Homeland Security Investigations

National Security Investigations Handbook

HSI HB 13-03 / April 26, 2013

U.S. Immigration and Customs Enforcement

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

Foreword

The National Security Investigations Handbook provides a uniform source of national policies, procedures, responsibilities, guidelines, and controls to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents when conducting national security-related investigations. This Handbook contains instructions and guidance to help ensure uniformity and operational consistency among all HSI field offices. Oversight over the HSI National Security Program resides with the Unit Chief, National Security Unit. (Note: On June 9, 2010, the ICE Offices of Investigations (OI), International Affairs, and Intelligence were realigned under HSI. Throughout this Handbook, documents issued prior to the June 9, 2010, realignment are referred to using the original organizational names in their titles, e.g., "OI" instead of "HSI").

This 2013 edition of the National Security Investigations Handbook amends Sections 12.1 and 12.3 of HSI HB 11-02, National Security Investigations Handbook," dated April 27, 2011. HSI HB 11-2 is hereby superseded. This 2013 edition also supersedes the HSI memorandum entitled, "Joint Terrorism Task Force Staffing," dated January 19, 2012.

The National Security Investigations Handbook is an internal policy of HSI and is not intended to confer any right or benefit on any private person or party. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Records and Disclosure Unit, as well as the Office of the Principal Legal Advisor at Headquarters and the local U.S. Attorney's Office, if appropriate, are to be consulted so that appropriate measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure in civil discovery pursuant to the law enforcement privilege. Any further request for disclosure of this Handbook or information contained herein should be referred to the HSI Records and Disclosure Unit.

The HSI Policy Unit is responsible for coordinating the development and issuance of HSI policy. All suggested changes or updates to this Handbook should be submitted to the HSI Policy Unit, which will coordinate all needed revisions with the National Security Unit.

4/26/2013

James A. Dinkins
Executive Associate Director
Homeland Security Investigations

Date

NATIONAL SECURITY INVESTIGATIONS HANDBOOK

Table of Contents

NATIONAL SECURITY INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The National Security Investigations Handbook establishes policy and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs) when conducting national security-related investigations within the scope of their authority. This Handbook also provides guidance governing investigations conducted by SAs in support of the Joint Terrorism Task Forces (JTTFs), under the authorities granted to ICE. (Note: The Federal Bureau of Investigation (FBI) is the designated coordinating agency, through its JTTFs, for counterterrorism investigations in the United States.)

Chapter 2. INTRODUCTION

Prior to the events of September 11, 2001, neither the immigration nor the customs authorities were widely recognized as effective and powerful counterterrorism tools in the United States. With the creation of the Department of Homeland Security (DHS), ICE became integral to the U.S. Government's approach to the Global War on Terrorism (GWOT) through the implementation of new programs to better address national security threats and detect potential terrorist activities in the United States. HSI investigates individuals and their money and materials that support terrorism and other criminal activity, and is uniquely suited, due to its broad law enforcement authorities, to investigate national security cases and further the GWOT.

The investigative approach used with national security investigations (NSIs) differs from approaches used with other criminal investigations, because 1) NSIs are primarily focused on intelligence collection while simultaneously run as criminal investigations; and 2) NSIs are frequently monitored to detect when intentions of a group (or an individual operating alone) match its capabilities to carry out an attack. The HSI National Security Unit (NSU) monitors NSIs to ensure deconfliction with other agencies.

HSI SAs work closely with HSI's partner agencies within DHS, such as the U.S. Customs and Border Protection (CBP)'s Office of Field Operations and Office of Border Patrol, U.S. Citizenship and Immigration Services (USCIS), and Transportation Security Administration (TSA), to provide a unified and coordinated effort in countering terrorist threats and to further JTTF investigations, particularly those where HSI's unique authorities are brought to bear. It is incumbent upon HSI SAs to form a cohesive and complementary partnership with other DHS components assigned to nationwide JTTFs within the provisions of interagency guidelines.

Chapter 3. DEFINITIONS

The following definitions are provided for the purposes of this Handbook:

3.1 Automated Biometric Identification System

The Automated Biometric Identification System (IDENT) is a part of the DHS biometric database. It collects biometric, biographical, and encounter-related data in operational environments. Biometric data includes, but is not limited to, fingerprints and photographs. Biographical data includes, but is not limited to, name, date of birth, nationality, and other personal descriptive data.

3.2 Central Index System

The Central Index System (CIS) is a master records management system that displays biographical information on certain classes of aliens and certain U.S. citizens. CIS also identifies the physical location of the alien's file (A-file).

3.3 Electronic System for Travel Authorization

The Electronic System for Travel Authorization is a CBP electronic system utilized by individuals wishing to travel to the United States under the Visa Waiver Program.

3.4 Enforcement Integrated Database

The Enforcement Integrated Database (EID) is an ICE database repository and event-based case management system that documents, tracks, and manages the reporting of enforcement cases. Its functions include subject processing, biometric identification, allegations and charges, preparation and printing of appropriate forms, data repository, and interface with national databases of enforcement events. The Enforcement Case Tracking System (ENFORCE) supports alien apprehension processing for both "Voluntary Return" and "Notice to Appear" actions. ENFORCE also contains the National Security Entry/Exit Registration System (NSEERS) module through which all NSEERS registrations are performed. ENFORCE is the principal user interface with EID.

3.5 Foreign Terrorist Organizations

Foreign Terrorist Organizations (FTOs) are foreign groups designated by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended. FTO designations play a critical role in HSI's fight against terrorism and are an effective means of curtailing support for terrorist activities and FTOs' ability to conduct business or financial transactions within the United States.

3.6 Joint Vetting Unit

Created in 2005 by HSI (then the Office of Investigations (OI)), the Joint Vetting Unit (JVU) is responsible for the deconfliction of HSI investigative leads with the FBI's Counterterrorism Division (CTD) Terrorism Financing Operations Section. (Note: The JVU is staffed by ICE HSI and FBI personnel.)

3.7 National Security Entry/Exit Registration System

NSEERS provides detailed information on nonimmigrants, including background, purpose of a nonimmigrant's visit to the United States, and departure information. On April 28, 2011, through a notice published in the Federal Register, DHS removed the list of countries whose nationals had been subject to NSEERS registration and reporting requirements. The notice also announced that DHS would no longer register aliens under the NSEERS program. DHS has suspended all special registration and reporting requirements associated with the NSEERS program.

3.8 National Security Interest

National Security Interest is a determination that a particular individual is someone for whom sufficient information exists to warrant opening an investigation in accordance with Attorney General (AG) Guidelines for NSIs and Foreign Intelligence Collection. A person of National Security Interest is any person engaging in (a) International terrorism, (b) Espionage and other intelligence activities, sabotage, or assassination, conducted by, for or on behalf of foreign powers, organizations, or persons; (c) Foreign computer intrusions; and/or (d) Other matters as determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

3.9 Significant Event Notification

The Significant Event Notification (SEN) system is an ICE Intranet application reporting system designed to facilitate the seamless entry and query of reports.

3.10 Student and Exchange Visitor Information System

Managed by the Student and Exchange Visitor Program (SEVP), the Student and Exchange Visitor Information System (SEVIS) is an integrated system that maintains accurate and current information on nonimmigrant students (F and M visas), exchange visitors (J visa), and their dependents (F-2, M-2, and J-2). SEVIS enables schools and program sponsors to transmit mandatory information and event notifications, via the Internet, to DHS and the Department of State (DOS) throughout a student or exchange visitor's stay in the United States.

3.11 Terrorist Identities Datamart Environment

The Terrorist Identities Datamart Environment (TIDE) is the U.S. Government's central repository of known or suspected international terrorist identities. It refers to the terrorist environment as a whole, as well as individual watch-listed subjects. (b)(7)(E)

(b)(7)(E)

3.12 Triggering Event

A Triggering Event is one that causes circumstances to exist inside or outside the boundaries of the United States that raise grave national security concerns requiring a rapid and coordinated law enforcement response.

3.13 United States Visitor and Immigrant Status Indicator Technology

United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is part of a continuum of biometrically-enhanced security measures that begin outside the U.S. borders and continue through a visitor's arrival in and departure from the United States. US-VISIT applies to all visitors (with limited exceptions) entering the United States, regardless of country of origin or whether they are traveling on a visa by air, sea, or land.

Chapter 4. AUTHORITIES/REFERENCES

4.1 Statutory Authorities Related to National Security Investigations

A. INA, Title 8, United States Code (U.S.C.), Sections 1101-1574, 1182 (2000), General Classes of Aliens Ineligible to Receive Visas and Ineligible for Admission;

B. Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, 108 Pub. L. 458, §§ 1021-1023, 118 Stat. 3638, 3825-3832, National Counterterrorism Center (NCTC), National Counter Proliferation Center, and National Intelligence Centers;

C. Id. at § 7215, Terrorist Travel Program;

D. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 107 Pub. L. 56 §§ 411-418, 418, 115 Stat. 272 (2001) [enhanced immigration provisions];

E. 8 U.S.C. § 1225, Inspection by Immigration Officers; Expedited Removal of Inadmissible Arriving Aliens;

F. 8 U.S.C. § 1324, Bringing in and harboring certain aliens;

G. 8 U.S.C. § 1357, Powers of Immigration Officers and Employees;

H. 19 U.S.C. § 482, Search of vehicles and persons;

I. 19 U.S.C. § 507, Assistance for Officers;

J. 19 U.S.C. § 1401(i), Customs Officers;

K. 19 U.S.C. § 1461, Inspection of merchandise and baggage;

L. 19 U.S.C. § 1467, Special inspection, examination, and search;

M. 19 U.S.C. § 1496, Examination of baggage;

N. 19 U.S.C. § 1499, Examination of merchandise;

O. 19 U.S.C. § 1581, Boarding vessels;

P. 19 U.S.C. § 1582, Search of persons and baggage, regulations;

Q. 19 U.S.C. § 1583, Examination of outbound mail;

R. 19 U.S.C. § 1589a, Enforcement authority of customs officers;

S. 19 U.S.C. § 1595, Searches and seizures;

T. 31 U.S.C. § 5317, Search authority for compliance with Currency and Monetary Instruments Reporting Act;

U. Title 8, Code of Federal Regulations (C.F.R.), Section 236.1(e), Privilege of Communication;

V. 19 C.F.R. Part 145, Mail importations;

W. 19 C.F.R. Part 162, Inspection, Search, and Seizure; and

X. 31 C.F.R. § 594.201, Treasury Office of Foreign Assets Control (OFAC) regulations authorize the blocking and seizing of international cargo and goods being imported and exported to Specifically Designated Global Terrorists (SDGTs), companies, and entities of SDGTs.

4.2 Specific Criminal Charges Used in National Security Investigations

A. 18 U.S.C. § 2332a, Use of weapons of mass destruction;

B. 18 U.S.C. § 2332b, Acts of terrorism transcending national boundaries;

C. 18 U.S.C. § 2332d, Financial transactions;

D. 18 U.S.C. § 2332f, Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities;

E. 18 U.S.C. § 2332g, Missile systems designed to destroy aircraft;

F. 18 U.S.C. § 2332h, Radiological dispersal devices;

G. 18 U.S.C. § 2339, Harboring or concealing terrorists;

H. 18 U.S.C. § 2339a, Providing material support to terrorists, organizations involved in torture or the recruitment of child soldiers;

I. 18 U.S.C. § 2339b, Providing material support to a designated foreign terrorist organization; and

J. 18 U.S.C. § 2339d, Receiving military-type training from a foreign terrorist organization.

4.3 General and ICE-Specific Criminal Charges Used in National Security Investigations

A. 8 U.S.C. § 1304(e), Failure to carry proof of permanent residence;

B. 8 U.S.C. § 1325, Improper Entry by Alien;

C. 8 U.S.C. § 1325(c), Marriage Fraud;

D. 8 U.S.C. § 1326, Re-entry after deportation/removal;

E. 13 U.S.C. § 305, Penalties for unlawful export information activities;

F. 18 U.S.C. § 371, Conspiracy;

G. 18 U.S.C. § 542, Entry of goods by means of false statements;

H. 18 U.S.C. § 545, Smuggling goods into the United States;

I. 18 U.S.C. § 554, Smuggling goods from the United States;

J. 18 U.S.C. § 641, Public money, property or records;

K. 18 U.S.C. § 911, False claims to U.S. citizenship;

L. 18 U.S.C. § 922(g)(5), Alien unauthorized to possess a firearm;

M. 18 U.S.C. § 951, Agent of foreign governments;

N. 18 U.S.C. § 1001, False statements;

O. 18 U.S.C. § 1015, Fraud and statements regarding naturalization, citizenship or alien registry;

P. 18 U.S.C. § 1028, Fraud and related activity in connection with identification documents, authentication features, and information;

Q. 18 U.S.C. § 1425, Naturalization Fraud;

R. 18 U.S.C. § 1543, Forgery or false use of passport;

S. 18 U.S.C. § 1546, Visa/Immigration Fraud;

T. 18 U.S.C. § 1956, Laundering of monetary instruments;

U. 18 U.S.C. § 1957(a), Engaging in monetary transactions in property derived from specified unlawful activity;

V. 18 U.S.C. § 1960, Prohibition of unlicensed money transmitting businesses;

W. 18 U.S.C. § 1961, Racketeer Influenced and Corrupt Organizations;

X. 18 U.S.C. § 2320, Trafficking in counterfeit goods or services;

Y. 22 U.S.C. § 401, Shipping Export Declaration, Violation;

Z. 22 U.S.C. § 611, Unregistered Agent of a Foreign Government;

AA. 22 U.S.C. § 2778, Conspiracy to violate the Arms Export Control Act;

BB. 31 U.S.C. § 5324, Structuring transactions to evade reporting requirement prohibited;

CC. 31 U.S.C. § 5332, Bulk cash smuggling into or out of the United States;

DD. 50 U.S.C. § 1701-05, International Emergency Economics Powers Act and Economic and Commercial activities associated with SDGTs; and

EE. 22 C.F.R. § 129.2(a), Brokering the sale and transfer of defense articles.

4.4 National Security-Related Administrative Charges

A. INA § 212(a)(3), Security Related Inadmissibility Grounds; and

B. INA § 237(a)(4), Security Related Deportation Grounds.

4.5 References

A. Presidential Decision Directive (PDD) 39, issued in 1995, was a formative document that stated, in part, that "it is the policy of the United States to deter, defeat, and respond vigorously to all terrorist attacks on our territory and against our citizens, or facilities."

B. PDD 62, issued in 1998, directs various U.S. agencies to develop integrated programs to increase interagency effectiveness in countering, managing, and containing terrorism. To that end, the JTTF program, which embodies the objectives of U.S. policy on counterterrorism as set forth in PDD 39, was reaffirmed and subsequently expanded following the terrorist attacks of September 11, 2001.

C. Homeland Security Presidential Directive (HSPD) 2 directs the AG to create the Foreign Terrorist Tracking Task Force to ensure that various agencies coordinate programs to deny entry into the United States to aliens associated with, suspected of being engaged in, or supporting terrorist activity, and to locate, detain, prosecute, or deport any such aliens already present in the United States.

D. HSPD 6 provides a consolidated approach to proactively target terrorist travel. It establishes the Terrorist Screening Center (TSC) to consolidate terrorist names and identifiers into a single database. Furthermore, it mandates that all international terrorist information be provided to the NCTC. Agencies are prohibited from maintaining a separate terrorist watchlist.

E. HSPD 7 establishes a framework for federal agencies to identify, prioritize, and protect the critical infrastructure and key resources (CIKR) of the United States from terrorist attacks. It established the National Infrastructure Protection Plan and sets forth the responsibilities for CIKR partners.

F. HSPD 15 (contents classified) aims to improve government coordination by limiting bureaucratic hindrances that limit the ability of various federal

agencies (including ICE) to combat terrorism. SAs should contact the Unit Chief, NSU, to obtain a classified copy of this HSPD.

G. HSPD 19 establishes a national policy on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States. It mandates that the Secretary of Homeland Security coordinate with other federal agencies to maintain secure information-sharing systems.

H. HSPD 24 establishes a framework to ensure that federal executive departments and agencies use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric information.

I. IRTPA of 2004, 108 Pub. L. 458, §§ 1021-1023, 118 Stat. 3638, 3825-3832. NCTC, National Counter Proliferation Center, and National Intelligence Centers.

J. Id. at § 7215. Terrorist Travel Program.

K. ICE Directive 7-6.0, "Border Searches of Documents and Electronic Media" (July 16, 2008, or as updated). (Superseded by ICE Directive 7-6.1 only as it relates to electronic devices.)

L. ICE Directive 10044.1 (former number: 7-6.1), "Border Searches of Electronic Devices" (August 18, 2009, or as updated).

M. HSI Directive 12-02, "Terrorist Identities Datamart Environment" (October 19, 2012, or as updated).

N. ICE Memorandum (Policy #10031.1), "Use of Joint Vetting Unit to Coordinate Terrorist Financing Investigations" (August 24, 2007, or as updated).

O. ICE Memorandum (Policy #10068.1), "DHS Guidance Regarding Polygraph Examinations of ICE Officers Assigned to the FBI Joint Terrorist Task Forces" (January 22, 2007, or as updated).

P. OI Memorandum, "Border Searches of Electronic Devices Directive" (August 31, 2009, or as updated).

Q. OI Memorandum, "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media" (December 12, 2008, or as updated).

R. OI Memorandum, "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry" (March 5, 2007, or as updated).

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

The Executive Associate Director (EAD) of HSI has the overall responsibility for the management and implementation of the policies and procedures set forth in this Handbook.

5.2 Special Agents in Charge

Special Agents in Charge (SACs) are responsible for implementing the provisions of this Handbook within their respective areas of responsibility (AORs).

5.3 Special Agents

SAs are responsible for complying with the provisions of this Handbook.

Chapter 6. NATIONAL SECURITY INVESTIGATIVE PRIORITIES AND PROGRAMS

6.1 National Security Investigative Priorities

NSU's mission is to oversee HSI's investigation, detection, interdiction, and participation in the prosecution and/or removal of the following classifications of targets:

(b)(7)(E)

NSU is part of the HSI National Security Investigations Division (NSID) and is comprised of four programmatic sections that oversee and provide operational guidance to SAs conducting NSIs.

Below is a brief summary of the four sections and their related responsibilities:

A. Counterterrorism Section

The Counterterrorism Section (CTS) provides programmatic oversight of HSI's nationwide participation in the JTTFs. CTS has dedicated HSI liaisons to the FBI's CTD International Terrorism Operations Section to monitor and support JTTF counterterrorism investigations from a Headquarters (HQ) perspective and ensure that HSI is appropriately engaged in NSIs where ICE authorities are viewed as the most likely avenue to dismantle a terrorist network or thwart an impending terrorist attack. CTS maintains a contingent staff at NSU to facilitate this programmatic oversight and respond to senior level ICE and DHS requests regarding NSIs.

B. Threat Analysis Section

The Threat Analysis Section (TAS) assesses threat reporting on high-risk targets and develops investigative leads relating to identified national security vulnerabilities. TAS also identifies non-obvious relationships between known or suspected terrorists and individuals located in the United States. TAS reports summarizing investigative pedigree information and potential actionable leads are forwarded to HSI JTTF SAs for coordination with their law enforcement counterparts.

TAS also manages HSI's Border Search Program, specifically as it relates to documents and digital media. TAS works closely with the DHS' Joint Analysis Group and other government organizations to provide enhanced forensic capability and translation services on those related items detained or seized in the course of NSIs.

TAS adds analytical value, in partnership with the Counterterrorism and Criminal Exploitation Unit (CTCEU) through the National Security Threat Task Force (NSTTF), which is responsible for reducing the vulnerability of the United States by improving the (b)(7)(E)
(b)(7)(E)

C. National Targeting Center

The ICE National Targeting Center (NTC), a Section in NSU, documents all positive TIDE matches and national security-related issues in the ICE NTC database. The ICE NTC will notify the appropriate SAC or designee if it becomes aware of a subject of interest, investigative activity, or threat in the

affected SAC's AOR outside the port of entry (POE). (b)(7)(E)

(b)(7)(E)

D. National Security Integration Center

The National Security Integration Center (NSIC) is responsible for developing and coordinating joint programs/initiatives with other law enforcement agencies and the Intelligence Community (IC) that appropriately utilize ICE's authorities and information to support DHS' responsibilities for mitigating threats to national security.

6.2 Post September 11, 2001, Congress Mandated Programs

In response to the events of September 11, 2001, and the subsequent increased threat of terrorism within the United States, Congress mandated two programs to identify, screen, and track nonimmigrants residing in or visiting the United States. These two programs were developed and placed under the direction of the CTCEU to monitor certain nonimmigrants in the United States. These programs, while not overseen or directed by NSU, nonetheless provide valuable investigative tools for HSI JTTF SAs.

A. National Security Entry/Exit Registration System

NSEERS requires the registration of those nonimmigrants designated by the AG (in consultation with the Secretary of State) who are citizens of designated countries. As stated in Section 3.7, on April 28, 2011, through a notice published in the Federal Register, DHS removed the list of countries whose nationals have been subject to NSEERS registration and reporting requirements. The notice also announced that DHS would no longer register aliens under the NSEERS program. DHS has suspended all special registration and reporting requirements associated with the NSEERS program. DHS is currently working on guidance regarding the NSEERS program.

B. Student and Exchange Visitor Information System

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 mandated the collection of current information on a continuing basis from

schools and exchange programs relating to nonimmigrant foreign students and exchange visitors enrolled in their programs. This was accomplished with the creation of SEVIS in 2003. This data is made available to ICE for the duration of the nonimmigrant's stay in the United States. In addition, it revises and enhances the process by which foreign students and exchange visitors gain entrance to the United States.

HSI's SEVP administers SEVIS and is ICE's primary outreach conduit to U.S. educational institutions and associations. SEVP augments HSI's ability to maintain up-to-date information on foreign students and exchange visitors, and take appropriate action if students fail to attend and/or participate in schooling or an exchange program in accordance with SEVP provisions, or properly maintain their status during their stay.

6.3 Terrorist Identities Datamart Environment

A. Background

TIDE is the U.S. Government's central repository of known or suspected international terrorist identities. TIDE contains classified information provided by members of the IC such as the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Security Agency (NSA), the FBI, and many others.

TIDE is administered by the NCTC and is available through the (b)(7)(E) (b)(7)(E) and other systems cleared for (b)(7)(E)

Federal agencies nominate individuals for inclusion in TIDE through the NCTC, based on intelligence and law enforcement terrorism information. (b)(7)(E)

From classified TIDE information, (b)(7)(E) (b)(7)(E) (b)(7)(E) (b)(7)(E) (b)(7)(E) (b)(7)(E) This also represents a major step forward from the pre-September 11, 2001 status of

multiple, disconnected, and incomplete watchlists throughout the U.S. Government.

(b)(7)(E)

B. TIDE Sub-Categories

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

C. Field Response to TIDE Notifications

When SAs receive a TIDE notification from the ICE NTC, they are required to respond and initiate appropriate enforcement action. When a SAC office becomes aware of a positive match to a TIDE or national security lookout at a place other than a POE, the SAC office shall immediately notify the ICE NTC.

When directed by the ICE NTC, SAs are required to (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

D. TIDE Notification from the ICE National Targeting Center

The ICE NTC will provide notification to SAs on positive encounters for appropriate responses.

E. TIDE Notifications from Field Offices to the ICE National Targeting Center

(b)(7)(E)

F. TIDE Issues When Engaged with Other Agencies

If there are any specific issues with other agencies involving the degree and nature of the HSI response to any subject of interest, the field office will contact the ICE NTC, which will coordinate with HSI HQ and field management.

G. TIDE Case Management and Reporting

SAs must thoroughly document all TIDE or national security-related encounters in (b)(7)(E) SAs will open one case number per SA per fiscal year; all TIDE responses will be documented under that one case number. (b)(7)(E)

(b)(7)(E)

H. TIDE Sample Questionnaire

See HSI Directive 12-2, "Terrorist Identities Datamart Environment," dated October 19, 2012, or as updated, for a TIDE Sample Questionnaire.

I. Overall TIDE Responsibilities

The EAD of HSI is responsible for the oversight and implementation of the provisions of HSI Directive 12-02, "Terrorist Identities Datamart Environment," dated October 19, 2012, or as updated.

6.4 National Security Law Section, Office of the Principal Legal Advisor

Located within the ICE Office of the Principal Legal Advisor (OPLA) at ICE HQ, the National Security Law Section (NSLS) is comprised of a team of attorneys who, in conjunction with approximately 100 nationwide specially-designated attorneys in the Offices of the Chief Counsel (OCCs), manage the litigation of national security cases in removal proceedings. (Note: OPLA's Criminal Law Section is the section that provides daily advice on enforcement of export control laws, as well as HSI's general criminal enforcement and border search authorities). NSLS provides legal advice and guidance to all ICE Directorates and Program Offices responsible for the growing number of cases involving terrorism, espionage, sabotage, and other immigration issues related to national security, specifically:

A. The detention and removal of "special interest" aliens.

B. The designation of terrorist entities under Title 8.

C. The civil arrest authority of SAs.

D. Criminal charges under Titles 8 and 18.

E. Benefit eligibility.

F. Denaturalization.

Because of the variety of considerations involved in national security cases, lodging of security and terrorism charges of inadmissibility (INA § 212(a)(3)) or deportability (INA § 237(a)(4)) requires the approval of OPLA's Deputy Principal Legal Advisor. In order to obtain this approval, the local OCC elevates a Prosecution Memorandum to NSLS requesting approval to lodge a national security charge.

NSLS provides assistance (in the form of training, legal review of DHS and ICE policies and procedures, and reviews of press and congressional responses) to DHS and ICE Directorates and Program Offices, including HSI, Enforcement and Removal Operations, the Office of Congressional Relations, the Office of Policy, and the Office of Public Affairs. It should be noted that NSLS also provides litigation support to the Department of Justice (DOJ) on immigration aspects of criminal prosecution cases involving aliens of national security concern. NSLS serves as a liaison in national security matters to the FBI, CIA, DOS, and various DOJ Offices and Divisions, such as the Office of International

Affairs (OIA), the Civil Division's Office of Immigration Litigation, the Criminal Division's CTS, and the local U.S. Attorney's Offices (USAOs).

6.5 Overseas Coordination in Support of National Security Investigations

Because of the international nature of NSIs, SAs may need to travel abroad or request information from foreign governments to further their cases. In locations where HSI OIA does not maintain a presence, NSU will assist SAs, provide support, and help coordinate with other agency partners to obtain the necessary information and ensure that proper support is received at the foreign location. NSU will also notify the appropriate HSI OIA Operations Manager to ensure coordination with the appropriate HSI Attaché.

In locations where there is an HSI Attaché, NSU will coordinate with that Attaché to support the SAs. In instances where foreign travel is required, NSU will ensure that all appropriate country clearances and notifications are made and coordinated through HSI OIA. If there are questions regarding ground support in the foreign location, NSU may provide additional assistance by providing HQ personnel to travel with the field office SAs. This will alleviate any security clearance issues or manpower conflicts encountered by HSI Attachés.

Chapter 7. CONDUCTING TERRORISM OR NATIONAL SECURITY INVESTIGATIONS

7.1 Field Coordination with Headquarters on National Security Investigations

For coordination and deconfliction purposes, SAs engaged in NSIs shall notify NSU of all significant national security-related investigative activity. It is also critical that HSI field offices share information and coordinate with USCIS at the field level to ensure that immigration benefits are not inappropriately extended to aliens who are under active investigation.

The following categories are defined as national security matters:

A. Terrorism-related cases/inquiries/allegations: Activity involving an individual who is suspected of being involved in terrorism or a direct or indirect supporter of a terrorist organization.

B. Other national security cases/inquiries/allegations: Activity involving suspected espionage; engaging in illegal acts involving weapons of mass destruction; being an agent or officer of a hostile foreign intelligence service; or engaging in violations of the import and export laws relating to sensitive information or technology.

7.2. Investigative Case Management

A. Documenting NSI Reports and Cases

(b)(7)(E)

B. NSI Case Categories

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

C. Proper Use of the JTTF and National Security Check Boxes

The mandatory JTTF and national security check boxes will be utilized throughout all (b)(7)(E) ase categories. The JTTF check box will be marked "yes" for:

(b)(7)(E)

(b)(7)(E)

The National Security check box will be marked "yes" for (b)(7)(E)
(b)(7)(E)

The JTTF and National Security check boxes ("Y" or "N") in (b)(7)(E) Case Management can be modified at any time.

(b)(7)(E)

D. Appropriate use of (b)(7)(E) Subject Record Status Codes in NSIs

SAs will not create (b)(7)(E) primary lookout records with Status Codes of
(b)(7)(E)

(b)(7)(E)

7.3 Investigative Methods/Strategies Relating to National Security Investigations

An NSI will usually involve a violation of federal law involving immigration and/or customs statutes. This section offers investigative guidance on common methods used in NSIs. This section is not intended to limit the use of any other approved investigative techniques.

The strategy and mindset of SAs conducting NSIs should be to utilize as many resources as appropriate based on HSI's broad statutory authority. SAs will remain involved in JTTF investigations that pertain to HSI's authorities. Continued and active involvement ensures that HSI remains engaged in significant JTTF investigations.

Investigative methods commonly begin with an allegation of an ICE-related violation of criminal or administrative law. The FBI JTTF case may begin with a broad allegation of terrorism based on an IC reporting or other non-law enforcement agency's database. SAs should review the predicating intelligence and any investigative data already contained in the FBI case file to identify any activity that involves ICE criminal or administrative violations.

Below are various investigative methods fundamental to most NSIs.

7.4 Initiating a National Security Investigation

When initiating an NSI, SAs should:

(b)(7)(E)

(b)(7)(E)

7.5 Information Security Considerations on a National Security Investigation

During the course of an NSI, it is critical that SAs remain fully aware of the security classifications of all information gathered. SAs must be vigilant in confirming the clearance authorizations of law enforcement officers they may consult regarding their NSI. This awareness of the classifications of information contained in the investigation will determine the format of any potential interview to further the NSI. Attempts should be made to recreate, in an unclassified format, any classified information discovered. (See Section 7.17.)

7.6 Collaboration with Federal, State, and Local Government, Police Agencies, and Task Force Officers

SAs should consult with appropriate federal, state, and local government and police agencies, in addition to the FBI, and review their reports for any information they maintain on a subject. SAs assigned to a JTTF should reach out to other Task Force Officers (TFOs) to determine if they have investigative insights to support an NSI. SAs should review reports from the FBI and other federal, state, and local government and law enforcement organizations for possible leads to witnesses or evidence to support allegations of ICE violations.

7.7 Identifying Potential Immigration Violations in National Security Investigations

SAs should carefully examine all available information to ascertain whether the subject is amenable to ICE action on civil or administrative grounds. If the alien is amenable to proceeding on other grounds, SAs should continue the investigation on that basis. (b)(7)(E)

(b)(7)(E)

7.8 Managing Foreign Government-Related Information in Furtherance of a National Security Investigation

When SAs require interaction with an outside law enforcement agency and/or a foreign government as part of an NSI, they should obtain the concurrence of their HSI supervisor and JTTF supervisor before such interaction takes place. In accordance with established procedures, SAs should also contact the appropriate HSI Attaché on any necessary foreign collateral investigation.

(b)(7)(E)

(b)(7)(E)

7.10 Engaging the U.S. Attorney's Office and the Local Office of the Chief Counsel in National Security Investigations

SAs are to consult with the USAO and the "national security" designated attorney in their local OCC early in the investigation and facilitate communications between the national-security designated OCC and Assistant U.S. Attorneys prior to the approval of charging documents and prosecution memorandums. In investigations of violations of the import and export laws relating to sensitive information or technology, SAs should consult with the local HSI embedded attorney.

7.11 Considerations When Interviewing and Taking Statements on Information Related to National Security Investigations

To determine the necessity of interviewing individuals who could have information pertinent to the NSI, SAs should consult with all government agencies that are parties to the investigation prior to conducting any interviews. (b)(5); (b)(7)(E)

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

7.12 Considerations on National Security Investigations Regarding Individuals Who Are Nonimmigrants

(b)(7)(E)

(b)(7)(E)

7.13 Other Investigative Activity in Furtherance of a National Security Investigation

(b)(7)(E)

7.14 JTTF Cooperative Target Designation Protocol

Pursuant to the JTTF cooperative target designation protocol, investigations may target individuals who may be subject to removal proceedings on security-related grounds and who are:

A. Naturalized citizens who have or had an occupational status which, if they had been aliens, would have entitled them to nonimmigrant status under INA sections 101(a)(15)(A) or (15)(G) (regarding Diplomatic Personnel).

B. Aliens who have been admitted for permanent residence, if such aliens had at the time of entry or subsequently acquired an occupational status which would, if they were seeking admission to the United States, entitle them to nonimmigrant status under INA sections 101(a)(15)(A) or (15)(G) and if they executed and filed with the AG a written waiver of all rights, privileges, exceptions, and immunities under any law or Executive Order, pursuant to section 247(b) of the INA.

C. Aliens who previously had a status under INA sections 101(a)(15)(A) or (15)(G).

Before conducting an investigation in such a case, SAs should contact the DOS Office of Protocol to ascertain whether the alien, in fact, has diplomatic status or if such status has been terminated. SAs should indicate in the request that enforcement action is being contemplated and request DOS' input on such action. All such charges and investigations require prior approval from the Deputy Assistant Director, NSID, and OPLA NSLS.

7.15 Immigration or Document Fraud Schemes and National Security Investigations

(b)(7)(E)

7.16 Headquarters-Led Antiterrorism and National Disruptive Efforts

HSI at HQ may disseminate benefit fraud cases with a significant national security nexus and/or concern that do not fall under the formal JTTF process as there may not be a definite identified link to terrorism. These cases may be in support of national level disruptive efforts or fall under other national anti-terrorism efforts. (b)(7)(E)

(b)(7)(E)

7.17 Classified Information in National Security Investigations

The predicating information to support a national security related investigation is often classified. Although this classified information may be important to the initiation of a case, in most circumstances, it will not be allowed to serve as the basis of criminal or administrative proceedings. For this reason, it is essential that SAs brief the respective USAO, as well as National Security-designated attorneys in their local OCC and OPLA NSLS on the substance of the classified information that has predicated the potential criminal and administrative aspects of the case (b)(5); (b)(7)(E)

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

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

7.18 Investigative Tools to Consider in National Security Investigations

One of the most important tools available to the U.S. Government in supporting NSIs and combating terrorist activities is the authority to pursue the removal of individuals engaged in the support or facilitation of terrorism.

Pen registers and Title III intercepts further a criminal investigation by establishing evidence of criminal activity and identifying relationships between known targets and larger networks of the criminal organization. While resource-intensive, a Title III investigation can produce significant enforcement results when all other investigative means have either failed or will otherwise not provide the evidentiary value to further the investigation. A complete list of criminal violations for which a Title III intercept may be authorized can be found in 18 U.S.C. § 2516.

HSI JTTF SAs also conduct investigations to obtain evidence to support judicial proceedings under section 340 of the INA. These investigations focus on the revocation of U.S. citizenship previously granted to members of terrorist groups or the denial of citizenship to such aliens under section 313(a). Additionally, HSI JTTF SAs develop evidence to deny applications for relief (e.g., obtaining lawful permanent residence in the United States under section 245 of the INA) when investigations reveal evidence of membership in or support of terrorist groups.

SAs conducting NSIs should be thoroughly familiar with the relevant provisions of the INA. The availability and accuracy of sound intelligence reporting is crucial to the

successful completion of these types of investigations. HSI is the repository for a majority of terrorist-related information maintained by ICE.

In addition, a National Security Investigative Development Worksheet (see Appendix A) may assist SAs in conducting a logical and thorough investigative effort in furtherance of NSIs.

Chapter 8. DEPARTMENT OF STATE COUNTERTERRORISM OFFICE

As provided in section 219 of the INA, DOS has compiled the complete list of designated terrorist organizations, including other names by which these organizations are known. According to the DOS Office of Counterterrorism, the following information applies to those organizations listed that have been designated FTOs (http://www.state.gov/s/ct/list/). (See Appendix B.)

8.1 Identification and Designation of Foreign Terrorist Organizations

(b)(7)(E)

8.2 Department of State Procedures for Designating a Group as a Foreign Terrorist Organization

Once a target is identified, S/CT prepares a detailed administrative record (b)(7)(E) (b)(7)(E) demonstrating that the statutory criteria for designation has been satisfied. If the Secretary of State, in consultation with the AG and the Secretary of the Treasury, decides to make the designation, Congress is notified of the Secretary of State's intent to designate the organization and given 7 days to review the designation, as required by the INA. Upon expiration of the 7-day waiting period and in the absence of Congressional action to block the designation, notice of the designation is published in the Federal Register, at which point the designation takes effect. By law, an organization designated as an FTO may seek judicial review of the designation in the U.S. Court of Appeals for the District of Columbia Circuit no later than 30 days after the designation is published in the Federal Register.

Before the passage of the IRTPA of 2004, the INA stated that FTOs must be re-designated by DOS every 2 years. Absent this re-designation, the original designation would automatically lapse. Under the IRTPA of 2004, the re-designation requirement was replaced by enhanced review and revocation procedures. IRTPA states that an FTO may file a petition for revocation 2 years after its original (or most recent) designation or 2

years after the determination date on its most recent petition for revocation. The petitioning FTO must provide sufficient evidence to convince DOS that the evidence that supported the initial designation is no longer valid.

If no FTO designation review has been conducted during a 5-year period, the Secretary of State is required to certify that the designation is still warranted. In addition, the Secretary of State may rescind a designation at any time upon a finding that the evidence supporting the initial designation has changed in such a manner as to warrant revocation. The same procedural requirements that apply to designations apply to revocations made by the Secretary of State. A designation may be revoked by an Act of Congress or set aside by a court order.

8.3 Legal Criteria for Designation as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act, as Amended

The following criteria apply to DOS applications for the designation of an FTO:

A. It must be a *foreign organization;* and

B. The organization must *engage in terrorist activity*, as defined in section 212 (a)(3)(B) of the INA (8 U.S.C. § 1182(a)(3)(B)), or in *terrorism*, as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (22 U.S.C. § 2656f(d)(2)), *or retain the capability and intent to engage in terrorist activity or terrorism;* and

C. The organization's terrorist activity must threaten the security of U.S. nationals *or* the national security (national defense, foreign relations, and/or the economic interests) of the United States.

8.4 Legal Ramifications of Designation as a Foreign Terrorist Organization

It is unlawful for a person in the United States (or subject to the jurisdiction of the United States) to knowingly provide material support or resources to a designated FTO. (The term "material support or resources" is defined in 18 U.S.C. § 2339A(b)(1) as any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safe houses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (one or more individuals who may be or may include oneself), and transportation, except medicine or religious materials. 18 U.S.C. § 2339A(b)(2) provides that, for these purposes, "the term 'training' means instruction or teaching designed to impart a specific skill, as opposed to general knowledge." 18 U.S.C. § 2339A(b)(3) further provides that, for these purposes, "the term 'expert advice or assistance' means advice or assistance derived from scientific, technical, or other specialized knowledge."

Representatives and members of a designated FTO, if they are aliens, are inadmissible to and, in certain circumstances, removable from the United States. (See 8 U.S.C. §§ 1182 (a)(3)(B)(i)(IV)-(V) and 1227(a)(1)(A).)

Any U.S. financial institution that becomes aware that it has possession of, or control over, funds in which a designated FTO or its agent has an interest must retain the funds and report the funds to the Department of the Treasury's OFAC.

SAs should contact the "national security" designated attorney in their local OCC with any questions as to whether the particular conduct of an individual constitutes "material support."

8.5 Other Effects of Designation as a Foreign Terrorist Organization

The designation of an organization as an FTO often positively affects the United States' proactive efforts to curb terrorism financing by yielding the below-listed desired results, while also encouraging other nations to do likewise. The designation of an organization as an FTO:

A. Stigmatizes and isolates the designated terrorist organization internationally.

B. Deters donations or contributions to, and economic transactions with, the named organization.

C. Heightens public awareness and knowledge of the terrorist organization.

D. Signals to other governments U.S. concerns about the designated organization.

8.6 Terrorist Exclusion List

Section 411 of the USA PATRIOT Act of 2001 (8 U.S.C. § 1182) authorized the Secretary of State, in consultation with or upon the request of the AG, to designate terrorist organizations for immigration purposes. This authority is known as the "Terrorist Exclusion List" (TEL) (see Appendix C). TEL designation bolsters homeland security efforts by facilitating the ability to exclude aliens associated with TEL entities from entering the United States.

8.7 Terrorist Exclusion List Designation Criteria

An organization can be placed on the TEL if the Secretary of State finds that the organization:

A. Commits or incites a terrorist activity under circumstances indicating an intention to cause death or serious bodily injury.

B. Prepares or plans a terrorist activity.

C. Gathers information on potential targets for terrorist activity.

D. Provides material support for the commission of terrorist activity to an individual who has committed or plans to commit terrorist activity or to a terrorist organization.

E. Soliciting funds for a terrorist activity or a terrorist organization.

F. Soliciting individuals to engage in terrorist activity or for membership in a terrorist organization.

Under the statute, terrorist activity is defined as any activity that is unlawful under U.S. law or the laws of the place where it was committed and involves hijacking or sabotage of an aircraft, vessel, vehicle, or other conveyance; hostage taking; a violent attack on an internationally protected person; assassination; or the use of any biological agent, chemical agent, nuclear weapon or device, or explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain) with the intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property. The definition also captures any threat, attempt, or conspiracy to perform any of these activities.

8.8 Terrorist Exclusion List Designation Process

The Secretary of State is authorized to designate groups as TEL organizations in consultation with or upon the request of the AG. Once an organization of concern is identified, or a request is received from the AG to designate a particular organization, DOS works closely with DOJ and the IC to prepare a detailed administrative record, which is a compilation of information, typically including both classified and open source information, demonstrating that the statutory criteria for designation has been satisfied. Once completed, the administrative record is sent to the Secretary of State who decides on designating the organization. Notices of designations are published in the Federal Regulation.

8.9 Effects of Designation for Those on the Terrorist Exclusion List

A designation on the TEL produces both legal and consequential ramifications.

A. Legal Ramifications for Those on the Terrorist Exclusion List

Individual aliens providing support to, or associated with, TEL-designated organizations may be found inadmissible to the United States, i.e., such aliens may be prevented from entering the United States or, if already in U.S. territory, may be deported in certain circumstances. Examples of activity that

may render an alien inadmissible as a result of an organization's TEL designation include:

1) Membership in a TEL-designated organization.

2) Use of the alien's position of prominence within any country to persuade others to support an organization on the TEL.

3) Solicitation of funds or other items of value for an organization on the TEL.

4) Solicitation of any individual for membership in an organization on the TEL.

5) Commission of an act that the alien knows, or should have reasonably known, provides material support to an organization on the TEL. Such material support may include the provision of a safe house, transportation, communications, funds, transfer of funds, or other material to obtain financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training.

(Note: Individual aliens may be determined inadmissible on the basis of other types of terrorist activity unrelated to TEL-designated organizations. (See 8 U.S.C. § 1182(a)(3)(B).))

B. Other Effects for Those on the Terrorism Exclusion List

TEL-designation also:

1) Deters donation or contributions to the named organizations.

2) Heightens public awareness and knowledge of the terrorist organizations.

3) Alerts other governments to U.S. concerns about organizations engaged in terrorist activities.

4) Stigmatizes and isolates the designated terrorist organizations.

Chapter 9. IMMIGRATION AND NATIONALITY ACT

9.1 Evidence to Be Considered for Security-Related Administrative Removal Grounds

SAs must look for admissible evidence which will establish a *prima facie* case for removal pursuant to INA sections 212(a)(3) or 237(a)(4). In order to collect the proper evidence, it is important to understand exactly what actions make an individual subject to removal on security related grounds.

According to INA sections 212(a)(3)(A) or 237(a)(4)(A), any alien who has engaged, is engaged, or at any time after admission engages in the following activities is deportable:

A. any activity to violate any law of the United States relating to espionage or sabotage or to violate or evade any law prohibiting the export from the United States of goods, technology, or sensitive information;

B. any other unlawful activity, such as criminal activity which endangers public safety or national security; or

C. any activity whose purpose is the opposition to, or the control or overthrow of, the Government of the United States by force, violence, or other unlawful means.

According to INA sections 212(a)(3)(B) or 237(a)(4)(B), any alien is inadmissible and/or removable if he or she:

A. has engaged in a terrorist activity,

B. is a member of a terrorist organization;

C. has received military-type training from a terrorist organization.

See INA 212(a)(3)(B)(i) for a complete list, the term "terrorist activity" means any activity that is unlawful under the laws of the place where it is committed (or which, if committed in the United States, would be unlawful under the laws of the United States or any of its States) and that involves any of those acts described in section 212(a)(3)(B)(iii) of the INA.

The term "engage in terrorist activity" means to commit, in an individual capacity or as a member of an organization, an act of terrorist activity or an act that the actor knows, or reasonably should know, affords material support to any individual, organization, or government in conducting a terrorist activity at any time, including any of those activities described in section 212(a)(3)(B)(iv) of the INA.

The term "representative" includes an officer, official, or spokesman of an organization, and any person who directs, counsels, commands, or induces an organization or its members to engage in terrorist activity.

(b)(7)(E)

Finally, an alien whose entry or proposed activities in the United States the Secretary of State has reasonable ground to believe would have potentially serious adverse foreign policy consequences for the United States is inadmissible. INA § 212(a)(3)(C)(i); see also INA § 237(a)(4)(C). There are statutory exceptions to this provision, which are included in section 212(a)(3)(C)(ii) and (iii) of the INA.

SAs should make every effort to obtain all available evidence on the issues of the subject's amenability to immigration proceedings or eligibility for discretionary relief.

9.2 Classified National Security Information/Evidence in Administrative Adjudicative Proceedings

SAC offices are reminded that the use of classified national security information in administrative adjudicative proceedings, whether by an ICE officer or an immigration judge, must be approved in advance. Approval for the use of such evidence is limited to the Secretary of Homeland Security, in consultation with the AG or his or her designee. Additionally, if the classified information is derived from the Foreign Intelligence Surveillance Act (FISA), the AG must also approve the use of such evidence.

In any case where the use of national security information is proposed, HSI offices must submit the materials proposed for use directly to NSU via secure means. Upon receipt, NSU and OPLA NSLS will review the materials. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

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

Three provisions of the INA specifically permit the use of classified information in immigration proceedings: (1) section 240 of the INA provides for the use of classified information in removal proceedings under certain circumstances; (2) section 235 of the INA provides for the use of classified evidence in expedited removal proceedings; and (3) section 501, *et seq.,* of the INA provide for the use of classified information in proceedings before the Alien Terrorist Removal Court (ATRC). (b)(5); (b)(7)(E)

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

First, classified information may only be used *ex parte* in standard immigration proceedings, under INA section 240, to oppose applications for admission to the United States, or for discretionary relief. (b)(5); (b)(7)(E)

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

Second, under INA section 235(c), while DHS may consider classified evidence in removal proceedings, (b)(5); (b)(7)(E)

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

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

Due to the fact that utilizing each provision presents challenges, SAs should contact their National Security-designated OPLA attorney for further guidance.

9.3 The Effect of the Real ID Act of 2005 on the Immigration and Nationality Act (INA) Relating to INA Definitions

In addition to establishing national standards for driver's licenses, funding border security projects, changing some visa limits, and introducing rules governing delivery bonds for non-detained aliens in proceedings, the Real ID Act provides enhancements regarding the deportation of aliens for terrorist activity.

9.4 Section 212(a)(3)(B)(iii) of the Immigration and Nationality Act, Terrorist Activities

The INA defines "terrorist activity" as any activity which is unlawful under the laws of the place where it is committed (or which, if committed in the United States, would be unlawful under the laws of the United States or any of its States) and which involves any of the following:

A. The hijacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle);

B. The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a government organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained;

C. A violent attack upon an internationally protected person (as defined in 18 U.S.C. § 1116(b)(4)) or upon the liberty of such a person;

D. An assassination; and/or

E. The use of any:

1) Biological agent, chemical agent, or nuclear weapon or device;

2) Explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with the intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property; and/or

F. A threat, attempt, or conspiracy to do any of the foregoing.

9.5 Definition of a Terrorist Organization in the Immigration and Nationality Act

Understanding the manner in which the INA defines a "terrorist organization" is critical to prosecuting national security cases; it is also key to understanding what the term "engaging in terrorist activity" means. INA § 212(a)(3)(B)(vi) lists three types of groups that qualify as terrorist organizations under the INA. Two groups involve Secretary of State designations discussed in Chapter 8 (sections 212(a)(3)(B)(vi)(I) and (II) of the INA). The definition of the third type of group, commonly referred to as undesignated or "Tier III" organizations, applies either to a terrorist organization that has not been officially designated as such, or to an organization that engaged in terrorist activities prior to the group's official designation as a terrorist organization, but only for the time period in which it participated in terrorist activities prior to the designation.

Section 212(a)(3)(B)(vi)(III) of the INA defines a terrorist organization as a group of two or more individuals, whether organized or not, that engages in, or has a subgroup which engages in, the terrorist activities described in subclauses (I) through (VI) of § 212(a)(3)(B)(iv) of the INA. Notably, unlike the first two definitions of "terrorist organization" in the INA, section 212(a)(3)(B)(vi)(III) does not include a list of terrorist organizations that meet the definition. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Chapter 10. FOREIGN INTELLIGENCE SURVEILLANCE ACT AND THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

This Chapter provides a brief overview of FISA for SAs conducting NSIs who encounter information that is unusual in general criminal or administrative investigations.

Signed into law in 1978, FISA, 50 U.S.C. §§ 1801-1862, authorizes law enforcement surveillance and searches in the United States of persons or entities suspected of being foreign powers or agents of foreign powers. FISA's primary purpose is to assist the Executive Branch in gathering foreign intelligence. Although intelligence operations often result in the discovery of evidence of crimes, this must be a secondary objective: FISA requires that "a significant purpose of the surveillance is to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B). FISA specifically states that its terms apply only when the subject of the surveillance is residing in the United States.

10.1 Relevant Definitions

FISA defines the terms "Foreign Power" and "Agent of a Foreign Power" broadly. A "Foreign Power" means 1) a foreign government, whether recognized by the United States or not; 2) a faction of a foreign nation or nations, not substantially composed of U.S. persons; 3) an entity directed and controlled by a foreign government or governments; 4) a group engaged in international terrorist activities; and 5) foreign-based political organizations, not substantially composed of U.S. persons. 50 U.S.C. § 1801(a).

An "Agent of a Foreign Power" includes both U.S. persons and non-U.S. persons. Definitions of foreign agents limited to non-U.S. persons include 1) officers and employees of a foreign power; 2) individuals who engage in clandestine intelligence activities contrary to U.S. interest; 3) individuals who engage in international terrorist activities; and 4) members of international terrorist organizations. 50 U.S.C. § 1801(b)(1).

The definition of an agent of a foreign power also includes any person (including U.S. citizens) who 1) knowingly engages in clandestine intelligence on behalf of a foreign power; 2) knowingly engages in international terrorist activities; 3) knowingly aids, abets, or conspires with others in such activities; and 4) knowingly enters the United States or otherwise uses a false or fraudulent identity for or on behalf of a foreign power. 50 U.S.C. § 1801(b)(2).

Under the statute, a "U.S. person" refers to a U.S. citizen or an alien lawfully admitted for permanent residence as defined in INA § 101(a)(20) (LPR or conditional resident alien).

Foreign intelligence information (FII) under FISA consists of information that relates to the ability of the United States to protect itself against actual or potential attacks, terrorism, sabotage, or clandestine intelligence activities by a foreign power or agent of a foreign power; or information with respect to a foreign power or foreign territory that relates to the national defense of the United States or the conduct of its foreign affairs.

10.2 United States Foreign Intelligence Surveillance Court

FISA authorized the creation of the U.S. Foreign Intelligence Surveillance Court (FISC), a federal court comprised of eleven district court judges from seven of the U.S. judicial circuits, to adjudicate applications for surveillance and physical searches against suspected foreign intelligence entities and agents inside the United States by federal law enforcement agencies, primarily the FBI. 50 U.S.C. §§ 1803, 1822(c).

10.3 Foreign Intelligence Surveillance Act Applications

FISA applications and orders are classified, and intelligence developed under FISA is also classified, generally at the Secret level. The Office of Intelligence, a component of the DOJ National Security Division, prepares and presents applications for FISA surveillance to the FISC. Applications are heard by a single judge.

(b)(7)(E)

10.4 Minimization Procedures

FISA intends that law enforcement agencies conducting surveillance intercept only material relating to the target and to the FII or crime with the least intrusion possible. To support this intent, FISA requires that each warrant application include a minimization procedure if the surveillance involves a U.S. person. 50 U.S.C. § 1805(a)(4), 50 U.S.C. § 1806. Minimization procedures are mechanisms reasonably designed to minimize the

acquisition and retention of information obtained on unconsenting U.S. persons. 50 U.S.C. § 1801(h)(1). The procedures must also minimize the dissemination of any information that identifies the individual. 50 U.S.C. § 1801(h)(2). FISA allows for the retention and dissemination of information that is evidence of a crime and is being retained or disseminated for law enforcement purposes. 50 U.S.C. § 1801(h)(3).

10.5 Uses of Foreign Intelligence Information

Sections 1806(a) and 1825(a) of FISA mandate that information collected under a FISA warrant with regard to a U.S. person may be used and disclosed without the consent of the U.S. person only in accordance with the minimization procedures included in the FISA order. Information obtained under FISA may not be used for unlawful purposes. No otherwise privileged information obtained by surveillance shall lose its privileged character. 50 U.S.C. § 1806(a).

No information acquired under FISA may be disclosed for law enforcement purposes unless it is accompanied by a statement that the information acquired and any information derived from such information may be used only in a criminal proceeding with the advance authorization of the AG. 50 U.S.C. § 1806(b).

10.6 FISA Authority vs. Court-Overseen Criminal Investigatory Surveillance Techniques

FISA authority differs significantly from criminal investigatory techniques under Title III. 18 U.S.C. § 2510. Under FISA, the U.S. Government does not have to show probable cause that a crime has been committed. However, successful applications require a showing of probable cause that the target of the application is a foreign power or agent of a foreign power and that each of the facilities targeted for electronic surveillance is being used or is about to be used by a foreign power or agent of a foreign power. In the case of searches, the applications must establish probable cause to believe that the premises or property to be searched is owned, used, possessed, or in transit to or from a foreign power or agent.

The U.S. Government does not need to show traditional probable cause for a U.S. person engaged in clandestine intelligence activities or espionage. However, "Congress allowed this lesser showing for clandestine intelligence activities, but not, notably, for other activities, including terrorism, because it was fully aware that such foreign intelligence crimes may be particularly difficult to detect." In *re* Sealed Case, 310 F.3d 717, at 738-39 (2002). (b)(7)(E)

(b)(7)(E)

10.7 FISA, Counterintelligence, and Law Enforcement

Before September 11, 2001, DOJ restricted access to intelligence and counterintelligence developed by the FBI. Criminal law enforcement, including counterterrorism enforcement, could not access such information. FISA applications required that the "primary purpose" of the surveillance was to obtain FII and not evidence for criminal prosecution. The USA PATRIOT Act amended FISA to allow applications where obtaining foreign intelligence was a "significant purpose" and explicitly granted consultation between DOJ criminal and intelligence employees. These amendments resulted in procedures allowing criminal enforcement officers and prosecutors to review counterintelligence information obtained through FISA. However, the information obtained through FISA remains classified and cannot be used in court without authorization from the AG.

10.8 Considerations of FISA Implications for U.S. Persons and Non-U.S. Persons

FISA treats U.S. persons and non-U.S. persons differently for the purposes of obtaining an order authorizing surveillance or search. The statute defines a U.S. person as a U.S. citizen or an LPR. 50 U.S.C. § 1801(i). Where the statutory "Agent of a Foreign Power" is a U.S. person, a successful application requires, by a showing of probable cause, that a nexus exists between the target and actual or potential FII, including espionage, international terrorism, sabotage, and certain identity fraud, as well as aiding, abetting, or conspiring in these offenses.

In applications targeting U.S. persons, the FISC reviews all submissions of statements and certifications for clear error. 50 U.S.C. 1804(a)(2)(B)(4). This requirement, however, does not apply to non-U.S. persons. Moreover, as discussed above, FISA designed the required minimization procedures to limit exposure of non-public information involving U.S. persons and to protect their privacy.

Notably, FISA prohibits the targeting of U.S. persons for surveillance, searches, or other investigations authorized by the statute, if the officer bases the investigation solely on account of the proposed target's First Amendment activities. 50 U.S.C. § 1805(a)(3)(A), 1842(a)(1), 1961(a)(1).

10.9 FISA Usage in Domestic Terrorist or Racketeering Enterprise Investigations

Due to FISA's limited scope to investigate foreign intelligence activity, targets of FISA applications must be foreign powers or foreign agents. Thus, absent any evidence that it meets the definition of a "Foreign Power" or an "Agent of a Foreign Power," a domestic terrorist organization or racketeering enterprise cannot be targeted using FISA.

10.10 Emergency FISA Applications

In cases of emergency, the AG may authorize surveillance or search without initial approval of FISC, subject to the requirements outlined in 50 U.S.C. § 1805(f). Notably,

emergency applications must meet the same requirements as those applications submitted to FISC, including minimization procedures. The applicant must submit a full written application to FISC within 72 hours. Surveillance must terminate when the information sought is obtained, the application is denied, or the 72-hour period is over. If the application is denied, no information or evidence derived from the investigation can be used in any legal proceeding unless the information indicates a threat of death or serious bodily harm to any person.

10.11 FISA Application in "Lone Wolf" Situations

FISA allows for the targeting of individuals not affiliated with any known international terrorist organization or foreign power. FISA extends the definition of "Agent of a Foreign Power" to include any non-U.S. person who "engages in international terrorism or activities in preparation therefor." FISA does not require that the individual be affiliated with any terrorist organization. 50 U.S.C. § 1801(b)(1)(C).

Chapter 11. BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC DEVICES

11.1 Background

At the border (or its functional equivalent), HSI has a broad authority to conduct searches of persons and goods upon their entry into or exit out of the United States without first obtaining a warrant and without suspicion. This authority stems from long-standing and well-recognized exceptions to the Fourth Amendment's warrant and probable cause requirements that are premised on the Government's interest in protecting its citizens from the entry of persons and items harmful to U.S. interests. Repeatedly, the Supreme Court has recognized that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." (See United States v. Ramsey, 431 U.S. 606, 616 (1977).)

HSI does not distinguish between the search of merchandise contained in electronic devices and merchandise contained in any other form that crosses U.S. borders. With respect to the border search of electronic devices, federal courts, including the U.S. Court of Appeals for the Ninth Circuit, have concluded that searching documents, including those in electronic form, is well within the broad border search exception exercised by HSI and have generally endorsed the view that laptop computers or other electronic devices are neither conceptually nor constitutionally different from other closed containers subject to suspicionless searches at the border. The exercise of this plenary authority has been critical to ensuring national security at U.S. borders.

11.2 Authorities

ICE Directive 7-6.0, Border Searches of Documents and Electronic Media, dated July 16, 2008, and ICE Directive 10044.1 (former number: 7-6.1), Border Searches of Electronic Devices, dated August 18, 2009, or as updated, set forth the legal guidelines and establish policy and procedures regarding border searches of documents and electronic devices. (Note: ICE Directive 7-6.0 was superseded by ICE Directive 10044.1 (former number: 7-6.1) only as it relates to electronic devices.). pursuant to Customs border search authorities, contained in Title 19 of the United States Code, HSI may conduct stops and searches of merchandise and persons at the U.S. border without any individualized suspicion. Additionally, pursuant to immigration authorities found in 8 U.S.C. §§ 1225 and 1357, HSI may inspect all aliens who apply for admission; take and consider evidence concerning the privilege of any person to enter, pass through, or reside in the United States that is material or relevant to the enforcement of immigration laws; and conduct a search without a warrant of any person and the personal effects in his or her possession when there is reasonable cause to suspect a basis for denying admission to the United States.

11.3 Border Searches by HSI Special Agents

Border searches must be conducted by HSI SAs or other properly designated Customs Officers, such as law enforcement officers cross-designated by ICE as customs officers (e.g., TFOs), and persons whose assistance to ICE is demanded under 19 U.S.C. § 507. During a border search, SAs may detain documents and electronic devices, or copies thereof, for further review, either on-site or at an off-site location, including an associated

(b)(7)(E)

(b)(7)(E)

Any demand for assistance made on an outside agency must be in compliance with existing Memorandums of Understanding (MOUs), Memorandums of Agreement (MOAs) or similar mechanism between ICE and the other agency, as well as meeting the parameters outlined in ICE Directive 7-6.0, Border Searches of Documents and Electronic Media, dated July 16, 2008, or as updated, and ICE Directive 10044.1 (former number: 7-6.1), Border Searches of Electronic Devices, dated August 18, 2009, or as updated.

(Note: ICE Directive 7-6.0 was superseded by ICE Directive 10044.1 (former number: 7-6.1) only as it relates to electronic devices.)

11.4 Chain of Custody

(b)(7)(E)

(b)(7)(E)

All detentions must be handled in accordance with ICE Directive 7-6.0, Border Searches of Documents and Electronic Media, dated July 16, 2008, or as updated, ICE Directive 10044.1 (former

number: 7-6.1), Border Searches of Electronic Devices, dated August 18, 2009, or as updated, and OI memorandum, "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media," dated December 12, 2008, or as updated. Whenever an HSI SA seizes documents or electronic devices, the seizing SA must enter the seizure into the Seized Asset and Case Tracking System (SEACATS) via the completion of an Incident Report.

(b)(7)(E)

11.5 Demands for Assistance

During a border search, SAs may encounter information in documents and electronic devices that requires the assistance of another federal agency or a non-federal entity in order to perform their duties. Assistance is typically required for issues related to foreign language translation, decryption, and other technical issues. SAs may demand this type of assistance in any case and without individualized suspicion.

SAs may also encounter information that is not in a foreign language or that has no decryption or technical issues, but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws administered and enforced by HSI. SAs may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by HSI.

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

(b)(5); (b)(7)(E) (See OI Memorandum, "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry," dated March 5, 2007, or as updated.) SAs are encouraged to contact the TAS Section Chief for additional guidance.

11.6 Information Sharing

HSI SAs acting under border search authority may share information relating to national security with law enforcement and intelligence agencies consistent with the guidelines and applicable laws set forth in ICE Directive 7-6.0, Border Searches of Documents and Electronic Media, dated July 16, 2008, or as updated, and ICE Directive 10044.1 (former number: 7-6.1), Border Searches of Electronic Devices, dated August 18, 2009, or as updated. It is important to note that border searches may not be conducted on behalf of a third-agency and any electronic media obtained through ICE border search authority must

be searched by an HSI SA or another properly authorized officer who meets the definition of "customs officer" under 19 U.S.C. § 1401(i). HSI SAs are encouraged to consult their respective local HSI embedded attorney for more detailed information regarding when and how information sharing with law enforcement and intelligence authorities is appropriate.

Chapter 12. JOINT TERRORISM TASK FORCE PARTICIPATION

12.1 JTTF Background

The first JTTF was established in 1980 in the FBI New York field office. There are 103 JTTFs throughout the United States (as of the date of issuance of this Handbook). The mission of the JTTFs is to utilize the collective resources of the participating agencies in the prevention, preemption, deterrence, and investigation of terrorism and illicit activities related to terrorism, which include both actual and potential terrorist acts against the United States or its interests in foreign countries. The mission also entails apprehending individuals who commit or threaten to commit such violations. The FBI maintains operational oversight of the JTTFs; however, the groups, organizations, and/or individuals to be investigated are specifically identified and agreed upon by the JTTF participating agencies, in accordance with the AG Guidelines.

HSI is partnered with the FBI JTTFs nationwide to ensure that HSI's authorities are leveraged to most effectively accomplish the national security mission that safeguards the security of the United States. HSI SAs substantially contribute to the JTTFs by enforcing the authorities entrusted to ICE that span a diverse set of investigative areas relating to immigration, money laundering, smuggling and trafficking, trade violations, cyber security, etc. HSI remains committed to the JTTF concept, evidenced by the fact that HSI is the largest federal contributor of personnel to JTTFs. At HQ, HSI maintains SAs assigned to various Divisions, Sections, and Units within FBI's CTD.

The FBI CTD National JTTF defined the criteria for full-time, part-time, and liaison JTTF membership (see Appendix D). HSI SAs contribute a wide range of support to the JTTFs such as investigative and legal expertise and knowledge of relevant criminal and administrative violations that are in direct support of the objectives of PDD 39 (see Section 4.5(A) and PDD 62 (see Section 4.5(B)). ICE HSI plays a pronounced and critical role in U.S. counterterrorism efforts to further the war on terrorism, and continues to provide unique investigative value that is widely recognized by law enforcement and the IC.

HSI dedicates full-time and part-time SAs to the JTTFs to utilize their unique criminal and administrative authorities and resources in the investigation of national security threats. Whenever feasible, HSI SAs should be designated as "case agents" or "co-case agents" on JTTF investigations where ICE authorities will most likely be utilized against an individual or individuals to disrupt or dismantle a terrorist organization or national security threat.

SAs assigned to the JTTFs may be tasked to lead or assist in investigations based on information generated from the FBI or may open a JTTF investigation based on information predicated by ICE. It is critical that HSI SAs lead JTTF investigations where ICE's unique and vast statutory authorities are viewed as the most likely legal avenue to disrupting a terrorist attack or dismantling a terrorist organization.

12.2 JTTF Commitment

SACs are encouraged to coordinate with the FBI to ensure that HSI continues to lead investigations where HSI's unique immigration and customs authorities can successfully mitigate a terrorist threat.

SAC offices are required to receive concurrence from the NSU Unit Chief prior to reducing ICE JTTF staffing levels from the current reported staffing. Additionally, prior to an SA rotation, SACs shall plan accordingly to obtain the proper security clearance for newly-assigned SAs prior to rotating out SAs currently assigned to the JTTF.

Pursuant to ICE memorandum (Policy #10068.1), "DHS Guidance Regarding Polygraph Examinations of ICE Officers Assigned to the FBI Joint Terrorism Task Forces," dated January 22, 2007, or as updated, SAs are not required to and will not undergo FBI counterintelligence psychophysiological detection of deception examinations as a condition of assignment to a JTTF.

12.3 JTTF Reduction in Staffing Requests

If a SAC office comes to the conclusion that a reduction in JTTF staffing is appropriate, the SAC will submit a memorandum to the NSU Unit Chief, justifying the proposed staffing reduction. No reduction in JTTF staffing will occur until the SAC receives approval from the EAD of HSI.

12.4 JTTF Investigations Predicated on ICE Information

If SAs develop information, either through a lead or during the normal course of an investigation where a demonstrative nexus to terrorism exists, they should refer the investigation to the JTTF. This does not mean that HSI relinquishes or otherwise minimizes its role, nor does it preclude HSI from initiating an NSI under the auspices of other NSID-approved National Security initiatives (e.g., Operation Allegiance or investigations developed as a result of HSI's liaison activities with the IC).

12.5 JTTF Investigations Predicated on FBI Information or Investigations in Which ICE Violations Are Predicate Offenses

HSI SAs will routinely partner with the FBI or other task force partners on investigations either in the role of case agents or co-case agents. Regardless of how the lead that predicated the investigation was developed, SACs should be particularly concerned with

ensuring that HSI investigative equities are represented and that HSI assumes the lead on any investigation in which ICE violations are the predication for the investigation.

12.6 MOUs and MOAs Pertaining to ICE's Participation in the JTTF

ICE utilizes the "Memorandum of Understanding between the U.S. Customs Service and the Federal Bureau of Investigation," dated January 6, 2000, and the "Memorandum of Understanding between the Immigration and Naturalization Service and the Federal Bureau of Investigation," dated June 18, 1999, to govern ICE's participation in the JTTF.

The following MOAs are also relevant to ICE's JTTF participation:

A. "Memorandum of Agreement between the Department of Homeland Security and the Federal Bureau of Investigation Regarding the Handling of Administrative Cases Involving Aliens of National Security Interest," dated June 7, 2007, or as updated; and

B. "Memorandum of Agreement between the Department of Justice and the Department of Homeland Security Concerning Terrorist Financing Investigations," dated May 13, 2003, or as updated.

12.7 National Security Letters

A "National Security Letter" (NSL) generally refers to any written direction to provide personal, privacy, or financial information which may be issued directly to third parties by the FBI or, where appropriate, another authorized investigative, intelligence, or counterintelligence agency, without judicial authorization or notice to the subject to which the requested records pertain. Recipients of NSLs may include telephone companies, financial institutions, Internet Service Providers, or consumer credit agencies.

In most cases, the authority to issue NSLs belongs exclusively to the FBI. Under some circumstances, however, DHS investigative personnel, such as those serving on the JTTFs, may be authorized to utilize NSLs. Only HSI SAs serving on the JTTFs may request that the FBI issue an NSL in accordance with established FBI guidelines governing the use of NSLs with respect to JTTF investigations. This clarification on the use of NSLs by HSI SAs will have no impact on HSI's traditional use of administrative subpoenas, summonses, or pen registers.

12.8 FBI National Security Requests for Alien File Review

FBI National Security related requests for physical review of an A-File will be routed through a designated HSI representative, preferably an HSI SA assigned to the local JTTF.

(b)(7)(E)

(b)(7)(E) Immigration status checks that

do not require a physical file review will continue to be vetted locally, or through the Law Enforcement Support Center via the National Law Enforcement Telecommunication System. SAC offices will enforce third-agency disclosure requirements when a physical review of alien files is requested from the FBI.

12.9 SAC Assignment of JTTF Representatives for National Security-Related Alien File Review

Every SAC will designate a point of contact (POC) for his or her entire AOR, or multiple POCs, as needed, for Deputy SAC, Assistant SAC, and Resident Agent in Charge offices.

Appendix A

NATIONAL SECURITY INVESTIGATIVE DEVELOPMENT WORKSHEET

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Appendix B

DESIGNATED FOREIGN TERRORIST ORGANIZATIONS

1. Abdallah Azzam Brigades (AAB)
2. Abu Nidal Organization (ANO)
3. Abu Sayyaf Group (ASG)
4. Al-Aqsa Martyrs Brigade (AAMS)
5. Al-Shabaab
6. Ansar al-Islam (AAI)
7. Army of Islam (AOI)
8. Asbat al-Ansar
9. Aum Shinrikyo (AUM)
10. Basque Fatherland and Liberty (ETA)
11. Communist Party of the Philippines/New People's Army (CPP/NPA)
12. Continuity Irish Republican Army (CIRA)
13. Gama'a al-Islamiyya (Islamic Group)
14. Haqqani Network (HQN)
15. HAMAS (Islamic Resistance Movement)
16. Harakat ul-Jihad-i-Islami/Bangladesh (HUJI-B)
17. Harakat ul-Mujahidin (HUM)
18. Hizballah (Party of God)
19. Indian Mujahedeen (IM)
20. Islamic Jihad Union (IJU)

21. Islamic Movement of Uzbekistan (IMU)

22. Jaish-e-Mohammed (JEM) (Army of Mohammed)

23. Jemaah Anshorut Tauhid (JAT)

24. Jemaah Islamiya organization (JI)

25. Jundallah

26. Kahane Chai (Kach)

27. Kata'ib Hizballah (KH)

28. Kongra-Gel (KGK, formerly Kurdistan Workers' Party, PKK, KADEK)

29. Lashkar-e Tayyiba (LT) (Army of the Righteous)

30. Lashkar i Jhangvi (LJ)

31. Liberation Tigers of Tamil Eelam (LTTE)

32. Libyan Islamic Fighting Group (LIFG)

33. Moroccan Islamic Combatant Group (GICM)

34. National Liberation Army (ELN)

35. Palestine Liberation Front (PLF)

36. Palestinian Islamic Jihad (PIJ)

37. Popular Front for the Liberation of Palestine (PFLF)

38. PFLP-General Command (PFLP-GC)

39. al-Qaida in Iraq (AQI)

40. al-Qa'ida (AQ)

41. al-Qa'ida in the Arabian Peninsula (AQAP)

42. al-Qaida in the Islamic Maghreb (formerly GSPC)

43. Real IRA (RIRA)

44. Revolutionary Armed Forces of Colombia (FARC)

45. Revolutionary Organization 17 November

46. Revolutionary People's Liberation Party/Front (DHKP/C)

47. Revolutionary Struggle (RS)

48. Shining Path (Sendero Luminoso (SL))

49. United Self-Defense Forces of Colombia (AUC)

50. Harakat-ul Jihad Islami (HUJI)

51. Tehrik-e Taliban Pakistan (TTP)

Appendix C

TERRORIST EXCLUSION LIST

1. Afghan Support Committee (a.k.a. Ahya ul Turas; a.k.a. Jamiat Ayat-ur-Rhas al Islamia; a.k.a. Jamiat Ihya ul Turath al Islamia; a.k.a. Lajnat el Masa Eidatul Afghania)

2. Al Taqwa Trade, Property and Industry Company Ltd. (f.k.a. Al Taqwa Trade, Property and Industry; f.k.a. Al Taqwa Trade, Property and Industry Establishment; f.k.a. Himmat Establishment; a.k.a. Waldenberg, AG)

3. Al-Hamati Sweets Bakeries

4. Al-Ittihad al-Islami (AIAI)

5. Al-Manar

6. Al-Ma'unah

7. Al-Nur Honey Center

8. Al-Rashid Trust

9. Al-Shifa Honey Press for Industry and Commerce

10. Al-Wafa al-Igatha al-Islamia (a.k.a. Wafa Humanitarian Organization; a.k.a. Al Wafa; a.k.a. Al Wafa Organization)

11. Alex Boncayao Brigade (ABB)

12. Anarchist Faction for Overthrow

13. Army for the Liberation of Rwanda (ALIR) (a.k.a. Interahamwe, Former Armed Forces (EX-FAR))

14. Asbat al-Ansar

15. Babbar Khalsa International

16. Bank Al Taqwa Ltd. (a.k.a. Al Taqwa Bank; a.k.a. Bank Al Taqwa)

17. Black Star

18. Continuity Irish Republican Army (CIRA) (a.k.a. Continuity Army Council)

19. Darkazanli Company

20. Dhamat Houmet Daawa Salafia (a.k.a. Group Protectors of Salafist Preaching; a.k.a. Houmat Ed Daawa Es Salifiya; a.k.a. Katibat El Ahoual; a.k.a. Protectors of the Salafist Predication; a.k.a. El-Ahoual Battalion; a.k.a. Katibat El Ahouel; a.k.a. Houmate Ed-Daawa Es-Salafia; a.k.a. the Horror Squadron; a.k.a. Djamaat Houmat Eddawa Essalafia; a.k.a. Djamaatt Houmat Ed Daawa Es Salafiya; a.k.a. Salafist Call Protectors; a.k.a. Djamaat Houmat Ed Daawa Es Salafiya; a.k.a. Houmate el Da'awaa es-Salafiyya; a.k.a. Protectors of the Salafist Call; a.k.a. Houmat ed-Daaoua es-Salafia; a.k.a. Group of Supporters of the Salafiste Trend; a.k.a. Group of Supporters of the Salafist Trend)

21. Eastern Turkistan Islamic Movement (a.k.a. Eastern Turkistan Islamic Party; a.k.a. ETIM; a.k.a. ETIP)

22. First of October Antifascist Resistance Group (GRAPO) (a.k.a. Grupo de Resistencia Anti-Fascista Premero De Octubre)

23. Harakat ul Jihad i Islami (HUJI)

24. International Sikh Youth Federation

25. Islamic Army of Aden

26. Islamic Renewal and Reform Organization

27. Jamiat al-Ta'awun al-Islamiyya

28. Jamiat ul-Mujahideen (JUM)

29. Japanese Red Army (JRA)

30. Jaysh-e-Mohammed

31. Jayshullah

32. Jerusalem Warriors

33. Lashkar-e-Tayyiba (LET) (a.k.a. Army of the Righteous)

34. Libyan Islamic Fighting Group

35. Loyalist Volunteer Force (LVF)

36. Makhtab al-Khidmat

37. Moroccan Islamic Combatant Group (a.k.a. GICM; a.k.a. Groupe Islamique Combattant Marocain)

38. Nada Management Organization (f.k.a. Al Taqwa Management Organization SA)

39. New People's Army (NPA)

40. Orange Volunteers (OV)

41. People Against Gangsterism and Drugs (PAGAD)

42. Red Brigades-Combatant Communist Party (BR-PCC)

43. Red Hand Defenders (RHD)

44. Revival of Islamic Heritage Society (Pakistan and Afghanistan offices -- Kuwait office not designated) (a.k.a. Jamia Ihya ul Turath; a.k.a. Jamiat Ihia Al- Turath Al-Islamiya; a.k.a. Revival of Islamic Society Heritage on the African Continent)

45. Revolutionary Proletarian Nucleus

46. Revolutionary United Front (RUF)

47. Salafist Group for Call and Combat (GSPC)

48. The Allied Democratic Forces (ADF)

49. The Islamic International Brigade (a.k.a. International Battalion, a.k.a. Islamic Peacekeeping International Brigade, a.k.a. Peacekeeping Battalion, a.k.a. The International Brigade, a.k.a. The Islamic Peacekeeping Army, a.k.a. The Islamic Peacekeeping Brigade)

50. The Lord's Resistance Army (LRA)

51. The Pentagon Gang

52. The Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs (a.k.a. Riyadus-Salikhin Reconnaissance and Sabotage Battalion, a.k.a. Riyadh-as-Saliheen, a.k.a. the Sabotage and Military Surveillance Group of the Riyadh al-Salihin Martyrs, a.k.a. Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Shahids (Martyrs))

53. The Special Purpose Islamic Regiment (a.k.a. the Islamic Special Purpose Regiment, a.k.a. the al-Jihad-Fisi-Sabililah Special Islamic Regiment, a.k.a. Islamic Regiment of Special Meaning)

54. Tunisian Combat Group (a.k.a. GCT, a.k.a. Groupe Combattant Tunisien, a.k.a. Jama'a Combattante Tunisien, a.k.a. JCT; a.k.a. Tunisian Combatant Group)

55. Turkish Hizballah

56. Ulster Defense Association (a.k.a. Ulster Freedom Fighters)

57. Ummah Tameer E-Nau (UTN) (a.k.a. Foundation for Construction; a.k.a. Nation Building; a.k.a. Reconstruction Foundation; a.k.a. Reconstruction of the Islamic Community; a.k.a. Reconstruction of the Muslim Ummah; a.k.a. Ummah Tameer I-Nau; a.k.a. Ummah Tameer E-Nau; a.k.a. Ummah Tameer-I-Pau)

58. Youssef M. Nada & Co. Gesellschaft M.B.H.

Appendix A

NATIONAL SECURITY INVESTIGATIVE DEVELOPMENT WORKSHEET

(b)(7)(E)

Appendix D

NATIONAL JOINT TERRORISM TASK FORCE MEMBERSHIP DESIGNATION CRITERIA

A. **Full-Time:** (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

B. **Part-Time:** (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Appendix E

ACRONYMS

ACS	Automated Case Support
AG	Attorney General
AOR	Area of Responsibility
ATRC	Alien Terrorist Removal Court
CBP	U.S. Customs and Border Protection
CFA	Computer Forensics Agent or Computer Forensics Analyst
CFR	Code of Federal Regulations
CIA	Central Intelligence Agency
CIKR	Critical Infrastructure and Key Resources
CIS	Central Index System
CTCEU	Counterterrorism/Criminal Exploitation Unit
CTD	Counterterrorism Division
CTS	Counterterrorism Section
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOJ	Department of Justice
DOS	Department of State
EID	Enforcement Integrated Database
ENFORCE	Enforcement Case Tracking System
FBI	Federal Bureau of Investigation
FII	Foreign Intelligence Information
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FR	Federal Register
FTO	Foreign Terrorist Organization
FTOX	Foreign Terrorist Organization X
GWOT	Global War on Terrorism
HSI	Homeland Security Investigations
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
INA	Immigration and Nationality Act
INS	Immigration and Naturalization Service
IRTPA	Intelligence Reform and Terrorism Prevention Act
JTTF	Joint Terrorism Task Force
JVU	Joint Vetting Unit
JWICS	Joint Worldwide Intelligence Communications System
KST	Known or Suspected Terrorist
PR	Lawful Permanent Resident
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding

NCTC	National Counterterrorism Center
NSA	National Security Agency
NSEERS	National Security Entry/Exit Registration System
NSI	National Security Investigation
NSIC	National Security Integration Center
NSID	National Security Investigations Division
NSL	National Security Letter
NSLS	National Security Law Section
NSTTF	National Security Threat Task Force
NSU	National Security Unit
NTC	National Targeting Center
OCC	Office of the Chief Counsel
OFAC	Office of Foreign Asset Controls
OI	Office of Investigations
OIG	Office of the Inspector General
OPLA	Office of the Principal Legal Advisor
PDD	Presidential Decision Directive
POC	Point of Contact
POE	Port of Entry
SA	Special Agent
SAC	Special Agent in Charge
SAFM	Special Agent Field Manual
S/CT	Office of the Coordinator for Counterterrorism
SDGT	Specifically Designated Global Terrorists
SEACATS	Seized Asset and Case Tracking System
SEN	Significant Event Notification
SEVIS	Student and Exchange Visitor Information System
SEVP	Student and Exchange Visitor Program
SIPRNet	Secret Internet Protocol Router System
TAS	Threat Analysis Section
TEL	Terrorism Exclusion List
TFO	Task Force Officer
TIDE	Terrorist Identities Datamart Environment
TS	Top Secret
TSA	Transportation Security Administration
TSC	Terrorism Screening Center
TSDB	Terrorist Screening Database
USAO	U.S. Attorney's Office
USC	U.S. Code
USCIS	U.S. Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
VRVK	Visa Revocation