and activity of status violators, and provide enhanced knowledge about a nonimmigrant visitors' social media postings, from the adjudication of the visa application, through admission to the United States, and during their time in the United States.
- Take action to bridge the gap between what is done by VSP screening on the front end and what CTCEU systems do on the back-end.

Task 4: Government and/or Contractor Provided Training.
The Contractor shall provide a dedicated training team that will be responsible for all initial system and database training. The Government, on occasion, shall provide subsequent training, but not specific to lead generation. The Government will also provide occasional advanced training to contract staff. This may include, but is not limited to:

- FALCON
- Student and Exchange Visitor Information System (SEVIS)
- United States Visitor Immigrant Status Indicator Technology Registration System (US-VISIT)
- Central Index System (CIS)
- Computer Linked Automated Information Management System (CLAIMS)
- Refugee, Asylum & Parole System (RAPS)
- Consular Consolidated Database (CCDI)
- ENFORCE Alien Removal Module (EARM)
- Treasury Enforcement Communications System (TECS II)
- National Crime Information Center (NCIC)
- Consolidated Lead Evaluation and Reporting System (CLEAR)
- Automatic Targeting System – Passenger (ATS-P)
- Enterprise Document Management System (EDMS)
- Interim Case Management Solution (ICMS)
- Open Source Analysis (OS)
- Standard Operating Procedures for LeadTrac Mod and supporting systems, protocols, and tasks.

Task 5: Statistical / Data Review Support.
The Contractor shall provide statistical and data review support that includes, but is not limited to, the following:

- Analyze data integrity and consistency to obtain a quantitative basis for decision making and resource allocation.
- Provide intelligence and threat analysis of the information that is tailored to the government's requirements.
- Provide written reports and populate DHS databases or any other designated database as required.
- Provide specialized analysis related to data integrity, content of information, and production support in the Mongodb environment.
- Evaluate new technological capabilities to enhance productivity and efficiency.
- Conduct trend analyses and advanced technical research techniques to develop products based on the government's requirements.

- Extract data and develop reports from the LeadTrac Mod system as required.
- Create whitepapers and update Standard Operating Procedures as required.

Task 6: Ad Hoc Reporting.

The Contractor shall develop and produce qualitative intelligence reports, referred to as CTCEU reports, utilizing government databases and open source analysis for a comprehensive product. The Contractor shall provide an assessment package of the targets of interests to include; briefings, presentations, discussion panel participation, supporting documents and reports. The Contractor shall conduct research, generate reports, and assist with classified projects, as requested.

Homeland Security Investigations
National Security Investigations Division
Assistant Director

U.S. Immigration and Customs Enforcement

Social Media Pilot Program Talking Points

(b)(5);(b)(7)(E)

[redacted]

This pilot program aims to more fully leverage social media as a tool to identify the whereabouts and activity of status violators, and provide enhanced knowledge about a non-immigrant visitors' social media postings.

The social media tracking gives the U.S. government better visibility should a non-immigrant visitor engage in unlawful activity (e.g. criminality, terrorism, administrative immigration violations).

The Social Media pilot program utilizes an automated social media vetting platform that ingests biographic data of non-immigrant visa applicants to conduct initial screening of online social media presence and provides screening results at the time of visa application.

(b)(5);(b)(7)(E)

[redacted]

(b)(7)(E);(b)(5)

[redacted]

Privacy Requirements for Operational Use of Social Media

November 2013

U.S. Immigration
and Customs
Enforcement

ICE

Training Goals & Objectives

- To ensure ICE personnel understand and comply with the DHS Privacy Policy for Operational Use of Social Media (June 8, 2012)
  - DHS Directive 110-01
  - DHS Instruction 110-01-001
- This course covers:
  - Key definitions
  - Rules of Behavior for Law Enforcement and Non-Law Enforcement Activities

U.S. Immigration and Customs Enforcement

ICE

What Does This Policy Do?

- Regulates how DHS collects personally identifiable information (PII) from “Social Media” Internet sites for an “Operational Use”
- Requires DHS components and offices to establish Rules of Behavior that personnel must follow
- Requires annual training of all personnel who engage in this type of activity

U.S. Immigration and Customs Enforcement

ICE

Why Was This Policy Created?

- To address public and congressional concerns about how DHS collects PII from Social Media sites
- To ensure DHS is not engaging in an unlawful or inappropriate collection of PII from Social Media
- To ensure that there are clear “dos and don’ts” for personnel to follow – these are called the “Rules of Behavior”
- To ensure all DHS personnel are aware of the rules through annual training

U.S. Immigration and Customs Enforcement

ICE

What is the "Operational Use" of "Social Media"?

When DHS is collecting PII about individuals from a Social Media site for the purpose of:

- Investigating them (criminal, civil, or administrative)
- Making a benefit decision about them
- Making a personnel or suitability decision about them
- Enhancing situational awareness (to support incident management decision making)
- Any other official purpose that potentially may affect their rights, privileges, or benefits

DHS Instruction 110-01-001, Section IV.D.

U.S. Immigration and Customs Enforcement

ICE

This Policy Does Not Apply To:

- Agency use of Social Media for communications and outreach to the public
- Personnel use of Social Media for professional development, such as training and continuing education
- Use of Social Media to facilitate internal meetings
- Use of internal DHS intranets or applications
- Use of search engines for general Internet research

U.S. Immigration and Customs Enforcement

What is Personally Identifiable Information (PII)?

"Any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

"For example, when linked or linkable to an individual, such information includes a name, Social Security Number, date and place of birth, mother's maiden name, Alien Registration Number, account number, license number, vehicle identifier number, license plate number, … IP address, biometric identifier, educational information, financial information, medical information, criminal or employment information," etc.

DHS Instruction 110-01-001, Section IV.E.

ICE

U.S. Immigration
and Customs
Enforcement

What is "Social Media"?

"The sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact.

"Social media take many different forms, including but not limited to web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies.

"This definition does not apply to internal Department intranets or applications."

DHS Instruction 110-01-001, Section IV.K.

How Do I Know When I Am on a "Social Media" Site Online?

- Some sites are clearly Social Media, like Facebook and Twitter
- Because of the trend toward including interactive, Social Media-type features on "regular" Internet sites, it is often hard to know if you are on a "regular" Internet site or a "Social Media" site
- Because of this, ICE has created local policies (Rules of Behavior) that govern the collection of PII online at all Internet sites, not just Social Media

ICE

How Do I Know When I Am on a "Social Media" Site Online?

- Because ICE's Rules of Behavior apply to all online activity where you collect PII, you do not have to be concerned about whether you are on a Social Media site, or a regular Internet site
- Simply follow the appropriate Rules of Behavior *anytime* you collect PII online:
  - Collection for a law enforcement purpose – follow the ICE Law Enforcement Rules of Behavior
  - Collection for a non-law enforcement purpose – follow the ICE Non-Law Enforcement Rules of Behavior

U.S. Immigration and Customs Enforcement

ICE

ICE Rules of Behavior (ROB) for Non-Law Enforcement Activities

U.S. Immigration
and Customs
Enforcement

ICE ROB for Online Non-Law Enforcement Activities

- Established in a Memorandum from John Morton to ICE Personnel, *Use of Public Online Information for Non-Law Enforcement Work-Related Activities* (May 17, 2013)
  - https://insight.ice.dhs.gov/mgt/oop/Documents/pdf/ice-internet-use-non-law-activities-memo.pdf

ICE

ICE ROB for Online Non-Law Enforcement Activities

- Applies to <u>any</u> ICE personnel conducting non-law enforcement activities:
  - Where PII is collected
  - For a non-law enforcement purpose
  - From the Internet

- Law enforcement personnel will follow these Rules when engaging in non-law enforcement activities (e.g., mission support, personnel, etc.) online.

U.S. Immigration and Customs Enforcement

ICE ROB for Non-LE Activities

- Use of equipment
  - You may use only government-issued equipment, government accounts, and government e-mail addresses.
- Use of email and accounts
  - You may use only online screen names or identities that indicate an official DHS affiliation and have been created using DHS e-mail addresses.

ICE

ICE ROB for Non-LE Activities

- Public interaction
  - You may access publicly available information only by reviewing posted information without interacting (e.g., “friending,” “fanning,” “liking”) with any individual who posted the information.
- Privacy settings
  - You must respect individual privacy settings and access only information that is publicly available unless the individual whose information you seek to access has given you consent to access it.

U.S. Immigration and Customs Enforcement

ICE

ICE ROB for Non-LE Activities

- PII collection
  - Collect the minimum PII necessary for your authorized duties.
- PII safeguards
  - Protect PII as required by the Privacy Act and DHS privacy policy.

U.S. Immigration and Customs Enforcement

ICE ROB for Non-LE Activities

- Documentation
  - Retain the contents of your use of the Internet, including social media, if you would have retained that information had it been written on paper.
  - Preserve in appropriate ICE recordkeeping systems in accordance with office procedures and in a manner authorized by the relevant records schedule.

ICE ROB for Non-LE Activities

- Online communications generally
  - You may use online services to communicate in the same way that you are authorized to use other types of communication tools, such as the telephone and the mail.
- Activity during personal time
  - While not on duty, you are generally free to engage in personal online pursuits.
  - If, however, the off-duty online activity on government issued or personal equipment directly and substantially relates to a work-related matter, you are bound by the same restrictions regarding the use of online information as would apply when on duty.

Non-LE Activities and LE Activities

- Non-LE Activities
  - If you only engage in Non-Law Enforcement Activities the training ends here.
  - Last slide of presentation contains contact information for additional questions.
  - Memorandum from John Morton to ICE Personnel, Use of Public Online Information for Non-Law Enforcement Work-Related Activities (May 17, 2013)
    - https://insight.ice.dhs.gov/mgt/oop/Documents/pdf/ice-internet-use-non-law-activities-memo.pdf
- LE Activities
  - If you engage in law enforcement activities, the training for Online Law Enforcement Activities continues on the next slide.

U.S. Immigration
and Customs
Enforcement

ICE