

# COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS HANDBOOK

## Table of Contents

<b>Chapter 1. PURPOSE AND SCOPE</b> .....	<b>1</b>
<b>Chapter 2. INTRODUCTION</b> .....	<b>1</b>
<b>Chapter 3. DEFINITIONS</b> .....	<b>2</b>
• 3.1 Alien Change of Address Request Database .....	2
• 3.2 Alien Flight Student Program .....	2
• 3.3 Alternate Responsible Officer.....	2
• 3.4 Analytical Framework for Intelligence .....	2
• 3.5 Arrival Departure Information System .....	2
• 3.6 Automated Biometric Identification System .....	3
• 3.7 Automated Targeting System-Passenger .....	3
• 3.8 Central Index System.....	3
• 3.9 Computer Linked Automated Information Management System.....	3
• 3.10 Consular Consolidated Database .....	3
• 3.11 Deportable Alien Control System (Historical) .....	4
• 3.12 Designated School Official .....	4
• 3.13 DHS Pattern Information and Collaboration Sharing System .....	4
• 3.14 Enforcement Case Tracking System (Historical) .....	4
• 3.15 Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement .....	5
• 3.16 ENFORCE Alien Removal Module.....	5
• 3.17 Enforcement Integrated Database .....	5
• 3.18 Fingerprint Identification Number .....	5
• 3.19 I-94 Subject Query in TECS .....	6
• 3.20 Intelligence Fusion Center (Historical).....	6
• 3.21 LeadTrac Database.....	6
• 3.22 National Security Entry-Exit Registration System .....	6
• 3.23 Office of Biometric Identity Management.....	6
• 3.24 Person Centric Query Service .....	6
• 3.25 Principal Designated School Official.....	7
• 3.26 Refugee, Asylum and Parole System.....	7
• 3.27 Responsible Officer .....	7
• 3.28 Secondary Inspection Tool .....	7
• 3.29 Significant Event Notification .....	7
• 3.30 Significant Incident Reports .....	7
• 3.31 Student and Exchange Visitor Information System.....	7

- 3.32 Student and Exchange Visitor Program .....8
- 3.33 TECS.....8
- 3.34 Web-Based Commercial Databases .....8

**Chapter 4. AUTHORITIES/REFERENCES .....8**

- 4.1 Authorities.....8
- 4.2 References.....14

**Chapter 5. RESPONSIBILITIES .....15**

- 5.1 Executive Associate Director, Homeland Security Investigations ...15
- 5.2 Deputy Assistant Director, National Security Program Division .....15
- 5.3 Unit Chief, Counterterrorism and Criminal Exploitation Unit .....16
- 5.4 Special Agents in Charge and Attachés .....16
- 5.5 Special Agents, Intelligence Research Specialists, and  
Investigative Assistants.....16

**Chapter 6. CTCEU PROGRAMS AND RELATED RESOURCES .....16**

- 6.1 Student and Exchange Visitor Information System.....16
- 6.2 Overstay Data Sources and Biometric Services.....20
- 6.3 Automated Biometric Identification System .....22
- 6.4 International Criminal Police Organization .....22
- 6.5 Visa Revocation Program .....24
- 6.6 International Military Student Absent Without Leave Program.....25
- 6.7 Lost and Stolen Passport Program .....25
- 6.8 Alien Flight Student Program .....25
- 6.9 Visa Waiver Enforcement Program .....26
- 6.10 Targeted Enforcement Program.....27
- 6.11 DHS National Security Overstay Initiative.....27
- 6.12 SEVIS Recurrent Student Vetting Program.....27
- 6.13 Project Campus Sentinel .....27
- 6.14 National Security Entry-Exit Registration System .....28
- 6.15 Compliance Enforcement Advisory Panel.....29
- 6.16 (b)(7)(E) .....30
- 6.17 FBI Counterterrorism Division .....30
- 6.18 Foreign Terrorist Tracking Task Force.....30
- 6.19 National Counterterrorism Center.....30
- 6.20 (b)(7)(E) .....30
- 6.21 NCTC Pursuit Group .....31
- 6.22 Open Source Team.....31

**Chapter 7. COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS.....31**

- 7.1 Violator Identification.....31
- 7.2 Database Analysis .....32
- 7.3 School and Program Leads .....33
- 7.4 LeadTrac Database.....34
- 7.5 Investigative Lead Referral.....34
- 7.6 TECS Case Categories.....34
- 7.6.1 TECS Primary Program Codes .....35
- 7.6.2 TECS Secondary Program Codes .....35
- 7.7 Collateral Request Assignment.....36
- 7.8 Timely Assignment and Reporting Requirement .....36
- 7.9 Database Review.....36
- 7.10 Field Investigation and Interview .....37
- 7.11 Criminal and Administrative Charges .....39
- 7.12 Database Reporting/Management Notification.....40

**Appendix**

- Appendix A Acronyms..... A-i

## **Chapter 3. DEFINITIONS**

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

### **3.1 Alien Change of Address Request Database**

The Alien Change of Address Request (Form AR-11) database is available (b)(7)(E)  or the U.S. Citizenship and Immigration Service's (USCIS) Person Centric Query Service (PCQS), and contains change of address information filed by aliens via Form AR-11.

### **3.2 Alien Flight Student Program**

The Alien Flight Student Program (AFSP) is the Transportation Security Administration (TSA) program utilized to vet and approve aliens for flight training. Section 113 of the U.S. Air Transportation Security Act amended Title 49, United States Code (U.S.C.) by adding a new section: Section 44939 (the authority granted by Section 113 of the Act is codified as 49 U.S.C. § 44939). Section 44939 establishes a waiting period for individuals or aliens who have requested training to operate certain aircraft while the Secretary of Homeland Security determines if that individual or alien poses a risk to aviation or national security.

### **3.3 Alternate Responsible Officer**

The Alternate Responsible Officer (ARO) is the official designated by the exchange visitor program to assist the Responsible Officer (RO) in performing responsibilities and duties pertaining to the Student and Exchange Visitor Information System (SEVIS). AROs input data into SEVIS and issue Forms DS-2019, "Certificates of Eligibility for Exchange Visitor (J-1) Status," to exchange visitors.

### **3.4 Analytical Framework for Intelligence**

ICE has partnered with U.S. Customs and Border Protection (CBP) to replace the capabilities of the Intelligence Fusion System (IFS) with the Analytical Framework for Intelligence (AFI). AFI increases analytic collaboration, cooperation, and efficiencies through enhanced and integrated information sharing. AFI enables users to conduct federated searches across numerous DHS systems and includes a full suite of tools designed to enhance all-source intelligence capability with data consolidation and research, analysis, collaboration, and reporting and production management. This single sign-on system is available to all SAs, IRSs, and IAs.

### **3.5 Arrival Departure Information System**

The Arrival Departure Information System (ADIS) is responsible for tracking the arrival and departure of non-U.S. citizen travelers. It receives messages from several external sources, such as CBP's TECS, the Automated Biometrics Identification System

(IDENT), SEVIS, the Computer-Linked Application Information Management System (CLAIMS), and the Electronic Immigration System.

In addition to providing users access to the data via web pages, ADIS sends arrival and departure information on students and exchange visitors to SEVIS. ADIS also generates many of the overstay leads that CTCEU vets and investigates. The Consolidated Appropriations Act signed into law by President Obama on Friday, January 17, 2014, transferred ADIS from the National Protection and Program Directorate Office of Biometric Identity Management (OBIM) to the CBP Office of Field Operations.

### **3.6 Automated Biometric Identification System**

IDENT is the DHS biometric database. It collects biometric, biographic, and encounter-related data. 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.

### **3.7 Automated Targeting System-Passenger**

Automated Targeting System-Passenger (ATS-P) is a CBP database capable of conducting a “superquery,” or a federated search for passengers, of multiple source systems containing travel, immigration, and law enforcement information.

### **3.8 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 contains information on the status of an alien, as well as the physical location of the individual’s Alien File (A-file).

### **3.9 Computer Linked Automated Information Management System**

CLAIMS contains information on aliens who have filed applications for immigration benefits with USCIS. It supports the processing and maintenance of applications and petitions for immigration benefits by providing an information systems infrastructure.

### **3.10 Consular Consolidated Database**

The Consular Consolidated Database (CCD) is a Department of State (DOS), Bureau of Consular Affairs, database that contains information on all immigrant and nonimmigrant visa applications submitted to U.S. consular offices and contains information on U.S. passport information.

### **3.11 Deportable Alien Control System (Historical)**

The Deportable Alien Control System (DACCS) was a legacy U.S. Immigration and Naturalization Service mainframe system that contained information regarding the status of illegal aliens under removal proceedings, including detention status and location. DACCS also contained information regarding the alien's entry and departure status until the alien was deported or relief was granted. (Note: The Enforcement Case Tracking System (ENFORCE) Alien Removal Module (EARM) replaced DACCS in August 2008.)

### **3.12 Designated School Official**

The Designated School Official (DSO) is the official designated by an academic institution to assist the Principal Designated School Official (PDSO) in performing responsibilities and duties pertaining to SEVIS. DSOs and PDSOs input all data in SEVIS and issue ICE Forms I-20 to foreign students. (Note: There are two I-20 forms: 1) ICE Form I-20 A-B entitled, "Certificate of Eligibility for Nonimmigrant (F-1) Student Status – For Academic and Language Students, and 2) ICE Form I-20 M-N entitled, "Certificate of Eligibility for Nonimmigrant (M-1) Student Status – For Vocational Students.") DSOs currently do not undergo formal background checks and are not vetted by the U.S. Government.

### **3.13 DHS Pattern Information and Collaboration Sharing System**

The DHS Pattern Information and Collaboration Sharing System (DPICS<sup>2</sup>) is a DHS search tool that allows DHS law enforcement users to conduct federated queries in data sets derived from multiple DHS law enforcement databases (TECS, SEVIS, the National Security Entry/Exit Registration System (NSEERS), ENFORCE, ADIS, the ICE Law Enforcement Support Center, and I-94 (Arrival-Departure Record)). It also allows users to conduct queries in law enforcement databases provided by other federal, state, and local law enforcement information sharing collaborations, including the Federal Bureau of Investigation (FBI) National Data Exchange system (FBI N-DEx), which may provide police record information ranging from traffic citations and booking information to departmental reports. Users receive hit information in the form of subject biographic information and photos or mug shots, if available. They also receive identifying record information from the source systems. DPICS<sup>2</sup> offers a visual linking tool and global relationship function that allow users to view information pertaining to subjects who are associated in the DHS source systems to the primary search subject.

### **3.14 Enforcement Case Tracking System (Historical)**

ENFORCE was an event-based case management system that documented, tracked, and managed the reporting of enforcement cases pertaining to immigration violations. Its functions included subject processing, biometric identification, allegations and charges, preparation and printing of appropriate forms, data repository, and interface with the national database of enforcement events. ENFORCE supported alien apprehension

processing for both “Voluntary Return” and “Notice to Appear” actions. ENFORCE also contained the NSEERS module through which all NSEERS registrations were performed.

ENFORCE was replaced by the Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement (EAGLE) as the principal user interface with the Enforcement Integrated Database (EID) in April 2013. SAs are now required to enter information on all administrative and criminal arrests into EAGLE.

### **3.15 Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement**

EAGLE is the primary HSI database for booking, searching, and entering a subject’s biometric information into EID, IDENT, and the Advanced Fingerprint Identification Technology (AFIT). It is a mobile-capable application used to conduct fingerprint and biographic searches and submit booking information to EID. EAGLE has three Biometric Search transactions (IDENT, the FBI’s Integrated Automated Fingerprint Identification System (IAFIS), and the Department of Defense (DOD)’s Automated Biometric Identification System and two Booking and Enrollment transactions. It uses existing service connections to OBIM’s IDENT, DOJ’s Joint Automated Booking System, the FBI Criminal Justice Information Services’ AFIT, the National Crime Information Center (NCIC), and DOD’s Automated Identification System to update biometrically verified information in near real-time. This information is available to all approved users internal and external to DHS and to other LEAs.

### **3.16 ENFORCE Alien Removal Module**

EARM is a web-based application that supports case management activities for Enforcement and Removal Operations (ERO). EARM is integrated with other enforcement applications through the use of EID which makes it possible to collect, track, manage, and store data in a secure centralized location. EARM is ICE’s replacement for DACS and is the official system of record for removal operations.

### **3.17 Enforcement Integrated Database**

EID is the data warehouse of information entered into ENFORCE and is the DHS common database repository for enforcement applications.

### **3.18 Fingerprint Identification Number**

The Fingerprint Identification Number (FIN) is the primary unique subject fingerprint reference used by DHS. FINs are generated by OBIM’s IDENT.

### **3.19 I-94 Subject Query in TECS**

The I-94 Subject Query (SQ 94) in TECS provides the user with the ability to query for information regarding the entry of a nonimmigrant and includes information on visa classification, intended address, and departure.

### **3.20 Intelligence Fusion System (Historical)**

IFS, formerly named the Advanced Visual Abstracted Links and Name Collection Handler Engine (AVALANCHE), was a database developed by the ICE Office of Intelligence that enables users to perform key word and biographic searches of numerous DHS systems simultaneously. IFS has been replaced by AFI.

### **3.21 LeadTrac Database**

LeadTrac is a stand-alone compliance enforcement database utilized almost exclusively by CTCEU to store, track, and manage information about potential nonimmigrant status violators. LeadTrac's primary purpose is to allow IRSs, contract analysts, and SAs to vet individuals for immigration violations, send collateral cases to HSI field offices for investigation, and track these cases through to their conclusion.

### **3.22 National Security Entry-Exit Registration System**

NSEERS provided detailed information about certain nonimmigrants, including background, additional identifying information, purpose of the nonimmigrant's visit to the United States, and departure confirmation. (Note: Although DHS removed the list of countries whose nationals were required to register in NSEERS and suspended all special registration and reporting requirements through a notice published in the Federal Register on April 28, 2011, the program is still viable and can be reactivated at any time.)

### **3.23 Office of Biometric Identity Management**

OBIM was created in March 2013, replacing the United States Visitor and Immigration Status Indicator Technology (US-VISIT) and streamlining operations. OBIM supports DHS's responsibility to protect the nation by providing biometric identification services that help federal, state, and local government decision-makers accurately identify the people they encounter and determine whether these people pose a risk to the United States. The primary mission of OBIM is to match, store, and share biometric data. OBIM also provides biographic services via ADIS that support missions that rely on entry/exit and overstay data.

### **3.24 Person Centric Query Service**

PCQS is a federated query tool owned by USCIS, which collects data from several source systems, including, but not limited to, CIS, CLAIMS, SEVIS, and CCD.



### **3.25 Principal Designated School Official**

The PDSO is the principal SEVIS point of contact (POC) for ICE at academic institutions, as well as the official designated by the academic institution to perform the responsibilities and duties pertaining to SEVIS.

### **3.26 Refugee, Asylum and Parole System**

The Refugee, Asylum and Parole System (RAPS) is a database maintained by USCIS that contains information pertaining to asylum applicants and related casework. RAPS contains updates regarding application status and progress.

### **3.27 Responsible Officer**

The RO is the primary SEVIS POC for ICE and DOS for exchange visitor programs, as well as the official designated by the exchange visitor program to perform the responsibilities and duties pertaining to SEVIS. Though responsible for maintaining exchange visitors' records, ROs are often not physically located where the exchange visitors are participating in their program.

### **3.28 Secondary Inspection Tool**

The Secondary Inspection Tool (SIT) is a web-based tool that functions within a suite of integrated applications. SIT relies on external data, such as IDENT, and other applications to help comprehensively identify a subject's identity, corroborate the subject's identity, and assess the risk that the subject's presence in the United States may pose. While SIT does not gather biographical and biometric data, it is the conduit for the use of that information to help confirm a subject's identity.

### **3.29 Significant Event Notification**

The Significant Event Notification (SEN) system is a transactional DHS Intranet application and reporting system designed to facilitate the seamless entry, query, and modification of reports such as the Significant Incident Report (SIR).

### **3.30 Significant Incident Reports**

SIRs are reports submitted through the SEN system and are the vehicle for reporting high-interest incidents, significant events, and other emerging or sensitive matters.

### **3.31 Student and Exchange Visitor Information System**

SEVIS is a web-based system that maintains current information on nonimmigrant students (F and M visas), exchange visitors (J visa), and their dependents (F-2, M-2, and J-2) visas. SEVIS enables schools and program sponsors to transmit mandatory

H. Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended

IRTPA grants explicit authority to DHS to remove an alien whose nonimmigrant visa is revoked by DOS. (See Section 6.5 for additional information.)

I. National Security Act of 1947, as amended

The National Security Act promotes national security by providing for a Secretary of Defense, a National Military Establishment, a Department of the Army, Navy, and Air Force, and the coordination of the activities of the National Military Establishment with other departments and agencies of the government concerned with national security.

J. Privacy Act of 1974, as amended (5 U.S.C. § 552a)

The Privacy Act protects certain federal government records pertaining to individuals.

K. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Section 416

The USA PATRIOT Act of 2001 mandates the full implementation and expansion of SEVIS as set forth in 8 U.S.C. § 1372.

L. Executive Order (EO) 12333

EO 12333 provides for timely and accurate intelligence information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents.

United States Intelligence Activities, 46 FR 59941, December 8, 1981, as amended by EOs 13287 (68 FR 4075, January 23, 2003), 13355 (69 FR 53597, August 27, 2004), and 13470 (73 FR 45325, July 30, 2008).

M. EO 13231

EO 13231 provides for the protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

Critical Infrastructure Protection in the Information Age, 66 FR 53063, October 18, 2001, as amended by EOs 13284 (January 23, 2003); 13286

JJ. 8 C.F.R. § 264.1(f), Registration, fingerprinting, and photographing of certain nonimmigrant aliens

Nonimmigrants may be required to register, submit fingerprints, and be photographed upon arrival to the United States if they are, or are believed to be, citizens or nationals of a designated country, or are believed to meet designated criteria. (Paragraph (f) was revised effective September 11, 2002, through notice in 67 FR 52584.)

KK. 22 C.F.R. § 62, Exchange Visitor Program

22 C.F.R. § 62 sets rules for the administration of the exchange visitor program (J visa holders – oversight for the program falls under DOS).

## 4.2 References

- A. Federal Register Notice where DHS removed the list of countries whose nationals have been subject to NSEERS registration and reporting requirements and suspended all special registration and reporting requirements associated with the NSEERS program, 76 FR 23831, dated April 28, 2011.
- B. Routine use “W” of the Student and Exchange Visitor Information System (SEVIS) System of Record Notice, 75 FR 412, dated January 5, 2010.
- C. Office of the Director of National Intelligence (ODNI) Instruction No. 2006-3, “Protection of Privacy and Civil Liberties,” dated February 22, 2006.
- D. ODNI Instruction No. 80.13, “Protection of Privacy and Civil Liberties,” dated February 27, 2006.
- E. ODNI Instruction 80.02, “Managing Breaches of Personally Identifiable Information,” dated February 20, 2008.
- F. Memorandum of Agreement Between the Attorney General and the Director of National Intelligence on Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center of Terrorism Information Contained within Datasets Identified as Including Non-Terrorism Information and Information Pertaining Exclusively to Domestic Terrorism, dated November 4, 2008.
- G. Memorandum of Understanding between the Secretary of State, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence on the Integration and Use of Screening Information to Protect Against Terrorism, as amended by Addendum B, effective January 2007.

- H. Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies and DHS Concerning Information Sharing, dated March 4, 2003.
- I. DHS memorandum signed by the Deputy Secretary, “Department of Homeland Security Guidance on Treatment of Individuals Previously Subject to the Reporting and Registration Requirements of the National Security Entry Exit Registration System,” dated April 16, 2012.
- J. “DHS Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy,” Privacy and Civil Liberties Guidance Memorandum 2009-01, dated June 5, 2009.
- K. DHS Privacy Policy Guidance Memorandum 2007-01, “Regarding Collection, Use, Retention and Dissemination of Information on Non-U.S. Persons,” dated January 7, 2009.
- L. Memorandum from the Secretary of DHS, “Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies,” dated April 18, 2007.
- M. ICE memorandum, “Minimum Standards on Compliance Enforcement Case Closures,” dated April 18, 2008, or as updated.
- N. HSI Directive 12.02, “Terrorist Identities Datamart Environment” (TIDE), dated October 19, 2012, or as updated.
- O. HSI memorandum, “Operation Clipped Wings,” dated December 7, 2011, or as updated.
- P. SEVIS Exploitation Enforcement Operations Guidebook, dated July 31 2013, or as updated.

## **Chapter 5. RESPONSIBILITIES**

### **5.1 Executive Associate Director, Homeland Security Investigations**

The Executive Associate Director (EAD) of HSI is responsible for the oversight of the policies and procedures set forth in this Handbook.

### **5.2 Deputy Assistant Director, National Security Program Division**

The Deputy Assistant Director, National Security Program Division, is responsible for the overall implementation of the policies and procedures in this Handbook.

### **5.3 Unit Chief, Counterterrorism and Criminal Exploitation Unit**

The CTCEU Unit Chief is responsible for the oversight of all programmatic areas in CTCEU's purview, including, but not limited to, operational, investigative, policy, personnel, budget, and logistical issues associated with those programs.

### **5.4 Special Agents in Charge and Attachés**

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

### **5.5 Special Agents, Investigative Research Specialists, and Investigative Assistants**

SAs, IRSs, and IAs are responsible for complying with the provisions of this Handbook.

## **Chapter 6. CTCEU PROGRAMS AND RELATED RESOURCES**

### **6.1 Student and Exchange Visitor Information System**

SEVIS is the database which provides end users, including HSI, educational institutions, and DOS-approved programs, with detailed information regarding F, M, and J visa holders and their dependents. CTCEU oversees investigations involving the exploitation of SEVIS. CTCEU analyzes SEVIS information and refers vulnerability-related and criminal investigative leads to HSI field offices for further investigation. In addition, CTCEU lends subject matter expertise to other initiatives in which an exploitation of SEVIS is suspected.

(b)(7)(E)

(b)(7)(E)

information is required to verify the nonimmigrant's student status, SAs can contact the DSOs directly. For issues concerning contact with DSOs, SAs should contact a CTCEU Program Manager.

F. Failure to Provide Information

If an institution has failed to provide the information requested within the specified time frame, SAs will contact the institution's PDSO to determine why the request was not addressed. If the failure to respond was due to an oversight by the school, SAs will make a second request and will notify a CTCEU Program Manager via email. The second request may be made orally or informally since the first written request meets the standard set forth in the regulation. If an institution fails to provide the requested information a second time or refuses to comply with the official ICE request, SAs will notify the CTCEU Program Manager for further action.

G. Rejection of PDSO/DSO

SEVP has the authority to certify who has access to SEVIS and may reject the submission of any DSO nominee or withdraw a previous appointment. Should an HSI office suspect that a PDSO/DSO is not eligible to access SEVIS, it should contact CTCEU for guidance on requesting the removal of the PDSO or DSO. (Note: Questions about this process should be directed to CTCEU.)

H. Requests for Data and Other Information

SAs can query SEVIS to obtain invaluable information to further their investigations. CTCEU can also assist SAs by reviewing, analyzing, and compiling SEVIS data. (b)(7)(E)

(b)(7)(E)

Requests for support of special projects or large-scale investigations can be initiated by completing the CTCEU Data Request which can be found (b)(7)(E) (b)(7)(E) The Data Request can be submitted to (b)(7)(E) @hs.gov with the subject line containing (b)(7)(E)

Additional information on how to conduct a SEVIS Exploitation investigation can be found in the “SEVIS Exploitation Enforcement Operations Guidebook,” dated July 31, 2013, or as updated.

I. Exchange Visitor Programs

Exchange visitor (J-1) visas are nonimmigrant visas for individuals approved to participate in exchange visitor programs in the United States. Exchange visitor programs are designated by DOS to oversee exchange visitors and their dependents, which include their spouse and children, via a Certificate of Eligibility for Exchange Visitor Status (DS 2019). Information on J1 and J2 visa holders can be found in SEVIS. The policies that apply to academic institutions and F and M nonimmigrant students in this section also apply to exchange visitors. The equivalent of the PDSO and DSO are the RO and ARO, and the equivalent of the academic institution is the exchange visitor program. The equivalent of ICE Form I-20 is Form DS-2019. More information on the responsibilities of DSOs and ROs and exchange visitor programs can be found in 8 C.F.R. § 214 and 22 C.F.R. § 62.

**6.2. Overstay Data Sources and Biometric Services**

CTCEU receives the majority of its data for potentially actionable leads on nonimmigrant overstays from ADIS and SEVIS. CTCEU works in close collaboration with the Overstay Analysis Unit for nonimmigrant overstay and status violator referrals. CTCEU conducts further law enforcement-specific analysis on the leads before sending them to HSI field offices.

DHS continues to work closely with DOS, building on the biographic and biometric collection underway at U.S. consulates around the world. In cases where a visitor requires a visa, DOS collects the visitor’s biometric and biographic information through the BioVisa program. The BioVisa program is checked against various U.S. Government watch lists, thereby improving the ability of DOS to make a visa determination.

When a visitor arrives in the United States, OBIM procedures allow DHS to determine whether the person applying for entry is the same person who was issued the visa by DOS. Additionally, OBIM’s watch list checks improve the ability of DHS to make admissibility decisions.

(b)(7)(E)

(b)(7)(E)

A. OBIM Biometric Watch List

An integral part of the OBIM process is a fingerprint comparison of foreign visitors’ fingerprints to the fingerprint records of individuals identified via the OBIM Biometric Watch List. Biometric comparisons of a foreign

(b)(7)(E)

All potential fingerprint matches to the various IDENT databases, including the OBIM Biometric Watch List, are referred to the DHS Biometric Support Centers (BSCs) for comparison and matching by certified fingerprint examiners.

(b)(7)(E)

(b)(7)(E)

CTCEU initiates collateral cases on immigration violators with significant derogatory information who are identified via the Biometric Watch List.

#### B. OBIM Biometric Support Center

In cases involving comparisons against IDENT watch list records, BSC fingerprint examiners immediately communicate all findings to the submitter. The OBIM BSCs are staffed by expert fingerprint examiners 365 days per year, 24 hours a day.

(b)(7)(E)

(b)(7)(E)

CTCEU and OBIM are collaborating in utilizing fingerprint data contained in IDENT to identify the fingerprints of unidentified suspects, victims, and witnesses. IDENT contains the fingerprints of millions of foreign nationals encountered by DHS and, during visa issuance, by DOS that are not accessible to state and local LEAs by any other means. The OBIM BSCs have access to millions of biometric and biographic records that are collected and maintained by DHS.



United States. The program's goal is to identify and locate foreign fugitives and career criminals, and to take the appropriate law enforcement action(s), including administrative and/or criminal arrest, removal, or extradition.

The USNCB provides fingerprints related to the INTERPOL Red, Blue, and Green Notices to OBIM, which are then uploaded and/or checked against IDENT. Subsequently, OBIM creates lookout records to provide notification to IDENT users if there is a fingerprint match related to the INTERPOL notices. Confirmed match information is forwarded to CTCEU for further analysis and potential field assignment.

(b)(7)(E)

(b)(7)(E) Explanations of the most common notices encountered by HSI SAs, as provided by INTERPOL, are as follows:

A. Red Notices

Red Notices seek the arrest of subjects for whom an arrest warrant has been issued and where extradition will be requested.

B. Blue Notices

Blue Notices seek information (identity or criminal records) for subjects who have committed a criminal offense, and are used to trace and locate a subject whose extradition may be sought (unidentified offenders or witnesses).

C. Green Notices

Green Notices provide information on career criminals who have committed or are likely to commit offenses in several countries (*e.g.*, habitual offenders, child molesters, or pornographers).

INTERPOL also utilizes other notices. Yellow Notices identify missing persons and parental abductions; Black Notices provide details of unidentified bodies; and Orange Notices are used to warn police and public institutions of potential threats posed by disguised weapons, parcel bombs, and other dangerous objects or materials.

U.S. law does not allow for the arrest of an individual based solely on the existence of a Red Notice from INTERPOL. U.S. law enforcement officers are required to obtain a provisional arrest warrant or develop probable cause for another violation of U.S. law. Provisional arrest warrants are obtained after the country requesting extradition from the United States submits a provisional arrest warrant package to DOJ's Office of International Affairs, and the provisional arrest warrant is issued by the appropriate U.S. court.

(b)(7)(E)

(b)(7)(E)

## 6.5 Visa Revocation Program

DOS is responsible for the issuance and revocation of nonimmigrant visas. DOS regularly revokes nonimmigrant visas for a variety of reasons, including national security concerns. DOS can revoke the visas of subjects who are already in possession of a valid U.S. visa but who no longer meet the criteria for admission to the United States. CTCEU is tasked with leading ICE's investigative efforts of visa revocation cases and has implemented standard operating procedures to ensure the timely and comprehensive investigation of all national security-related revocation cases. In coordination with DOS, the Terrorist Screening Center, the FBI, and CBP, CTCEU ensures that all nonimmigrant aliens in the United States who have had their visas revoked on national security grounds are thoroughly investigated and, if possible, removed from the United States.

It is important to note that the IRTPA of 2004 granted explicit authority to DHS to remove aliens whose nonimmigrant visas are revoked by DOS (see 8 U.S.C. § 1227(a)(1)(B)). DOS has long had the authority to revoke an alien's visa at any time as a matter of discretion pursuant to INA § 221(i). Generally, revocations by DOS are not reviewed by courts under the doctrine of consular non-reviewability. This protection from judicial review gives DOS flexibility to revoke visas on a low threshold of information. While IRTPA § 5304 grants explicit authority to DHS to remove aliens based on a DOS revocation, that revocation is subject to judicial review when a visa revocation is the sole basis for DHS removing an alien.

(b)(7)(E)

(b)(7)(E)

When DOS revokes a visa because of national security concerns, CTCEU is notified and HSI ensures that the proper investigative actions are taken.

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

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

2011, CTCEU assumed responsibility for evaluating the immigration status of foreign flight candidates.

CTCEU developed Operation Clipped Wings on December 7, 2011 as an enforcement operation to combat the vulnerabilities identified in AFSP and the critical infrastructure areas associated with aircrafts. Alien flight training is still a grave reminder of what can happen when the immigration system is exploited – three of the 9/11 hijackers attended flight schools with the incorrect visa status. If CTCEU determines that a nonimmigrant alien flight student is in violation of his or her status or is amenable to removal, it will forward a lead to the appropriate HSI field office for further investigation.

Nonimmigrants who wish to attend flight training that will lead to a Federal Aviation Administration (FAA) certification type or rating must submit a request to TSA. Flight candidates use the TSA AFSP website on the internet and submit their background information and flight training requests. TSA reviews the applications and conducts a terrorist database and criminal history check to determine if the alien is eligible for flight training. Not every flight school is SEVP-certified. TSA monitors approximately 2,500 flight schools of which only approximately 400 are SEVP-certified. Typically, alien flight students will have an F or M visa; however, other nonimmigrant visa categories can take flight training incident to their primary purpose of visit. (b)(7)(E)

(b)(7)(E) (b)(7)(E) SEVP-certified flight schools must follow all SEVIS requirements, including providing requested documentation. HSI (b)(7)(E)

## 6.9 Visa Waiver Enforcement Program

CTCEU developed the Visa Waiver Enforcement Program (VWEP) to address inherent vulnerabilities in the Visa Waiver Program (VWP) by identifying and targeting high-risk overstay and status violators who entered the United States under VWP. VWP enables nationals from VWP countries to travel to the United States for tourism or business with waiver-tourist (WT)/waiver-business (WB) status for up to 90 days without obtaining a nonimmigrant visa. (b)(5); (b)(7)(E)

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

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

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

## 6.10 Targeted Enforcement Program

CTCEU has implemented a Targeted Enforcement Program (TEP) that applies person-centric targeting to overstay leads. This initiative is designed to detect and identify individuals exhibiting specific risk factors based on intelligence reporting, including international travel from specific geographic locations to the United States, and in-depth criminal research and analysis of dynamic social networks. The TEP represents a person-centric approach to nonimmigrant prioritization and targeting efforts, (b)(7)(E)

(b)(7)(E)

(b)(7)(E) Combined with CTCEU's traditional prioritization scheme and the existing TIDE, Biometric Watchlist, and INTERPOL programs, the TEP works to mitigate enduring vulnerabilities within the nation's open immigration system.

## 6.11 DHS National Security Overstay Initiative

CTCEU conducts the DHS National Security Overstay Initiative to identify terrorism threats within the overstay population and to prioritize overstay enforcement actions. The DHS National Security Overstay Initiative was designed to better protect the United States from a national security threat in the overstay population by vetting it in new and innovative ways which help counter the evolution of the terrorist threat. This initiative led to further collaboration between OBIM, CBP, and CTCEU, especially with regards to the processing of overstay leads.

## 6.12 SEVIS Recurrent Student Vetting Program

CTCEU oversees the SEVIS Recurrent Student Vetting Program. (b)(7)(E)

(b)(7)(E)

## 6.13 Project Campus Sentinel

To aid schools in complying with the requirements of SEVIS, CTCEU developed Project Campus Sentinel (PCS), an outreach program designed to open the channels of communication between school officials and staff and local HSI SAs. SAs from local HSI offices meet with and provide training to school officials within their SAC's AOR. HSI SAs can assist schools by alerting officials to patterns of criminal behavior or radicalism. HSI SAs can also provide training in the identification of fraudulent documents to school officials to avoid unintentional violations by the learning institution.

(b)(7)(E)

annually in order to calibrate the priority scheme to effectively mitigate current national security risks.

(b)(7)(E)

**6.17 FBI Counterterrorism Division**

CTCEU maintains a liaison to the FBI Counterterrorism Division (CTD). The liaison’s main responsibility is to establish and/or maintain current coordination between CTD and CTCEU (b)(7)(E)

**6.18 Foreign Terrorist Tracking Task Force**

CTCEU maintains a liaison to the Foreign Terrorist Tracking Task Force (FTTTF) who is responsible for acting as a conduit between CTCEU and FTTTF in order to enhance ICE’s integration within the interagency counterterrorism environment, (b)(7)(E)

(b)(7)(E)

**6.19 National Counterterrorism Center**

In January 2012, CTCEU initiated the use of NCTC resources in support of the Overstay Program to screen overstays in order to identify potential matches to derogatory IC holdings. CTCEU capabilities further enhanced the Overstay Mission by adding a new program designed to screen foreign students who lawfully remain in the United States without scrutiny: the Recurrent Student Vetting Program. Both programs resulted in a new partnership with an Other Government Agency (OGA) to batch SEVIS and/or ADIS records against the terrorism related IC holdings through NCTC. OGA resources utilize very mature entity resolution capabilities to return detailed findings which are manually reviewed.

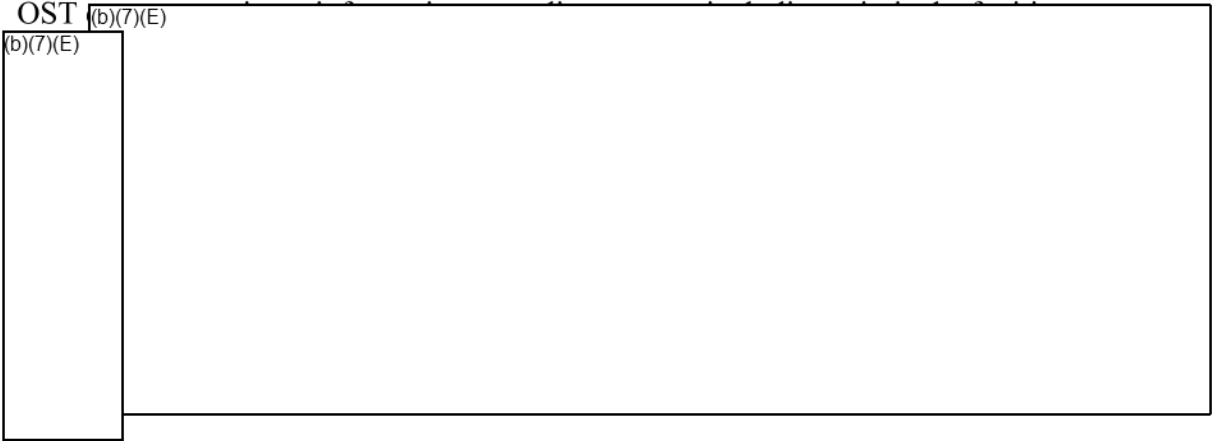
(b)(7)(E)

## 6.21 NCTC Pursuit Group

In support of the CTCEU programs and NCTC, the Pursuit Group, which is part of the Directorate of Intelligence at NCTC, provides information to identify and examine, as early as possible, leads that could become terrorist threats to the Homeland and U.S. interests abroad.

## 6.22 Open Source Team

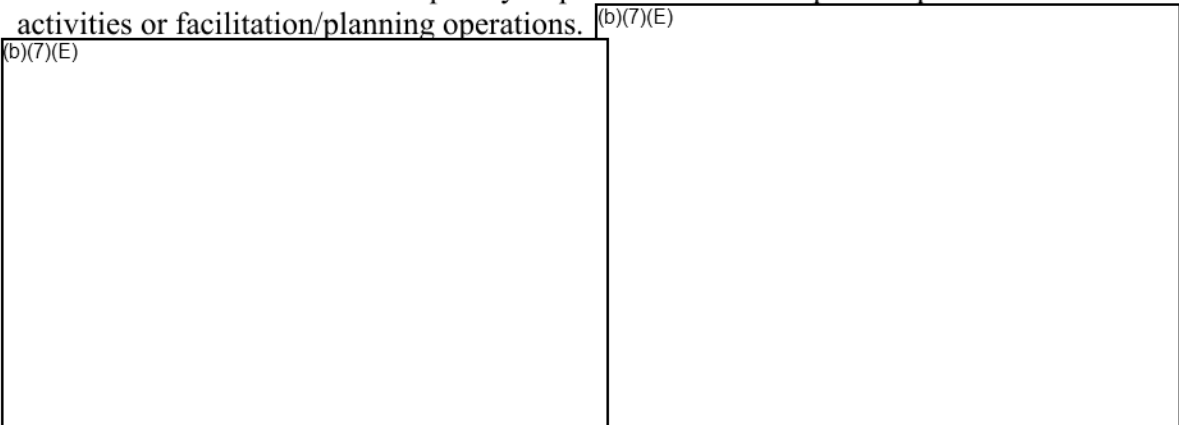
With the proliferation of openly available information through ever-changing internet technologies, CTCEU has created an Open Source Team (OST) to capture and analyze an expanding share of unclassified information available through various open sources. The OST



# Chapter 7. COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS

## 7.1 Violator Identification

CTCEU collaborates with multiple law enforcement partners to identify high priority individuals who are in violation of their U.S. immigration status. CTCEU assists SAs in their investigations, often resulting in criminal or administrative to ultimately remove them from the United States as quickly as possible in order to prevent potential terrorist activities or facilitation/planning operations.



A. System Leads

CTCEU obtains leads on potential status violators (b)(7)(E) from SEVIS and OBIM. OBIM provides information on overstays, while SEVIS provides information on students and exchange visitors who may have violated their immigration status.

B. Specialized Leads

(b)(7)(E)

(b)(7)(E)

**7.2 Database Analysis**

As one of its core functions, CTCEU generates leads on individuals who have violated their nonimmigrant status and refers high priority cases to HSI field offices for investigation. To do this, (b)(7)(E)

(b)(7)(E)

While assessing the viability of a nonimmigrant status violator lead, CTCEU IRSs determine if the nonimmigrant is present in the United States. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

#### 7.4 LeadTrac Database

Information collected relating to nonimmigrant status violators is consolidated, categorized, and entered into LeadTrac, CTCEU's internal database. LeadTrac information is entered, tracked, verified, and managed by CTCEU IRSs and program managers at headquarters (HQ).

#### 7.5 Investigative Lead Referral

CTCEU works closely with the IC to maintain a risk-based matrix which is used to prioritize the hundreds of thousands of potential status violators that CTCEU reviews annually. Furthermore, CTCEU works with partner agencies to identify person-centric targeting metrics. CTCEU IRSs thoroughly vet leads using various systems.

(b)(7)(E)

In addition to its own internal school targeting process, CTCEU receives leads on possible fraudulent schools, programs, and school and program officials from any number of outside sources, including DOS, SEVP, CBP, TSA, USCIS, foreign embassies, HSI field offices, and tips from the public.

(b)(7)(E)

#### 7.6 TECS Case Categories

Investigative activities are divided into various categories based on the types of activities under investigation. This categorization assists in the generation and analysis of data in TECS.

(b)(7)(E)



FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FERPA	Family Educational Rights and Privacy Act
FIN	Fingerprint Identification Number
FOUO	For Official Use Only
FR	Federal Register
FTTTF	Foreign Terrorist Tracking Task Force
HB	Handbook
HQ	Headquarters
HSI	Homeland Security Investigations
IA	Investigative Assistant
IAFIS	Integrated Automated Fingerprint Identification System
IC	Intelligence Community
ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
IFS	Intelligence Fusion System
IIRIRA	Illegal Immigration Reform and Immigration Responsibility Act
IMS	International Military Student
INA	Immigration and Nationality Act
INTERPOL	International Criminal Police Organization
IPR	Intellectual Property Rights
IRS	Intelligence Research Specialist
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
JTTF	Joint Terrorism Task Force
LEA	Law Enforcement Agency
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NSEERS	National Security Entry-Exit Registration System
NLSL	National Security Law Section
NTC	National Targeting Center
OBIM	Office of Biometric Identity Management
OCC	Office of the Chief Counsel
ODNI	Office of the Director of National Intelligence
OGA	Other Government Agency
OI	Office of Investigations
OST	Open Source Team
PCQS	Person Centric Query Service
PCS	Project Campus Sentinel
PDSO	Principal Designated School Official
POC	Point of Contact
POE	Port of Entry
RAPS	Refugee, Asylum and Parole System
RO	Responsible Officer
ROI	Report of Investigation
SA	Special Agent
SAC	Special Agent in Charge

SCB	School Certification Branch
SEACATS	Seized Asset and Case Tracking System
SEN	Significant Event Notification
SEVIS	Student and Exchange Visitor Information System
SEVP	Student and Exchange Visitor Program
SIR	Significant Incident Report
SIT	Secondary Inspection Tool
TEP	Targeted Enforcement Program
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration
TTPG	Terrorist Tracking and Pursuit Group
USAO	U.S. Attorney's Office
U.S.C.	United States Code
USCIS	U.S. Citizenship and Immigration Services
USNCB	U.S. National Central Bureau
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
USA PATRIOT Act	Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
VWEP	Visa Waiver Enforcement Program
VWP	Visa Waiver Program
WB	Waiver Business
WT	Waiver Tourist

- 4.6 Group Supervisors .....6
- 4.7 Special Agents .....7

**Chapter 5. HUMAN SMUGGLING STATUTES AND REFERENCES .....7**

- 5.1 Statutes .....7
- 5.1.1 8 U.S.C. § 1324 – Bringing in and Harboring Certain Aliens .....7
- 5.1.2 8 U.S.C. § 1327 – Aiding or Assisting Certain Aliens to Enter .....8
- 5.1.3 8 U.S.C. § 1328 – Importation of Alien for Immoral Purpose .....8
- 5.2 References. ....8

**Chapter 6. HUMAN SMUGGLING INVESTIGATIVE GUIDANCE.....10**

- 6.1 Accomplishing the Mission.....10
- 6.2 Identifying Human Smuggling Organizational Structures .....11
- 6.3 Developing Targets .....13
- 6.3.1 Resources for Target Development .....13
- 6.3.2 Assistance from U.S. Customs and Border Protection.....14
- 6.3.3 Smuggled Undocumented Aliens .....14
- 6.4 Investigating Human Smuggling.....14
- 6.5 Responding to Human Smuggling Incidents.....15
- 6.5.1 Encountering Unaccompanied Children in Human Smuggling Investigations.....16

**Chapter 7. EXTRATERRITORIAL CRIMINAL TRAVEL STRIKE FORCE AND ILLICIT PATHWAYS ATTACK STRATEGY .....16**

- 7.1 Extraterritorial Criminal Travel Strike Force .....16
- 7.2 Illicit Pathways and Attack Strategy .....18

**Chapter 8. HUMAN TRAFFICKING STATUTES AND REFERENCES .....19**

- 8.1 Statutes .....19
- 8.1.1 18 U.S.C. § 1581 – Peonage; Obstructing Enforcement .....19
- 8.1.2 18 U.S.C. § 1584 – Sale into Involuntary Servitude .....19
- 8.1.3 18 U.S.C. § 1589 – Forced Labor.....19
- 8.1.4 18 U.S.C. § 1590 – Trafficking with Respect to Peonage, Slavery, Involuntary Servitude, or Forced Labor .....19
- 8.1.5 18 U.S.C. § 1591 – Sex Trafficking of Children or by Force, Fraud, or Coercion .....19
- 8.1.6 18 U.S.C. § 1592 – Unlawful Conduct with Respect to Documents in Furtherance of Trafficking, Peonage, Slavery, Involuntary Servitude, or Forced Labor.....20
- 8.1.7 18 U.S.C. § 1593A – Benefiting Financially from Peonage, Slavery, and Trafficking in Persons .....20

- 8.1.8 18 U.S.C. § 1594 – General Provisions.....20
- 8.1.9 Transportation for Illegal Sexual Activity and Related Crimes .....20
- 8.2 Human Trafficking Authorities/References .....20

**Chapter 9. HUMAN TRAFFICKING INVESTIGATIVE GUIDANCE .....21**

- 9.1 Indicators of Human Trafficking.....22
- 9.2 HSI Trafficking in Persons Strategy .....23
- 9.3 Sex Trafficking.....25
- 9.4 Labor Trafficking .....25
- 9.5 Human Smuggling v. Human Trafficking.....25
- 9.6 Understanding Force, Fraud, and Coercion.....26
- 9.7 Responding to Trafficking Victims’ Leads .....27
- 9.8 Victim-Centered Approach .....29
- 9.9 Human Trafficking Computer-Based Training for Special Agents .....30

**Chapter 10. HUMAN SMUGGLING AND TRAFFICKING UNDERCOVER OPERATION AUTHORITY .....30**

- 10.1 Authority .....30
- 10.2 International Alien Transportation Operations.....32
- 10.3 Alien Transportation Operating Procedures.....32
- 10.4 Proprietary Drop House Operations .....35
- 10.5 Proceeds.....37

**Chapter 11. APPLICABLE MONEY LAUNDERING LAWS IN SUPPORT OF HUMAN SMUGGLING AND HUMAN TRAFFICKING INVESTIGATIONS .....37**

- 11.1 Money Laundering Laws.....38
- 11.2 Specified Unlawful Activities Related to Human Smuggling and Trafficking.....38
- 11.3 Forfeiture Laws .....38
- 11.4 Financial Investigative Methodology .....39

**Chapter 12. HOSTAGE SITUATIONS.....40**

- 12.1 Hostage Recovery.....40
- 12.2 Guidelines.....41

**Chapter 13. IMMIGRATION RELIEF OPTIONS FOR HUMAN SMUGGLING AND HUMAN TRAFFICKING INVESTIGATIONS .....45**

- 13.1 Material Witness Warrant .....45
- 13.2 Significant Public Benefit Parole .....46

- 13.3 Deferred Action .....46
- 13.4 Administrative Stay of Removal .....46
- 13.5 S Nonimmigrant Status .....46
- 13.6 Departure Control Order .....47
- 13.7 Continued Presence .....47
- 13.8 T Nonimmigrant Status and U Nonimmigrant Status .....48
- 13.9 Victim Assistance Coordinators and Victim Assistance Specialists.....48

**Chapter 14. CASE MANAGEMENT .....49**

- 14.1 TECS Case Categories .....49
- 14.2 TECS Program Codes .....49

**Chapter 15. INVESTIGATIVE RESOURCES .....50**

- 15.1 Human Smuggling and Trafficking Unit.....51
- 15.2 Human Smuggling and Trafficking Center .....51
- 15.3 National Human Trafficking Resource Center.....51
- 15.4 Victim Assistance Program .....52
- 15.5 Forensic Interview Program .....52
- 15.6 Office of Refugee Resettlement .....53
- 15.7 Non-Governmental Organizations .....53
- 15.8 HSI Office of Intelligence .....53
- 15.9 Human Trafficking Prosecution Unit.....54
- 15.10 Human Rights and Special Prosecution Section .....54
- 15.11 International Organized Crime Intelligence and Operations Center .....54
- 15.12 Special Operations Division.....55
- 15.13 Undercover Operations.....55
- 15.14 Counterterrorism and Criminal Exploitation Unit.....55

**APPENDICES**

Appendix A Domestic and International Undercover Alien Smuggling Investigations Approval Guidance Chart.....A

Appendix B Alien Tracking Sheet .....B

Appendix C Interview Questions for Human Smuggling Investigations.....C

Appendix D Interview Questions for Human Trafficking Investigations .....D

Appendix E Human Trafficking Case Notification .....E

Appendix F (b)(7)(E)

Appendix G Superseded Documents.....G

Appendix H Acronyms.....H

(b)(7)(E)

(Note: Smugglers may perform one or more of the above roles at any given time. For instance, during the course of an investigation, a drop house may be discovered and the harbinger may be arrested. Therefore, the criminal organization may require that a transporter or guide take on the role of the harbinger.)

### 6.3 Developing Targets

SAs should consider several factors in the development of a target. Some of the common factors include, but are not limited to, the following:

(b)(7)(E)

(b)(7)(E)

#### 6.3.1 Resources for Target Development

During target development, SAs are likely to receive information concerning HSOs and allegations that certain individuals are actively engaged in the smuggling of aliens into the United States. While considering the above factors, SAs should

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

### 6.3.2 Assistance from U.S. Customs and Border Protection

SAs should seek assistance from the CBP Office of Field Operations (OFO) and Office of Border Patrol (OBP) in human smuggling investigations when necessary. OBP utilizes various resources to combat human smuggling that may be useful to HSI SAs during their investigations of HSOs. Resources utilized

(b)(7)(E)

### 6.3.3 Smuggled Undocumented Aliens

(b)(7)(E)

## 6.4 Investigating Human Smuggling

When conducting a human smuggling investigation, SAs should try to:

(b)(7)(E)

(b)(7)(E)

### 6.5.1 Encountering Unaccompanied Children in Human Smuggling Investigations

HHS is responsible for the care and custody of unaccompanied children, including responsibility for detention where appropriate. SAs shall contact the Enforcement and Removal Operations (ERO) Field Office Juvenile Coordinator (FOJC) in their AOR upon encountering an individual who claims to be an unaccompanied child or the SAs suspect is an unaccompanied child, or where it cannot be determined within the 72-hour period that the unaccompanied child is a victim of human trafficking as outlined in Section 9.7 of this Handbook. The SA must also contact DUCS by calling the 24-hour DUCS Intake Hotline at (b)(7)(E) and emailing (b)(7)(E) with the information about the unaccompanied child.

The ERO FOJC is responsible for coordinating the actual placement of juveniles with ORR. Prior to transferring the juvenile into the custody of DUCS, the juvenile shall be served with an appropriate removal charging document (e.g., Notice to Appear (Department of Homeland Security (DHS) Form I-862) or Notice of the Intent/Decision to Reinstate Prior Order (DHS Form I-871)) under section 240 of the INA. SAs should continue to investigate whether or not the unaccompanied child is a crime victim. If it is determined that the unaccompanied child is in fact a crime victim, SAs should follow the procedures stated in Section 9.7 (F) of this Handbook.

(Note: For further policy guidance pertaining to the handling of unaccompanied children by ERO and HSI, see the DRO/OI memorandum entitled, “DRO/OI Protocols and Handling Unaccompanied Alien Children,” dated October 1, 2007, or as updated. *See also* Appendix B, “Alien Tracking Sheet,” and Appendix C, “Interview Questions for Human Smuggling Investigations.”

(Note: The above steps are not exhaustive. SAs should use their knowledge and judgment as situations arise.)

## Chapter 7. EXTRATERRITORIAL CRIMINAL TRAVEL STRIKE FORCE AND ILLICIT PATHWAYS ATTACK STRATEGY

### 7.1 Extraterritorial Criminal Travel Strike Force

(b)(7)(E)

(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

## 7.2 Illicit Pathways Attack Strategy

The IPAS is HSI's internal implementation plan to support the Transnational Organized Crime (TOC) Strategy which was revised by the National Security Council in 2011.

The IPAS is built upon the following four core principles:

- A. Working with counterparts to investigate, identify, disrupt, and dismantle transnational criminal organizations prior to their illicit activities reaching U.S. borders;
- B. Prioritization of networks and pathways posing the greatest threats;
- C. Robust interagency engagement; and
- D. A coordinated regional approach that leverages foreign partners.

HSI designed the IPAS to build, balance, and integrate its authorities and resources, both domestic and foreign, in a focused and comprehensive manner to target, disrupt, and dismantle transnational organized crime. As recognized in the TOC Strategy, resources are not limitless. Therefore, targets must be prioritized in a systematic manner. The IPAS provides a methodology and mechanism for HSI to prioritize threats and vulnerabilities within its mission and to coordinate its own efforts internally and within the interagency framework. HSTU is responsible for designating a case as an IPAS investigation based on established criteria.

(b)(7)(E)

(b)(7)(E)

## 9.2 HSI Trafficking in Persons Strategy

As part of HSI's continuing efforts to enhance its investigative capability to target human traffickers globally, HSI has developed a comprehensive strategy through which it will target criminal organizations and individuals engaged in trafficking in persons. The primary components of the Trafficking in Persons Strategy (TIPS) are outreach, coordination, and coalition building. In addition, HSI has partnered with state, local, federal, and international law enforcement components to develop universal strategies and investigative techniques to infiltrate HTOs and those involved in trafficking men, women, and children for the purpose of forced labor and forced commercial sex. The key objectives of this Handbook are to assist SAs in identifying HTOs, prioritizing investigations according to the degree of risk posed to national security and public safety, and coordinating investigations in order to dismantle HTOs and eliminate their ability to function and seize their illicit assets.

### A. Outreach

(b)(7)(E)

HSTU monitors and drives outreach efforts by requiring a quarterly outreach report to be submitted by SAC and Attaché offices. The reports consist of specific information regarding the NGOs, as well as content and frequency of contact.

B. Coordination

(b)(7)(E)

C. Coalition Building

(b)(7)(E)

intimidation, and extreme violence to maintain control of their victims and force them to toil in the most inhumane of conditions.

The sexual or economic exploitation of children for human trafficking purposes is one of the most reprehensible crimes within the investigative purview of HSI. Due to the nature of this offense, trafficking situations require specialized procedures and skills to assist the victims, especially child victims. SAs should utilize the VAC or the VAS to ensure that the needs of the victims are met. (Note: Additional information regarding the roles and responsibilities of the VAC and VAS is provided in Section 13.9 of this Handbook and in ICE Directive 10071.1, “Victim Assistance Program,” dated August 25, 2011, or as updated.)

Victims of trafficking are statutorily eligible for significant benefits under the law. SAs must provide CP to all victims, regardless of the victims’ cooperation in the investigation. It should be indicated in the CP application whether or not the victim is cooperating but this should have no bearing on the victim’s eligibility for CP. Human trafficking investigations should reflect a victim-centered approach whereby the identification, rescue, and protection of the victim is a priority and equally important to prosecuting the violator(s). SAs should always seek prosecution of human traffickers and the seizure of all their assets.

### 9.9 Human Trafficking Computer-Based Training for Special Agents

The mandatory Computer-Based Training on Human Trafficking for SAs provides specialized training as part of the DHS Blue Campaign – DHS’ multi-faceted approach to combatting human trafficking which includes public awareness, training, victim assistance, and law enforcement investigations. The course provides an overview of human trafficking, reality-based case scenarios, and the appropriate response when an HSI employee encounters a human trafficking situation. All SAs are required to take this training one time. New SAs must take the course prior to the completion of their first year of employment.

## Chapter 10. HUMAN SMUGGLING AND TRAFFICKING UNDERCOVER OPERATION AUTHORITY

(b)(7)(E)

### 10.1 Authority

HSI is granted the authority to conduct undercover investigative operations under the auspices of the Homeland Security Act, 19 U.S.C. § 2081 and 8 U.S.C. § 1363a. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

## 10.2 International Alien Transportation Operations

(b)(7)(E)

## 10.3 Alien Transportation Operating Procedures

SAC offices must comply with the following procedures for all domestic and international operations regarding the transportation of UDAs:

(b)(7)(E)

(b)(7)(E)

## 10.5 Proceeds

(b)(7)(E)

(b)(7)(E)

## Chapter 11. APPLICABLE MONEY LAUNDERING LAWS IN SUPPORT OF HUMAN SMUGGLING AND HUMAN TRAFFICKING INVESTIGATIONS

Since human smuggling and human trafficking criminal enterprises exist to make illicit profits, federal money laundering laws are appropriate and applicable to the investigation and prosecution of these types of criminal organizations. In fact, applying money laundering and asset forfeiture laws is a powerful means of attacking the human smuggling and human trafficking threat. Enhanced penalties for violating money laundering statutes are significant and include fines of up to \$500,000 and/or imprisonment up to 20 years.

HSI initiated Project STAMP (Smuggler and Trafficker Assets, Monies, and Proceeds) in order to attack human smuggling and human trafficking through anti-money laundering means and by seizing any illicit assets, thereby shutting down the entrenched criminal activity.

involved in smuggling and harboring, peonage, slavery, and trafficking in persons or money laundering as it relates to the aforementioned SUAs.

**B. 18 U.S.C. 982 – Criminal Forfeiture**

Criminal forfeiture law embodies actions against a person in question with the requirement that the government establish a beyond-a-reasonable-doubt guilt of a person and the person’s proprietary interest in the property in the indictment. The criminal forfeiture law allows for the government to obtain a general judgment against a person and allows for substitution of assets if the property is not available.

(Note: SAs should seek more detailed guidance by consulting the Asset Forfeiture Handbook (HSI HB 10-04), dated June 30, 2010, or as updated.)

**11.4 Financial Investigative Methodology**

During human smuggling or human trafficking investigations, once SAs fully establish all the elements of applicable SUAs as listed above, appropriate money laundering laws can be invoked in order to enhance the investigation.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

## Chapter 12. HOSTAGE SITUATIONS

Hostage situations generally come to the attention of HSI as the result of a report by a family member or a sponsor of the hostage victim who has contacted a federal, state, or local law enforcement agency with information pertaining to an extortion demand by members of an HSO.

(b)(7)(E)

(b)(7)(E) The violence or threats of violence and/or increase of the smuggling fee satisfy the criminal elements necessary to initiate the investigation and prosecution of a hostage-taking violation. *See* 18 U.S.C. § 1203.

(b)(7)(E)

### 12.1 Hostage Recovery

The primary goal of conducting a hostage-taking investigation is the successful recovery of the hostage(s). There are multiple methods that can be implemented to accomplish this goal. Determination of which method is the best for recovery of the hostage may vary from case to case depending on several factors.

(b)(7)(E)



(b)(7)(E)

## **Chapter 13. IMMIGRATION RELIEF OPTIONS FOR HUMAN SMUGGLING AND HUMAN TRAFFICKING INVESTIGATIONS**

While conducting human smuggling or human trafficking investigations, SAs should be aware of the immigration relief options available when encountering foreign national victims/witnesses. These options should be used in instances where it has been determined that presence of the victim/witness is required and is in the U.S. Government's best interest. SAs must thoroughly evaluate the totality of circumstances, identify special considerations (i.e., juveniles, witnesses who are also victims, criminal history, immigration history, security concerns, etc.) and then select the most appropriate option. The following descriptions contain only brief summaries and are not intended to provide detailed protocols or procedures related to each option.

### **13.1 Material Witness Warrant**

Pursuant to 18 U.S.C. § 3144, a federal judge or magistrate may order the arrest of a witness in criminal proceedings upon the filing of an affidavit demonstrating that the witness' testimony is material to the case and that it may be impractical to secure the witness' presence by subpoena. The court will determine if the witness shall be detained or released utilizing the conditions set forth in 18 U.S.C. § 3142. Witnesses ordered to be detained are remanded to the custody of the U.S. Marshals Service.

(b)(7)(E)

(b)(7)(E)

### 13.2 Significant Public Benefit Parole

SPBP may be used to bring an alien victim/witness, and, in some cases, the victim's/witness' immediate family members, into the United States for 1-year intervals. SPBP may be used for alien witnesses in judicial, administrative, or legislative proceedings. SPBP may also be used for alien victims on a case-by-case basis for "urgent humanitarian reasons" or significant public benefit for any alien applying for admission to the United States. *See* 8 U.S.C. § 1182(d) (5)(A). An SPBP is not an admission into the United States; however, employment authorization may be granted.

(Note: Additional guidance for SPBP can be found in the OI memorandum entitled, "Accountability of U.S. Immigration and Customs Enforcement (ICE) Significant Public Benefit Paroles," dated June 27, 2006, or as updated, and the OI memorandum entitled, "Interim Policy and Guidelines for Immediate Assumption of Significant Public Benefit Parole Responsibilities," dated August 8, 2006, or as updated.)

### 13.3 Deferred Action

Deferred action is "an act of administrative convenience to the government which gives some cases lower priority." *See* 8 C.F.R. § 274a.12(c)(14). In some cases, the determination to issue a deferred action is a discretionary decision made by the SAC. In other cases, such as when a victim has applied for certain benefits, the consideration of deferred action has been established as a matter of policy. Deferred action does not confer legal immigration status upon a victim/witness. An alien victim/witness granted deferred action may, upon application, be granted employment authorization. *See* 8 C.F.R. § 274a.12(c)(14).

### 13.4 Administrative Stay of Removal

An Administrative Stay of Removal (ASR) may be used for an alien witness with a Final Order of Removal. *See* 8 C.F.R. § 241.6. An ASR may be used when an alien is needed to "testify in the prosecution of a person for a violation of a law of the United States or of any State." *See* 8 U.S.C. § 1231(c) (2)(A)(ii). SACs should coordinate this option with the local ERO Field Office Director who has the discretionary authority to issue an ASR. An ASR does not confer legal immigration status upon an alien witness and the alien witness is not authorized to receive employment authorization based solely upon the ASR.

### 13.5 S Nonimmigrant Status

The S nonimmigrant status (also referred to as the "S Visa") may be granted to an alien witness and, in some cases, to the witness' immediate family members whose presence is "essential to the success of an authorized criminal investigation or the successful prosecution of an individual involved in the criminal organization or enterprise." *See* 8 U.S.C. § 1101 (a) (15)(S)(i)(III). An alien who is granted the S nonimmigrant status is eligible to receive employment authorization.

A sponsoring office may apply for the S nonimmigrant status using an Inter-Agency Alien Witness and Informant Record (USCIS Form I-854). SACs are advised to coordinate their requests with the Victim Assistance Program and Management Oversight (VAP/MO) Unit, ISD.

### 13.6 Departure Control Order

Although it does not provide the authority to physically detain any aliens, 8 U.S.C. § 1185 permits DHS to prevent the departure of certain aliens from the United States. The regulations implementing this provision state that the departure of an “alien who is needed in the United States as a witness in, or as a party to, any criminal case under investigation or pending in a court in the United States” shall be deemed prejudicial to the interests of the United States. *See* 8 C.F.R. § 215.3(g). When a departure control officer knows, or has reason to believe, that such person is going to depart, the officer shall serve such person with a written temporary order directing that the person shall not depart until further notified. *See* 8 C.F.R. § 215.2(a). The issuance of a Departure Control Order is issued upon the alien and cannot be used as a substitute for an ASR. SACs are delegated departure control authority in ICE Delegation Number 0001 entitled, “Delegation of Authority to the Directors, Detention and Removal and Investigations, and to Field Office Directors, Special Agents in Charge and Certain Other Officers of the Bureau of Immigration and Customs Enforcement,” dated June 6, 2003, or as updated.

### 13.7 Continued Presence

HSI recognizes that, in order to successfully investigate and prosecute traffickers, victims must be stable and free from fear and intimidation to be effective witnesses. Equal value should be placed on the identification and rescue of victims and the prosecution of traffickers. Short-term immigration benefits shall be provided to certified victims of human trafficking in the form of CP and can be requested only by a federal law enforcement agency with jurisdiction to investigate human trafficking violations.

(b)(7)(E)

(b)(7)(E)

The Secretary of DHS may permit these victims to remain in the United States to facilitate the investigation and prosecution of those individuals responsible for such offense. CP is initially granted for 12 months, is adjudicated by the Law Enforcement Parole Section (LEPS), Parole and Law Enforcement Programs Unit, TCPSD, and can be extended if necessary.

After it adjudicates a CP application, LEPS informs the USCIS Vermont Service Center for production of the Employment Authorization Document. USCIS then issues an Employment Authorization Document and an Arrival-Departure Record (CBP Form I-94) to the victim. Once a cooperating victim has been granted CP, the victim is also statutorily eligible for many additional benefits, including, but not limited to, mental health services, health

care assistance, housing or shelter assistance, food assistance, income assistance, employment assistance, and English language training.

During the investigation and prosecution of the suspected traffickers, SAs should make reasonable efforts to protect the safety of trafficking victims. This should include protection of trafficking victims and their families from intimidation, threats of reprisals, and reprisals from traffickers and their associates. SAs should be aware that, in addition to CP, law enforcement officials may also submit written requests to the Secretary of DHS, in accordance with the INA, to permit the parole into the United States of certain relatives of alien human trafficking victims or victims granted CP. If appropriate, victims and their family members may also be considered for the HSI Exigent Security for Witnesses Program (ESWP).

(Note: SAs should contact the VAP/MO Unit for more information on the ESWP. For further guidance concerning CP, SAs should refer to section 205 of the TVPRA and contact their local VAC or VAS.)

### **13.8 T Nonimmigrant Status and U Nonimmigrant Status**

The T nonimmigrant status and the U nonimmigrant status are used in human trafficking investigations as benefits for the victims of such crimes. While the T nonimmigrant status is used specifically for human trafficking cases, the U nonimmigrant status covers various criminal activities, including trafficking. *See* 8 C.F.R. §§ 214.11 and 214.14. Qualifying crimes for the U nonimmigrant status include, but are not limited to, kidnapping, manslaughter, peonage, sexual assault, and domestic violence. (Note: For further guidance, see the T Nonimmigrant Status Handbook (OI HB 09-03), dated October 5, 2009, or as updated, and the U Nonimmigrant Status Handbook (OI HB 09-04), dated December 1, 2009, or as updated.)

### **13.9 Victim Assistance Coordinators and Victim Assistance Specialists**

Due to the complex nature of human trafficking cases and the multitude of short-term and long-term needs experienced by victims, HSI human trafficking investigations are closely coordinated with activities provided under the VAP. HSI VACs and VASs are responsible for ensuring that victims are afforded their rights under the law and are connected to emergency services and resources. Each SAC office has SAs who are assigned the collateral duty of serving as VACs and receive special training on VAC responsibilities. In addition, there are full-time VASs located in various SAC offices nationwide. There are also victim assistance subject matter experts at HSI HQ in the VAP Section, VAP/MO Unit, ISD, who provide training, technical assistance, and case consultation to field offices, as needed. If victim services are needed for an investigation, SAs should contact their local VAC or VAS for resources and assistance.

VACs and VASs are trained to recognize indicators of human trafficking during the course of an investigation and to provide direct support and assistance when victims are encountered. VACs and VASs are responsible for ensuring that victims are aware of their rights under the TVPA and other relevant federal laws. They are also responsible for assisting case agents with applying for CP on behalf of victims; arranging suitable housing, health care, interpreter services, and other basic needs in the immediate aftermath of a rescue; and ensuring that law enforcement interviews

CODE	DESCRIPTION	ADDITIONAL INFORMATION
(b)(7)(E)		

## Chapter 15. INVESTIGATIVE RESOURCES

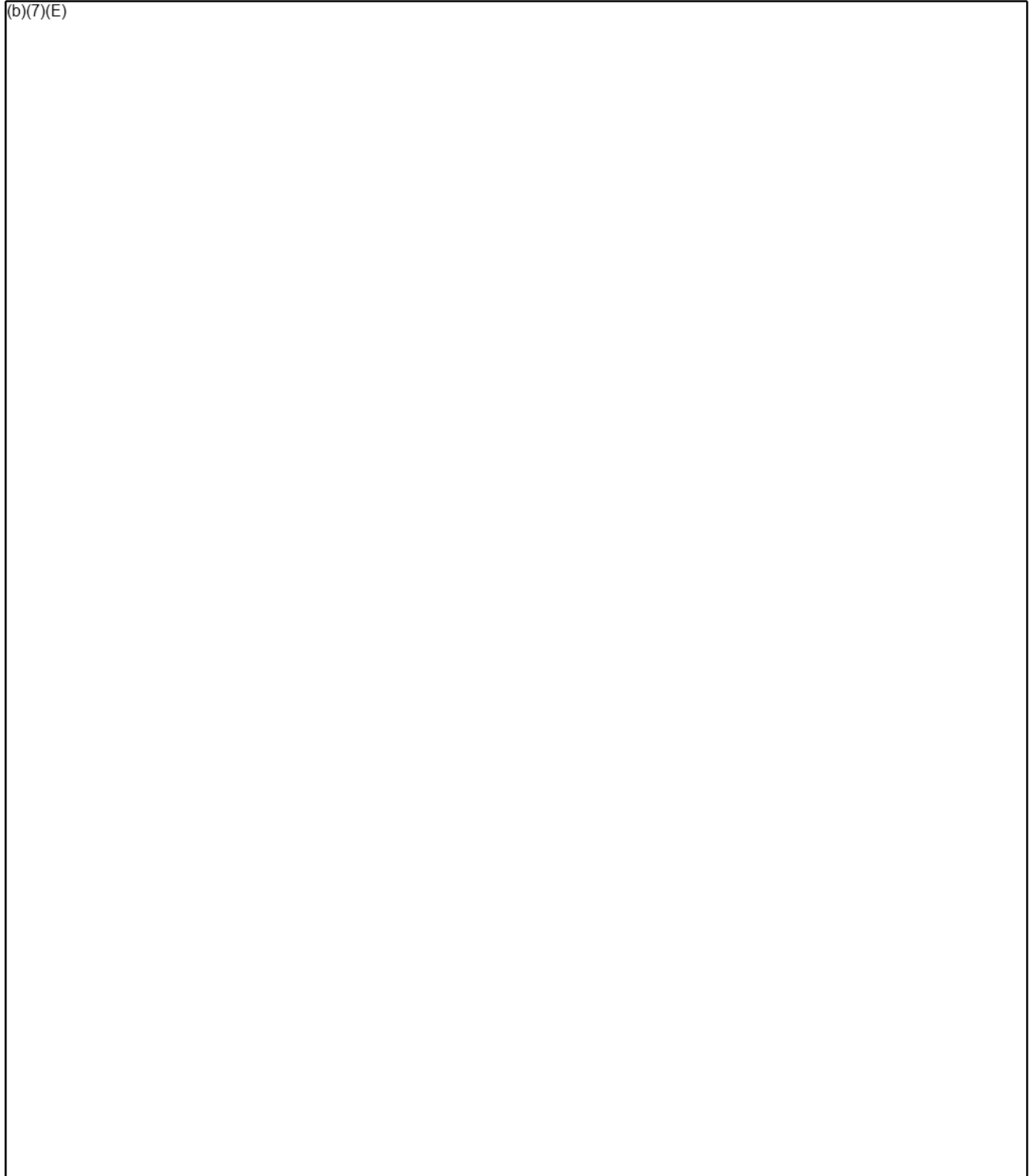
When conducting human smuggling or trafficking investigations, SAs need to be aware of organizations and entities that will aid in primary and secondary aspects of their investigations.

**DOMESTIC AND INTERNATIONAL UNDERCOVER  
ALIEN SMUGGLING INVESTIGATIONS**

**APPROVAL GUIDANCE CHART**

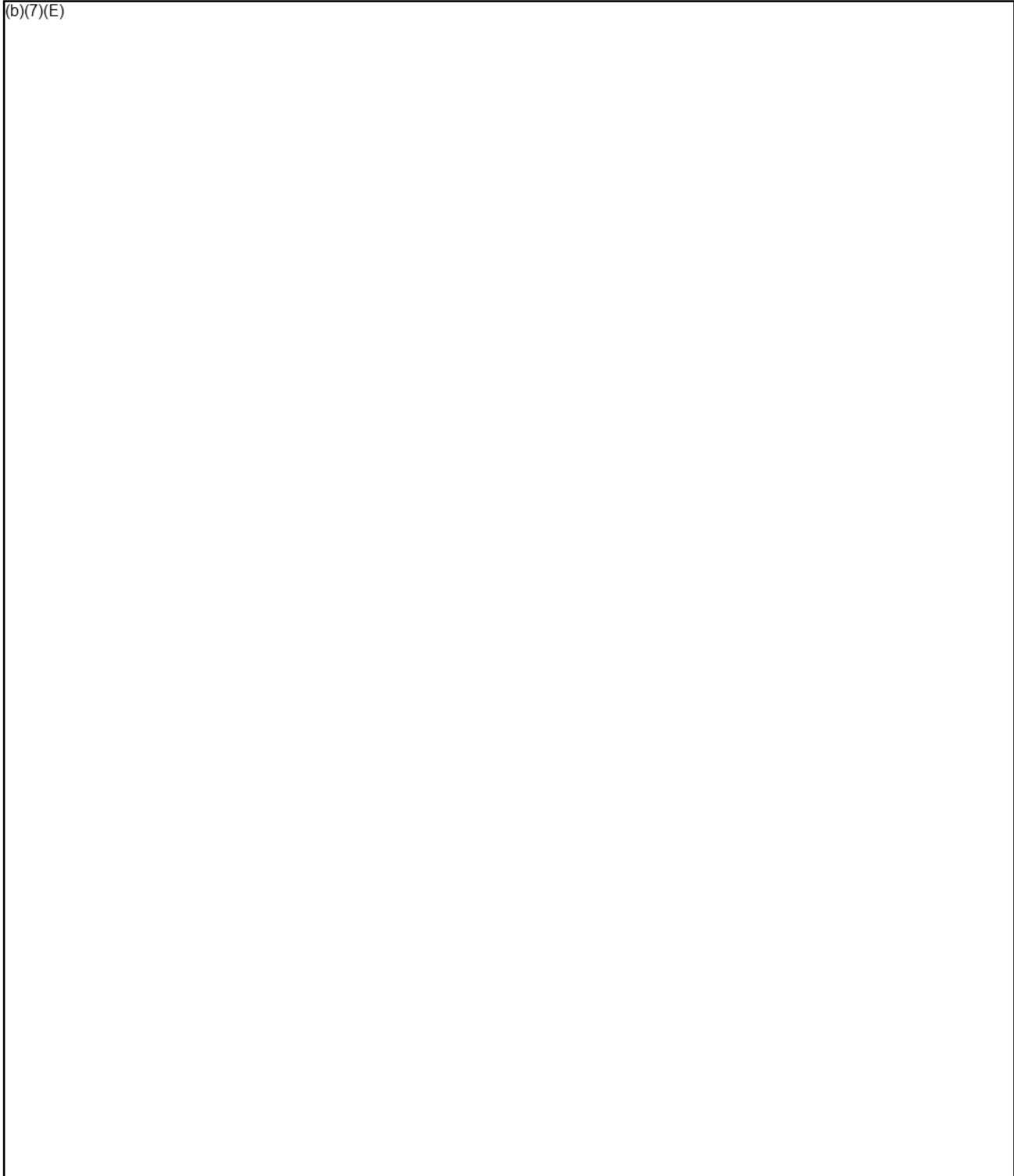
**INTERVIEW QUESTIONS  
FOR HUMAN SMUGGLING INVESTIGATIONS**

(b)(7)(E)



**INTERVIEW QUESTIONS  
FOR HUMAN TRAFFICKING INVESTIGATIONS**

(b)(7)(E)





**HUMAN TRAFFICKING CASE NOTIFICATION**

(b)(7)(E)

**DESCRIPTION OF INVESTIGATION**

(b)(7)(E)

**STATUS**

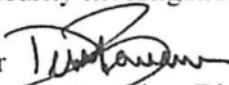
(b)(7)(E)




U.S. Immigration  
and Customs  
Enforcement

MAR 20 2017

MEMORANDUM FOR: Peter T. Edge  
Executive Associate Director  
Homeland Security Investigations

THROUGH: Derek Benner   
Deputy Executive Associate Director  
Homeland Security Investigations

FROM: Patrick J. Lechleitner   
Acting Assistant Director  
National Security Investigations Division

SUBJECT: TIDE Notification Process Termination

Purpose

This memorandum provides background information on the Terrorist Identities Datamart Environment (TIDE) notification process and discusses the value of the program moving forward.

Background

National Security Investigations Division (NSID), Visa Security Coordination Center (VSCC) has a National Program Manager (NPM), and an Intelligence Research Specialist (IRS) assigned to U.S. Customs and Border Protection (CBP) National Targeting Center-Passenger (NTC-P). The primary function of this section is to coordinate the vetting of TIDE encounters and provide notifications on positive encounters to Homeland Security Investigations (HSI) Special Agents and HSI Attachés for appropriate response. VSCC has been located at the NTC-P since 2005.

(b)(7)(E)

**SUBJECT: TIDE Notification Process Termination**

**Page 2**

(b)(7)(E)

The purpose of this process is to identify derogatory information for possible criminal prosecution, possible inadmissibility, and to provide information obtained during the interview and search to the Intelligence Community (IC) to update the TIDE record.

The VSCC provides notification to HSI domestic offices and HSI Attaché offices on over 700 TIDE encounters each year. Below is the current TIDE notification process.

(b)(7)(E)

**Issues**

Field compliance with the TIDE policy is remarkably low, averaging approximately 10-12% annually.

(b)(7)(E)

**Statistics**

**FY16**

<b>Notifications</b>	<b>ROIs completed</b>	<b>Compliance Rate</b>
<b>566</b>	<b>41</b>	<b>7%</b>

**FY15**

<b>Notifications</b>	<b>ROIs completed</b>	<b>Compliance Rate</b>
<b>750</b>	<b>100</b>	<b>13%</b>

~~LAW ENFORCEMENT SENSITIVE~~

FY14		
Notifications	ROIs completed	Compliance Rate
721	85	12%
FY13		
Notifications	ROIs completed	Compliance Rate
757	94	12%
FY12		
Notifications	ROIs completed	Compliance Rate
708	60	9%

There are no enforcement statistics, seizures or arrests, resulting from TIDE notifications.

(b)(7)(E)

Discussion

The TIDE notification effort was essential at its inception but over time, the Watchlisting and screening community has evolved and developed more efficient, while HSI process has changed little. Therefore, this effort is now ineffective and duplicative. VSCC recommends that HSI terminate the program and reassign two of the personnel to other duties.

(b)(7)(E)

Recommendation

The termination of the VSCC TIDE notification process is justified and approved.

Approve *[Signature]* Disapprove \_\_\_\_\_  
Modify \_\_\_\_\_ Needs more discussion \_\_\_\_\_

# NARCOTICS AND TRANSNATIONAL ORGANIZED CRIME REWARDS PROGRAMS HANDBOOK

## Table of Contents

<b>Chapter 1.</b>	<b>PURPOSE AND SCOPE</b> .....	<b>1</b>
<b>Chapter 2.</b>	<b>INTRODUCTION</b> .....	<b>1</b>
<b>Chapter 3.</b>	<b>DEFINITIONS</b> .....	<b>1</b>
	• 3.1 Chief of Mission .....	1
	• 3.2 Chargé(e) d’Affaires .....	2
	• 3.3 Classified Information .....	2
	• 3.4 Confidential Informant.....	2
	• 3.5 Cooperating Individual .....	2
	• 3.6 Foreign Government Information .....	2
	• 3.7 For Official Use Only .....	3
	• 3.8 Law Enforcement Sensitive .....	3
	• 3.9 Major Violator of Transnational Organized Crime Activity .....	3
	• 3.10 Major Violator of U.S. Narcotics Law.....	3
	• 3.11 Request Proposal.....	3
	• 3.12 Rewards Committees .....	4
	• 3.13 Reward Offer .....	4
	• 3.14 Reward Payment .....	4
	• 3.15 Sensitive But Unclassified Information .....	5
<b>Chapter 4.</b>	<b>AUTHORITIES/REFERENCES</b> .....	<b>5</b>
<b>Chapter 5.</b>	<b>RESPONSIBILITIES</b> .....	<b>5</b>
	• 5.1 Executive Associate Director, Homeland Security Investigations .....	5
	• 5.2 Deputy Assistant Director, Investigative Services Division.....	6
	• 5.3 Unit Chief, Undercover Operations Unit .....	6
	• 5.4 Section Chief, Confidential Informants and Investigative Services Section.....	6
	• 5.5 National Program Manager, Rewards Programs .....	6
	• 5.6 Special Agents in Charge and Attachés .....	6
	• 5.7 Group Supervisors .....	6
	• 5.8 Assistant Attachés .....	6
	• 5.9 Special Agents .....	7

<b>Chapter 6. PROGRAM CLASSIFICATION.....</b>	<b>7</b>
<b>Chapter 7. PREPARING AND TRANSMITTING PROPOSALS FOR REWARD PAYMENTS.....</b>	<b>7</b>
<b>Chapter 8. NARCOTICS REWARDS PROGRAM.....</b>	<b>8</b>
• 8.1 Narcotics Reward Offer and Payment Proposal Format.....	9
• 8.2 Criteria for Determining Reward Amounts .....	11
<b>Chapter 9. TRANSNATIONAL ORGANIZED CRIME REWARDS PROGRAM .....</b>	<b>12</b>
• 9.1 Reward Offer Proposal Format.....	12
• 9.2 Reward Payment Proposal Format.....	15
<b>Chapter 10. HSI MARKING REQUIREMENTS.....</b>	<b>18</b>
• 10.1 Classification Guidance for Draft Proposals.....	18
• 10.2 E-mails Containing Classified Supplemental Information .....	21
• 10.3 E-mails Containing Unclassified Supplemental Information .....	22
<b>Chapter 11. DOS BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS MARKING REQUIREMENTS .....</b>	<b>24</b>
• 11.1 Final Proposal .....	24
• 11.2 E-mails Transmitting Supplemental Information to INL.....	27
<b>Chapter 12. TRANSMISSION REQUIREMENTS .....</b>	<b>29</b>
• 12.1 HSI Transmission Requirements .....	29
• 12.2 DOS INL Transmission Requirements .....	29

**APPENDICES**

Appendix A	Marking Requirements Summary .....	A-i
Appendix B	Factors to Consider When Determining Reward Amount.....	B-i
Appendix C	Acronyms.....	C-i

### **3.2 Chargé(e) d’Affaires**

A diplomat, usually a diplomatic secretary, counselor, or minister, who heads a diplomatic mission (e.g., an embassy) in the absence of the Ambassador.

### **3.3 Classified Information**

Classified information is information that has been determined, pursuant to Executive Order (EO) 13526, “Classified National Security Information,” or any predecessor EO, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

### **3.4 Confidential Informant**

A CI is a person who: 1) provides HSI with credible information concerning unlawful activity and works under the direction and control of an HSI SA; 2) has a reasonable expectation of confidentiality; and 3) is documented in compliance with the provisions of the Informants Handbook (HSI HB 12-03), dated August 2, 2012, or as updated. Any individual who is paid more than \$2,500 in payment of purchases of information per fiscal year and/or receives immigration-related benefits must be documented as a CI or Cooperating Individual. Only HSI SAs are permitted to document and manage CIs within the guidelines of the HSI Informants Handbook. (See Section 3.5 of the Informants Handbook.)

### **3.5 Cooperating Individual**

A Cooperating Individual is a person who: 1) provides HSI with credible information concerning unlawful activity and works under the direction and control of an HSI SA; 2) has **no** reasonable expectation of confidentiality; and 3) is documented in compliance with the provisions of HSI Informants Handbook (HSI HB 12-03), dated August 2, 2012, or as updated. The assumed name will be waived, but the Cooperating Individual will be assigned a CI number. Only HSI SAs are permitted to document and manage Cooperating Individuals within the guidelines of the HSI Informants Handbook. (Note: See Section 3.9 of the Informants Handbook.) (Note: The term CI is used throughout this Handbook; however, all policies and procedures outlined in this Handbook also apply to Cooperating Individuals unless otherwise noted.)

### **3.6 Foreign Government Information**

Foreign government information is:

- A. Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

- B. Information produced by the U.S. Government pursuant to, or as a result of a joint arrangement with, a foreign government or governments or an international organization of governments or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or
- C. Information received and treated as “foreign government information” under the terms of a predecessor EO.

### **3.7 For Official Use Only**

For Official Use Only (FOUO) information is unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest.

### **3.8 Law Enforcement Sensitive**

Law Enforcement Sensitive (LES) information is a type of FOUO information that is compiled for law enforcement purposes, the loss or misuse of, or unauthorized access to, which could adversely affect the national interest or the conduct of investigative work, disclose the identity of a CI or a source of information, endanger life or physical safety, or impact the privacy to which individuals are entitled under the Privacy Act or the Department of Homeland Security (DHS) Directive 047-01, Privacy Policy and Compliance, dated July 7, 2011.

### **3.9 Major Violator of Transnational Organized Crime Activity**

Any individual who threatens U.S. national interests through transnational organized crime activity beyond drug trafficking, such as human trafficking, wildlife trafficking, cybercrime, money laundering, and trafficking in arms and other illicit goods.

### **3.10 Major Violator of U.S. Narcotics Law**

Any individual who has been designated a significant foreign narcotics trafficker under the Foreign Narcotics Kingpin Designation Act, designated as a Consolidated Priority Organization Target (CPOT), or anyone identified and recognized as a major violator of U.S. narcotics law.

### **3.11 Request Proposal**

The Request Proposal is the format that INL recommends for the submission of requests for reward offers and payments. The content requirements for the letters are prescribed in INL’s “Narcotics Reward Payment Request Guidance,” (dated February 2013) and “Transnational Organized Crime Rewards Program Standard Operating Procedure,” dated August 29, 2014. (Note: See Sections 8.1, 9.1, and 9.2 of this Handbook for further guidance.)



## **5.2 Deputy Assistant Director, Investigative Services Division**

The Deputy Assistant Director (DAD), Investigative Services Division (ISD), is responsible for the overall implementation of the provisions of this Handbook.

## **5.3 Unit Chief, Undercover Operations Unit**

The Unit Chief, UOU, is responsible for approving proposals for the DOS Rewards Programs.

## **5.4 Section Chief, Confidential Informants and Investigative Services Section**

The Section Chief, Confidential Informants and Investigative Services Section, is responsible for reviewing proposals for participation in the Rewards Program and ensuring that such proposals satisfy the HSI and DOS INL requirements. The Section Chief may also represent HSI at the DOS INL IRC.

## **5.5 National Program Manager, Rewards Programs**

The Rewards Program National Program Manager (NPM) is responsible for ensuring that HSI proposals meet the requirements mandated by INL, consulting with SAs, providing guidance to HSI field offices on completing proposals for the NRP and TOCRP, derivatively classifying field office reward offers and payment requests in consultation with SAs, serving as the liaison to DOS for the Rewards Programs, and representing HSI on the IRC.

## **5.6 Special Agents in Charge and Attachés**

Special Agents in Charge (SACs) and Attachés (or Assistant Attachés if no Attaché is present in country) are responsible for implementing the provisions of this Handbook within their respective areas of responsibility.

## **5.7 Group Supervisors**

Group Supervisors (GSs) are responsible for ensuring that proposals comply with HSI and DOS INL requirements prior to submission to UOU.

## **5.8 Assistant Attachés**

Assistant Attachés are responsible for briefing the Attaché and the Chief of Mission on the NRP or TOCRP proposals received from the UOU NPM. The Assistant Attaché is also responsible for forwarding the cable to DOS.

## 5.9 Special Agents

SAs are responsible for complying with the provisions of this Handbook. SAs must complete the Office of Professional Responsibility (OPR) Security Division's Derivative Classification Training Webinar and obtain access to the Homeland Security Data Network (HSDN) prior to submitting a request.

## Chapter 6. PROGRAM CLASSIFICATION

To ensure confidentiality under its Rewards Programs, DOS requires that the identity of the CIs and the information they provide be classified under EO 13526, "Classified National Security Information." (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Requests for reward offers submitted to INL are classified according to the information contained in the request.

## Chapter 7. PREPARING AND TRANSMITTING PROPOSALS FOR REWARD PAYMENTS

The following procedures must be followed when requesting reward payments:

- A. The SA will draft a proposal in accordance with INL content and formatting requirements.
- B. The SA will refer to the CI by his or her assigned CI number only and review the draft proposal to ensure that it contains no other information that could reveal the CI's identity (e.g., family member names or relationships, addresses, and telephone numbers).
- C. The SA will transmit the draft proposal to the GS or Assistant Attaché in accordance with the transmission requirements in Chapter 12.
- D. The GS will review the draft proposal for compliance with INL content and formatting requirements and ensure that CI confidentiality is maintained and, if necessary, revise the draft proposal.
- E. The SA or GS will transmit the final proposal to UOU for review in accordance with the transmission requirements in Chapter 12.

- F. If the NPM or INL have questions on the proposal or requests for supplemental information, they will forward the questions or request to the SA or GS who prepared the proposal.
- G. The SA will prepare answers to the questions or the supplemental information requested and have the GS review them.

Completed proposals must be forwarded to the DAD of ISD for review. Once all requirements are met for the applicable request, the NRP/TOCRP NPM will mark the proposal in accordance with the requirements in Chapter 10. The HSI Attaché is responsible for briefing the U.S. Ambassador or Chargé(e) d’Affaires to obtain his or her concurrence. Once concurrence is received from the Ambassador or Chargé(e) d’Affaires, the HSI Attaché Office is responsible for converting the content into cable formatting and forwarding the cable to INL.

(Note: All requests must conform to DOS guidelines and have concurrence from the SAC, the HSI Attaché, the appropriate U.S. Ambassador, and—for reward payments only for matters over which there is federal criminal jurisdiction—the appropriate U.S. Attorney. All requests to INL must include the requested reward offer or reward payment amount, which may not exceed \$5 million.)

## **Chapter 8. NARCOTICS REWARDS PROGRAM**

The Narcotics Rewards Program was established by Congress in 1986 as a tool to assist the U.S. Government in identifying and bringing to justice the major violators of U.S. narcotics laws responsible for bringing hundreds of tons of illicit drugs into the United States each year. Under this program and subject to the availability of appropriated funds, the Secretary of State has the statutory authority (22 U.S.C. § 2708) to offer rewards of up to \$25 million for information leading to the arrest and/or conviction of major narcotics traffickers who operate outside the United States to send drugs into the United States. For the purpose of this Handbook, HSI reward offers and payment requests may not exceed \$5 million. (Note: Promises of a reward payment from the DOS NRP may NOT be made to CIs. Only the Secretary of State may make the determination to pay a reward. Note also: U.S. and foreign government employees, including police, are not eligible for rewards under the NRP.)

The IRC must unanimously recommend approval of both the reward offer and the amount requested; the IRC may agree to change the amount. Once the IRC reaches a consensus, NRP will seek internal DOS clearance and forward the nomination to the INL Assistant Secretary with a recommendation for approval or denial. The INL Assistant Secretary will send a letter to ISD confirming the decision and the reward amount. If a nomination is denied, the letter will also include the basis for denial. Approved reward offers are embargoed until a date determined by DOS in consultation with ISD.

## 8.1 Narcotics Reward Offer and Payment Proposal Format

The following format, including section headings, will be used for all NRP proposals. This format is taken from DOS's NRP Reward Payment Request Guidance. Each of the section headings below should be numbered in the proposal. (Note: SAs must not submit the proposal using "all caps.")

### A. Issue for Decision

(b)(7)(E)
(b)(7)(E)

### B. Importance of the Trafficker Involved

(b)(7)(E)
-----------

### C. Role of the Proposed Reward Recipient

(b)(7)(E)
-----------

Include responses to the following questions:

(b)(7)(E)
-----------

(b)(7)(E)

**D. Arrest**

Describe the events leading up to and including the arrest of the trafficker, and how the CI's information and/or assistance were helpful. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

**E. Risk to the Proposed Reward Recipient(s)**

(b)(7)(E)

**F. Additional Considerations**

(b)(7)(E)

(b)(7)(E)

7) Include the following affirmation statement in the request cable:

“I, (requesting SA’s full name), hereby confirm that all the information in this request is true and accurate and that the individual(s) recommended for a reward payment meets all the statutory qualifications for eligibility. The Reward Program Participant provided the information voluntarily, without any promises that a reward payment would be made. (Name and title of supervisor) of my parent agency has approved this recommendation.”

## **8.2 Criteria for Determining Reward Amounts**

In preparing the Request Proposal, HSI will determine the initial amount of the reward based on the following factors:

- A. Significance of the target;
- B. Value of the information provided;
- C. Risk to the CI and/or family members as a result of providing the information;
- D. The level of cooperation by the CI to provide the information;
- E. The CI’s involvement with narcotics transnational criminal enterprises; and
- F. Other forms of compensation.

HSI SAs should take these factors into consideration to determine if a reward amount is appropriate. The initial reward payment proposal is presented to the IRC for review and

(b)(7)(E)

2) Reward Amount (b)(7)(E)

a) Justification of Reward Amount:

(b)(7)(E)

**B. Criminal Activity:**

(b)(7)(E)

**C. Identifiers:**

1) Must include the following:

(b)(7)(E)

- e) Nationality
- f) Citizenship
- g) Height (ft/in)
- h) Weight (lbs)
- i) Eye Color
- j) Hair Color
- k) Distinguishing marks, scars, tattoos, etc.

D. Primary Types of Criminal Activity:

- 1) Describe in detail the criminal activity, including the following:

(b)(7)(E)

- 2) Description of Organization:

(b)(7)(E)



(b)(7)(E)

3) Publicity

(b)(7)(E)

4) Approvals:

(b)(7)(E)

**9.2 Reward Payment Proposal Format**

The following format, including section headings, will be used for all TOCRP reward payment proposals. All nomination proposals for reward payments must include the requestor's (SA) name, rank, office location, and contact information, including phone number and e-mail address.

A. General

(b)(7)(E)

(b)(7)(E)

**B. Narrative Description of Target and Circumstances**

(b)(7)(E)

**C. Role of the Rewards Program Participant**

(b)(7)(E)

(b)(7)(E)

D. Required Information:

(b)(7)(E)

E. Approvals:

(b)(7)(E)

(b)(7)(E)

F. Required Statement:

Include the following statement in the request cable:

“I, (requesting SA’s full name), hereby confirm that all the information in this request is true and accurate and that the individual(s) recommended for a reward payment meet(s) all the statutory qualifications for eligibility. The Reward Program Participant provided the information voluntarily, without any promises that a reward payment would be made. (Name and title of supervisor) of my parent agency has approved this recommendation.”

## Chapter 10. HSI MARKING REQUIREMENTS

SAs will prepare draft reward offer and payment requests and supplemental e-mails when recommending CIs for participation in the Rewards Programs. The NPM will review the draft, place appropriate classification markings, and finalize the document for submission to the HSI Attaché for the Attaché to debrief the INL in-country point of contact and the U.S. Ambassador. (See Appendix A, Marking Requirements - Summary.) The HSI Attaché representative will be responsible for ensuring that a cable is transmitted, with the final proposal, to INL.

### 10.1 Classification Guidance for Draft Proposals

SAs who prepare draft proposals requesting reward offers or payments for CIs will use information collected in the normal course of investigative activity. Such information is marked in accordance with its sensitivity; in field offices, this is generally FOUO and FOUO-LES.

As a general rule, SAs will NOT author award recommendations where the information or investigation is classified. If an SA is engaged in an investigation or documenting information that is classified at the Confidential or above level, such information CANNOT be entered into (b)(7)(E) and all classified documents must be properly handled and secured. The NPM must be informed of all recommendations involving classified information at the onset and closely coordinate with the SAC or Attaché office. The NPM will review and apply the markings (if classified above Confidential) and the classification authority markings for the draft document.

A. Investigative or Other Information Meeting Standards for Classification under EO 13526.

Draft proposals containing investigative or other information that meets the standards for classification in EO 13526 must be marked in accordance with the requirements prescribed below. (Note: This Subsection addresses information that is classified *prior to* its association with the Rewards Programs. Information classified *because of* its association with the Rewards Program is discussed in Section 11.1.A(3)(b).

1) Overall Classification Marking

The overall classification level of a draft proposal containing classified information must correspond to the highest overall classification level of information from an authorized source document or a Security Classification Guide (SCG). This marking must be placed on the front page and on the back of the last page (if printed in hard copy).

2) Page Markings

Each page of the draft proposal must be marked with the highest overall classification level of the entire document or with the highest level of information contained on the page.

3) Portion Markings

- a) Each portion of the draft proposal that contains classified information must be marked in accordance with the authorized source document or SCG (e.g., (S) or (C) – for Secret or Confidential, respectively – preceding the portion).
- b) Any portion that contains FOUO-LES information but does NOT contain any classified information must be marked with “(U) (FOUO-LES)” preceding the portion.
- c) Any portion that contains FOUO information that is not LES but does NOT contain any classified information must be marked with “(U) (FOUO)” preceding the portion.
- d) Any portion that contains *only* other SBU information (i.e., the portion does not contain any classified information or any FOUO-LES information) must be marked in accordance with the governing statute or regulations, as appropriate (e.g., “(U) (SSI)” – for Unclassified or SSI, respectively – or “(U) (PCII)” – for Unclassified or PCII, respectively – preceding the portion).

- e) Any portion that contains *only* unclassified information must be marked with “(U)” preceding the portion.

4) Classification Authority Markings

The draft proposal must contain classification authority markings (usually in the form of a block) on the front page. The NPM will draft the classification authority markings for the draft document. The classification authority markings must contain the following:

- a) A “Classified By” line that provides the name of the NPM who is generating the request proposal.
- b) A “Derived From” line that provides identifying information on the source that authorizes the classification of the information, which is the name of the authorized source document or SCG.
- c) A “Declassify On” line that provides the date that the information may be declassified, as determined in the authorized source document or SCG.
- d) Sample classification authority block:

(b)(7)(E)
-----------

B. Investigative Information Not Meeting Standards for Classification under EO 13526.

Draft proposals containing investigative information that does not meet the requirements for classification under EO 13526 must be marked as follows:

1) Page Markings.

Draft proposals containing investigative information must be marked with “FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE” across the bottom of the front page and each interior page that contains investigative information.

2) Portion Markings.

- a) Each portion of the draft proposal that contains investigative information must be marked with “(U) (FOUO-LES)” preceding the portion.
- b) Any portion of the draft proposal that contains FOUO information (other than FOUO-LES) must be marked with “(U) (FOUO)” preceding the portion.

- c) Any portion of the draft proposal that contains information protected by a statute or federal regulations must be marked in accordance with the statute or regulations, as appropriate (e.g., “(U) (SSI)” or “(U) (PCII)” preceding the portion).
  - d) Any portion of the draft proposal that contains *only* unclassified information must be marked with “(U)” preceding the portion.
- 3) Warning Statement.

The following warning statement must be included on the bottom of the front page of the draft proposal:

**WARNING:** This document has been designated Department of Homeland Security (DHS) LAW ENFORCEMENT SENSITIVE by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), and must be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS and ICE policy relating to LAW ENFORCEMENT SENSITIVE information. *This information may not be distributed beyond the original addressees without prior authorization of HSI.*

- 4) Other Unique Required Markings

Unique markings required by statute or regulations (e.g., warning statements or banners) must be included on the draft proposal in accordance with the statute or regulations, as appropriate (e.g., an SSI footer).

## 10.2 E-mails Containing Classified Supplemental Information

Occasionally, information provided to INL in a reward offer or a payment request must be supplemented with additional supporting information. SAs generating e-mails containing supplemental information that meets the standards for classification in EO 13526 must mark the e-mails in accordance with the requirements prescribed below. (Note: This Section addresses information that is classified *prior to* its association with the Rewards Programs. Information classified *because of* its association with the Rewards Program is discussed in Section 11.1.A(3)(b).)

### A. Overall Classification Marking

The overall classification level of the e-mail must correspond to information from an authorized source document or an SCG.

### B. Portion Markings

- 1) Each portion of the e-mail that contains classified information must be marked in accordance with the authorized source document or SCG (e.g., (S) or (C) preceding the portion).
- 2) Any portion that contains FOUO-LES information but does NOT contain any classified information must be marked with “(U) (FOUO-LES)” preceding the portion.
- 3) Any portion that contains FOUO information (that is not LES) but that does NOT contain any classified information must be marked with “(U) (FOUO)” preceding the portion.
- 4) Any portion that contains SBU information protected by statute or federal regulations but does NOT contain any classified information must be marked in accordance with the statute or regulations, as appropriate (e.g., “(U) (SSI)” or “(U) (PCII)” preceding the portion).
- 5) Any portion that contains *only* unclassified information must be marked with “(U)” preceding the portion.
- 6) Classification Authority Markings

The e-mail must contain classification authority markings (usually in the form of a linear string) underneath the signature block but before the overall classification marking. The classification authority markings must contain the following:

- a) A “Classified By” line that provides the name of the SA who is generating the classified e-mail.
- b) A “Derived From” line that provides identifying information on the source that authorizes the classification of the information in the e-mail, which is the name of the authorized source document or SCG.
- c) A “Declassify On” line that provides the date when the information may be declassified, as determined in the authorized source document or SCG.
- d) Sample classification authority linear string:

(b)(7)(E)

### 10.3 E-mails Containing Unclassified Supplemental Information

SAs generating e-mails containing unclassified supplemental information (i.e., containing no classified information) must mark the e-mails as prescribed below, depending on the type of unclassified information.



#### A. Overall Marking

E-mails containing unclassified supplemental information must be marked with “FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE” at the top of the e-mail.

#### B. Portion Markings

- 1) Any portion that contains FOUO-LES information must be marked with “(U) (FOUO-LES)” preceding the portion.
- 2) Any portion that contains FOUO information (that is not LES) must be marked with “(U) (FOUO)” preceding the portion.
- 3) Any portion that contains SBU information protected by statute or federal regulations must be marked in accordance with the statute or regulations, as appropriate (e.g., “(U) (SSI)” or “(U) (PCII)” preceding the portion).
- 4) To avoid ambiguity, any portion that contains *only* unclassified information must be marked with “(U)” preceding the portion.

#### C. Warning Statement

The following warning statement must be included at the bottom of the e-mail:

**WARNING:** This e-mail contains information designated as Department of Homeland Security (DHS) LAW ENFORCEMENT SENSITIVE by U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and must be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS and ICE policy relating to LAW ENFORCEMENT SENSITIVE information. ***This e-mail may not be distributed beyond the original recipients without prior authorization of HSI.***

#### D. Other Unique Required Markings

Unique markings required by statute or regulations (e.g., warning statements or banners) must be included on the e-mail in accordance with the statute or regulations, as appropriate (e.g., an SSI footer).

## **Chapter 11. DOS BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS MARKING REQUIREMENTS**

Documents recommending CIs for participation in the Rewards Programs that are being provided to INL must be marked in accordance with the requirements in EO 13526 and the instructions from INL. (See Appendix A, Marking Requirements - Summary.)

### **11.1 Final Proposal**

The UOU NPM shall prepare the final classified proposal for transmission to the HSI Attaché Office for the Attaché to debrief the INL in-country point of contact and the U.S. Ambassador. The HSI Attaché representative is responsible for ensuring that a cable is transmitted with the final proposal to the INL as follows:

#### **A. Required INL Markings**

The final proposal must be marked as follows:

##### **1) Overall Classification Marking.**

The overall classification of the payment request is “SECRET/Not Releasable to Foreign Nationals.” The marking “SECRET/NOFORN” must be placed at the top and bottom of the front page, each interior page, and the back of the last page (if printed in hard copy). Reward offer requests should be marked according to the classification level of the information contained in the request.

##### **2) Page Markings**

Each page of the reward payment request must be marked with the highest overall classification, which is “SECRET/NOFORN.” Each page of the reward offer must be marked according to the highest level of classification contained on that page.

##### **3) Portion Markings**

- a) Each portion of the final proposal that contains information that is classified under EO 13526 must be marked with “(S/NF)” – for Secret and Not Releasable to Foreign Nationals, respectively – preceding the portion. In particular, the following information must be marked with “(S/NF)”:

(b)(7)(E)

- b) Each portion of the final proposal that contains information that could be used to identify the CI must be marked with “(S/NF)” preceding the portion. Information that could be used to identify a CI includes:

(b)(7)(E)

(b)(7)(E)

- c) Each portion of the final proposal that contains FOUO-LES information but does not contain any information that could be used to identify the CI must be marked with “(U) (FOUO-LES)” preceding the portion.
  - e) Any portion of the final proposal that contains FOUO information (that is not LES) and does not contain any information that could be used to identify the CI must be marked with “(U) (FOUO)” preceding the portion.
  - f) Any portion of the final proposal that contains SBU information protected by statute or federal regulations must be marked in accordance with the statute or regulations, as appropriate (e.g., “(U) (SSI)” or “(U) (PCII)” preceding the portion).
  - g) Any portion of the final proposal that contains *only* unclassified information must be marked with “(U)” preceding the portion.
- 4) Classification Authority Markings.

The classification authority block must contain the following:

- a) A “Classified By” line that provides the name of the supervisor who is transmitting the proposal to INL.
- b) A “Derived From” line that provides the name of the source that authorizes the classification of the information.

(b)(7)(E)

- c) A “Declassify On” line that provides the date when the information may be declassified, as determined by INL, which is 25 years from the date of the final proposal.

d) Sample Classification Authority Blocks:

(b)(7)(E)

## 11.2 E-mails Transmitting Supplemental Information to INL

The UOU NPM shall respond to INL questions and requests for additional information via classified e-mail.

### A. Required Markings

The e-mails must be marked as follows:

#### 1) Overall Classification Marking

(b)(7)(E)

#### 2) Portion Markings

- a) Each portion that contains information that is classified under EO 13526 must be marked with “(S/NF)” preceding the portion. (See Subsection 11.1 (A)(3)(a) above.)
- b) Each portion that contains information that could be used to identify the CI must be marked with “(S/NF)” preceding the portion. (See Subsection 11.1 (A)(3)(b) above.)
- c) Each portion that contains FOUO-LES information but does not contain information classified under EO 13526 or that could be used to identify the CI must be marked with “(U) (FOUO-LES)” preceding the portion.

- d) Any portion that contains FOUO information (that is not LES) and does not contain information classified under EO 13526 or information that could be used to identify the CI must be marked with “(U) (FOUO)” preceding the portion.
- h) Any portion that contains SBU information protected by statute or federal regulations must be marked in accordance with the statute or regulations, as appropriate (e.g., “(U) (SSI)” or “(U) (PCII)” preceding the portion).
- i) Any portion that contains *only* unclassified information must be marked with “(U)” preceding the portion.

3) Classification Authority Markings

The e-mail must contain classification authority markings (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

The classification authority markings must contain the following:

- a) A “Classified By” line that provides the name of the supervisor who is transmitting the e-mail to INL.
- b) A “Derived From” line that provides the name of the source that authorizes the classification of the information.

(b)(7)(E)

d) Sample Classification Authority

(b)(7)(E)

(b)(7)(E)

## Chapter 12. TRANSMISSION REQUIREMENTS

### 12.1 HSI Transmission Requirements

Proposals and supplemental e-mails must be transmitted in accordance with the following requirements:

A. E-mails Containing or Transmitting Classified Information.

E-mails containing or transmitting classified information must be transmitted in accordance with the requirements in DHS Instruction 121-01-011, Administrative Security Program, dated April 25, 2011. (Note: This Section addresses information that is classified *prior to* its association with the Rewards Programs. Information classified *because of* its association with the Rewards Program is discussed in Section 11.1.A(3)(b).)

B. E-mails Containing or Transmitting FOUO/LES.

E-mails containing FOUO/LES information (but not containing classified information) or transmitting proposals that are marked “FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE” must be transmitted by one of the following methods:

(b)(7)(E)

## MARKING REQUIREMENTS - SUMMARY

HSI MARKING REQUIREMENTS	
SPECIAL AGENT	
<p><b>Draft Proposals:</b></p> <p><u>Containing Classified Information:</u> (Apply <b>ONLY IF</b> classified <u>prior to its association with the Rewards Programs</u>)</p> <ul style="list-style-type: none"> <li>▪ <b>Overall classification level</b> at the top and bottom of each page</li> <li>▪ <b>Portion markings preceding each portion:</b> <ul style="list-style-type: none"> <li>– At the appropriate classification level if portion contains classified information</li> <li>– “(U)(FOUO-LES)” if portion contains unclassified investigative information that is FOUO and LES</li> <li>– “(U)(FOUO)” if portion contains unclassified information that is FOUO but is not LES</li> <li>– Other SBU portion markings, if appropriate</li> <li>– “(U)” if portion contains <b>ONLY</b> unclassified information</li> </ul> </li> <li>▪ <b>Classifier markings:</b></li> </ul> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">(b)(7)(E)</div>	<p><b>Supplemental E-mails:</b></p> <p><u>Containing Classified Information:</u> (Apply <b>ONLY IF</b> classified <u>prior to its association with the Rewards Programs</u>)</p> <ul style="list-style-type: none"> <li>▪ <b>Overall classification level</b> at the top and bottom of the e-mail</li> <li>▪ <b>Portion markings preceding each portion:</b> <ul style="list-style-type: none"> <li>– At the appropriate classification level if portion contains classified information</li> <li>– “(U)(FOUO-LES)” if portion contains unclassified investigative information that is FOUO and LES</li> <li>– “(U)(FOUO)” if portion contains unclassified information that is FOUO but is not LES</li> <li>– Other SBU portion markings, if appropriate</li> <li>– “(U)” if portion contains <b>ONLY</b> unclassified information</li> </ul> </li> <li>▪ <b>Classifier markings:</b> (b)(7)(E)</li> </ul> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">(b)(7)(E)</div>
Containing <b>ONLY</b> Unclassified Information:	
<ul style="list-style-type: none"> <li>▪ <b>“FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE”</b> across the bottom of each page</li> <li>▪ “(U)(FOUO-LES)” preceding each portion that contains investigative information that is FOUO and LES</li> <li>▪ “(U)(FOUO)” if portion contains unclassified information that is FOUO but is not LES</li> <li>▪ Other SBU portion markings, if appropriate</li> <li>▪ “(U)” if portion contains <b>ONLY</b> unclassified information</li> <li>▪ <b>FOUO-LES Warning Statement</b> at the bottom of the front page</li> </ul>	<ul style="list-style-type: none"> <li>▪ <b>“FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE”</b> across the top and bottom of the e-mail</li> <li>▪ “(U)(FOUO-LES)” preceding each portion that contains investigative information that is FOUO and LES</li> <li>▪ “(U)(FOUO)” if portion contains unclassified information that is FOUO but is not LES</li> <li>▪ Other SBU portion markings, if appropriate</li> <li>▪ “(U)” if portion contains <b>ONLY</b> unclassified information</li> <li>▪ <b>FOUO-LES Warning Statement</b> at the bottom of the e-mail</li> </ul>
DOS MARKING REQUIREMENTS	
SUPERVISOR	
<p><b>Final Proposals:</b></p> <ul style="list-style-type: none"> <li>▪ <b>“SECRET/NOFORN”</b> at the top and bottom of each page</li> <li>▪ <b>Portion markings preceding each portion:</b> <ul style="list-style-type: none"> <li>– “(S/NF)” if portion contains classified information</li> <li>– “(S/NF)” if portion contains information that could be used to identify the confidential informant</li> <li>– “(U)(FOUO-LES)” if portion contains unclassified investigative information that is FOUO and LES</li> <li>– “(U)(FOUO)” if portion contains unclassified information that is FOUO but is not LES</li> <li>– Other SBU portion markings, if appropriate</li> <li>– “(U)” if portion contains <b>ONLY</b> unclassified information</li> </ul> </li> <li>▪ <b>Classifier markings:</b></li> </ul> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">(b)(7)(E)</div>	<p><b>Supplemental E-mails:</b></p> <p><u>Sent to INL or Containing Classified Information:</u></p> <ul style="list-style-type: none"> <li>▪ <b>“SECRET/NOFORN”</b> at the top and bottom of the e-mail</li> <li>▪ <b>Portion markings preceding each portion:</b> <ul style="list-style-type: none"> <li>– “(S/NF)” if portion contains classified information</li> <li>– “(S/NF)” if portion contains information that could be used to identify the confidential informant</li> <li>– “(U)(FOUO-LES)” if portion contains unclassified investigative information that is FOUO and LES</li> <li>– “(U)(FOUO)” if portion contains unclassified information that is FOUO but is not LES</li> <li>– Other SBU portion markings, if appropriate</li> <li>– “(U)” if portion contains <b>ONLY</b> unclassified information</li> </ul> </li> <li>▪ <b>Classifier markings:</b></li> </ul> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;">(b)(7)(E)</div>
<p><b>FOUO-LES Warning Statement:</b></p> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p><b>WARNING:</b> This document has been designated Department of Homeland Security (DHS) LAW ENFORCEMENT SENSITIVE by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), and must be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS and ICE policy relating to LAW ENFORCEMENT SENSITIVE information.</p> <p><i>This information may not be distributed beyond the original addressees without prior authorization of HSI.</i></p> </div>	<p><u>Sent to Special Agent:</u></p> <ul style="list-style-type: none"> <li>▪ <b>“FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE”</b> across the top and bottom of the e-mail</li> <li>▪ “(U)(FOUO-LES)” preceding each portion that contains investigative information that is FOUO and LES</li> <li>▪ “(U)(FOUO)” if portion contains unclassified information that is FOUO but is not LES</li> <li>▪ Other SBU portion markings, if appropriate</li> <li>▪ “(U)” if portion contains <b>ONLY</b> unclassified information</li> <li>▪ <b>FOUO-LES Warning Statement</b> at the bottom of the e-mail</li> </ul>



**FACTORS TO CONSIDER WHEN DETERMINING REWARD AMOUNT**

This chart provides details on factors to be considered when evaluating a proposed narcotics reward amount.

Value of the individual caught (Major Violators of U.S. Narcotics Law)	Value of information with respect of capturing or killing the wanted criminal	Risk to informant's life or family as a result of providing information	Willingness to provide information	Was the informant involved in illegal acts	Other forms of compensation
(b)(7)(E)					

**NATIONAL SECURITY INVESTIGATIONS  
HANDBOOK**

**Table of Contents**

**Chapter 1. PURPOSE AND SCOPE.....1**

**Chapter 2. INTRODUCTION .....1**

**Chapter 3. DEFINITIONS.....2**

- 3.1 Automated Biometric Identification System .....2
- 3.2 Central Index System.....2
- 3.3 Electronic System for Travel Authorization .....2
- 3.4 Enforcement Integrated Database .....2
- 3.5 Foreign Terrorist Organizations.....2
- 3.6 Joint Vetting Unit.....3
- 3.7 National Security Entry/Exit Registration System .....3
- 3.8 National Security Interest .....3
- 3.9 Significant Event Notification .....3
- 3.10 Student and Exchange Visitor Information System.....3
- 3.11 Terrorist Identities Datamart Environment.....4
- 3.12 Triggering Event .....4
- 3.13 United States Visitor and Immigrant Status Indicator Technology .....4

**Chapter 4. AUTHORITIES/REFERENCES .....4**

- 4.1 Statutory Authorities Related to National Security Investigations .....4
- 4.2 Specific Criminal Charges Used in National Security Investigations .....6
- 4.3 General and ICE-Specific Criminal Charges Used in National Security Investigations.....6
- 4.4 National Security-Related Administrative Charges.....8
- 4.5 References.....8

**Chapter 5. RESPONSIBILITIES.....10**

- 5.1 Executive Associate Director, Homeland Security Investigations .....10
- 5.2 Special Agents in Charge.....10
- 5.3 Special Agents .....10

**Chapter 6. NATIONAL SECURITY INVESTIGATIVE PRIORITIES AND PROGRAMS .....10**

- 6.1 National Security Investigative Priorities .....10
- 6.2 Post September 11, 2001, Congress Mandated Programs .....12
- 6.3 Terrorist Identities Datamart Environment.....13
- 6.4 National Security Law Section, Office of the Principal Legal Advisor ....16
- 6.5 Overseas Coordination in Support of National Security Investigations ....17

**Chapter 7. CONDUCTING TERRORISM OR NATIONAL SECURITY INVESTIGATIONS.....17**

- 7.1 Field Coordination with Headquarters on National Security Investigations .....17
- 7.2 Investigative Case Management .....18
- 7.3 Investigative Methods/Strategies Relating to National Security Investigations .....21
- 7.4 Initiating a National Security Investigation .....21
- 7.5 Information Security Considerations on a National Security Investigation.....23
- 7.6 Collaboration with Federal, State, and Local Government, Police Agencies, and Task Force Officers .....23
- 7.7 Identifying Potential Immigration Violations on National Security Investigations .....23
- 7.8 Managing Foreign Government-Related Information in Furtherance of a National Security Investigation .....23
- 7.9 (b)(7)(E)
- 7.10 Engaging the U.S. Attorney’s Office and the Local Office of the Chief Counsel in National Security Investigations .....24
- 7.11 Considerations When Interviewing and Taking Statements on Information Related to National Security Investigations.....24
- 7.12 Considerations on National Security Investigations Regarding Individuals Who Are Nonimmigrants.....24
- 7.13 Other Investigative Activity in Furtherance of a National Security Investigation .....25
- 7.14 JTTF Cooperative Target Designation Protocol .....25
- 7.15 Immigration or Document Fraud Schemes and National Security Investigations .....26
- 7.16 Headquarters-Led Antiterrorism and National Disruptive Efforts .....26
- 7.17 Classified Information in National Security Investigations.....26
- 7.18 Investigative Tools to Consider in National Security Investigations.....27

**Chapter 8. DEPARTMENT OF STATE COUNTERTERRORISM OFFICE .....28**

- 8.1 Identification and Designation of Foreign Terrorist Organizations.....28
- 8.2 Department of State Procedures for Designating a Group as a Foreign Terrorist Organization .....28
- 8.3 Legal Criteria for Designation as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act, as Amended .....29
- 8.4 Legal Ramifications of Designation as a Foreign Terrorist Organization.....29
- 8.5 Other Effects of Designation as a Foreign Terrorist Organization .....30
- 8.6 Terrorist Exclusion List .....30
- 8.7 Terrorist Exclusion List Designation Criteria.....30
- 8.8 Terrorist Exclusion List Designation Process.....31
- 8.9 Effects of Designation for Those on the Terrorist Exclusion List .....31

**Chapter 9. IMMIGRATION AND NATIONALITY ACT.....33**

- 9.1 Evidence to Be Considered for Security-Related Administrative Removal Grounds .....33
- 9.2 Classified National Security Information/Evidence in Administrative Adjudicative Proceedings .....34
- 9.3 The Effect of the Real ID Act of 2005 on the Immigration and Nationality Act (INA) Relating to INA Definitions .....35
- 9.4 Section 212(a)(3)(B)(iii) of the Immigration and Nationality Act, Terrorist Activities .....35
- 9.5 Definition of a Terrorist Organization in the Immigration and Nationality Act.....36

**Chapter 10. FOREIGN INTELLIGENCE SURVEILLANCE ACT AND THE FOREIGN INTELLIGENCE SURVEILLANCE COURT .....37**

- 10.1 Relevant Definitions .....37
- 10.2 United States Foreign Intelligence Surveillance Court.....38
- 10.3 Foreign Intelligence Surveillance Act Applications .....38
- 10.4 Minimization Procedures .....38
- 10.5 Uses of Foreign Intelligence Information .....39
- 10.6 FISA Authority vs. Court-Overseen Criminal Investigatory Surveillance Techniques .....39
- 10.7 FISA, Counterintelligence, and Law Enforcement.....40
- 10.8 Considerations of FISA Implications for U.S. Persons and Non-U.S. Persons.....40
- 10.9 FISA Usage in Domestic Terrorist or Racketeering Enterprise Investigations .....40

- 10.10 Emergency FISA Applications .....40
- 10.11 FISA Application in “Lone Wolf” Situations.....41

**Chapter 11. BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC DEVICES .....41**

- 11.1 Background.....41
- 11.2 Authorities.....42
- 11.3 Border Searches by HSI Special Agents.....42
- 11.4 Chain of Custody .....42
- 11.5 Demands for Assistance.....43
- 11.6 Information Sharing .....43

**Chapter 12. JOINT TERRORISM TASK FORCE PARTICIPATION .....44**

- 12.1 JTTF Background .....44
- 12.2 JTTF Commitment.....45
- 12.3 JTTF Reduction in Staffing Requests .....45
- 12.4 JTTF Investigations Predicated on ICE Information .....45
- 12.5 JTTF Investigations Predicated on FBI Information or Investigations in Which ICE Violations Are Predicate Offenses .....45
- 12.6 MOUs and MOAs Pertaining to ICE’s Participation in the JTTF .....46
- 12.7 National Security Letters .....46
- 12.8 FBI National Security Requests for Alien File Review.....46
- 12.9 SAC Assignment of JTTF Representatives for National Security-Related Alien File Review .....47

**APPENDICES**

Appendix A	National Security Investigative Development Worksheet.....	A-i
Appendix B	Designated Foreign Terrorist Organizations.....	B-i
Appendix C	Terrorist Exclusion List .....	C-i
Appendix D	National Joint Terrorism Task Force Membership Designation Criteria .....	D-i
Appendix E	Acronyms.....	E-i

### 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];

## **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



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) (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

## 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) case 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)

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)

(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 predicated 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)

### **7.10 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 predicated 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)(7)(E)

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) 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

(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:

## 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

(b)(7)(E)

## 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

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

## 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

**NATIONAL SECURITY  
INVESTIGATIVE DEVELOPMENT WORKSHEET**

(b)(7)(E)



## 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)

**C. Liaison:** (b)(7)(E)

(b)(7)(E)

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