



Homeland Security Investigations

Narcotics and Transnational Organized Crime Rewards Programs Handbook

HSI HB 16-03 / August 11, 2016



U.S. Immigration
and Customs
Enforcement

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

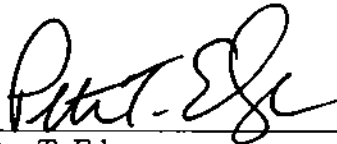
Foreword

The Narcotics and Transnational Organized Crime Rewards Programs Handbook provides a single source of national policies, procedures, responsibilities, guidelines, and controls to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents when recommending informants for participation in the Department of State (DOS)'s Rewards Programs. This Handbook contains instructions and guidance to help ensure uniformity and operational consistency among all HSI field offices. Oversight over ICE's submissions to and interactions with the Rewards Programs resides with the Unit Chief, Undercover Operations Unit.

This is the originating and establishing HSI Handbook on HSI's participation in the DOS Narcotics and Transnational Organized Crime Rewards Programs.

The Narcotics and Transnational Organized Crime Rewards Programs Handbook is an internal policy of HSI. It is not intended, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter, nor are any limitations hereby placed on otherwise lawful enforcement prerogatives of ICE. This Handbook is For Official Use Only (FOUO) – Law Enforcement Sensitive. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and the ICE Directive on Safeguarding Law Enforcement Sensitive Information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Records and Disclosure Unit, as well as the appropriate ICE Counsel and/or U.S. Attorney, should be consulted so that appropriate measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure pursuant to the law enforcement privilege. Any further request for disclosure of this Handbook or information contained herein should be referred to the HSI Records and Disclosure Unit.

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



Peter T. Edge
Executive Associate Director
Homeland Security Investigations

11 AUG 2016
Date

NARCOTICS AND TRANSNATIONAL ORGANIZED CRIME REWARDS PROGRAMS HANDBOOK

Table of Contents

Chapter 1.	PURPOSE AND SCOPE	1
Chapter 2.	INTRODUCTION	1
Chapter 3.	DEFINITIONS	1
• 3.1	Chief of Mission	1
• 3.2	Chargé(e) d’Affaires	2
• 3.3	Classified Information	2
• 3.4	(b)(7)(E)	2
• 3.5	2
• 3.6	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
Chapter 4.	AUTHORITIES/REFERENCES	5
Chapter 5.	RESPONSIBILITIES	5
• 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	(b)(7)(E)	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

Chapter 6.	(b)(7)(E)	7
Chapter 7. PREPARING AND TRANSMITTING PROPOSALS FOR REWARD PAYMENTS		7
Chapter 8. NARCOTICS REWARDS PROGRAM		8
• 8.1	Narcotics Reward Offer and Payment Proposal Format	9
• 8.2	(b)(7)(E)	11
Chapter 9. TRANSNATIONAL ORGANIZED CRIME REWARDS PROGRAM		12
• 9.1	Reward Offer Proposal Format	12
• 9.2	Reward Payment Proposal Format	15
Chapter 10. HSI MARKING REQUIREMENTS		18
• 10.1	(b)(7)(E)	18
• 10.2		21
• 10.3		22
Chapter 11. DOS BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS MARKING REQUIREMENTS		24
• 11.1	Final Proposal	24
• 11.2	E-mails Transmitting Supplemental Information to INL	27
Chapter 12. TRANSMISSION REQUIREMENTS		29
• 12.1	HSI Transmission Requirements	29
• 12.2	DOS INL Transmission Requirements	29
 APPENDICES			
Appendix A	(b)(7)(E)	A-i
Appendix B		B-i
Appendix C	Acronyms	C-i

NARCOTICS AND TRANSNATIONAL ORGANIZED CRIME REWARDS PROGRAMS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Narcotics and Transnational Organized Crime Rewards Programs Handbook provides policy and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) managers, supervisors, and Special Agents (SAs) when submitting an HSI confidential informant (CI) for a reward under the Department of State (DOS)'s Bureau of International Narcotics and Law Enforcement Affairs (INL) Narcotics Rewards Program (NRP) or Transnational Organized Crime Rewards Program (TOCRP) (collectively "Rewards Programs").

Chapter 2. INTRODUCTION

Under Section 36 of the Department of State Basic Authorities Act of 1956 (P.L. 84-885), as amended (Title 22, United States Code (U.S.C.), Section 2708 *et seq.*), Congress provided the authority for DOS to establish several rewards programs, including rewards programs focusing on foreign narcotics trafficking and transnational organized crime. The purpose of this authority was to provide additional tools to help the U.S. Government identify, locate, and bring to justice major violators of U.S. narcotics and transnational organized crime laws.

DOS INL administers both rewards programs and provides policy guidance, as needed. Under the Rewards Programs, the submission and approval of reward proposals consist of two distinct steps: 1) Reward Offer and 2) Reward Payment. The HSI Confidential Informants and Investigative Section, Undercover Operations Unit (UOU), oversees ICE's submissions to and interactions with the Rewards Programs, ensuring that all reward proposal submissions are appropriate and meet the requirements established by DOS INL.

Chapter 3. DEFINITIONS

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

3.1 Chief of Mission

The Chief of Mission, under the direction of the President of the United States and designated by the Secretary of State, is the principal officer in charge, or the Ambassador, of a diplomatic mission of the United States or of a U.S. office in a foreign country. The Chief of Mission is fully responsible for the direction, coordination, and supervision of all U.S. Government employees within the Executive Branch assigned to that diplomatic mission and is informed of their activities and operations.

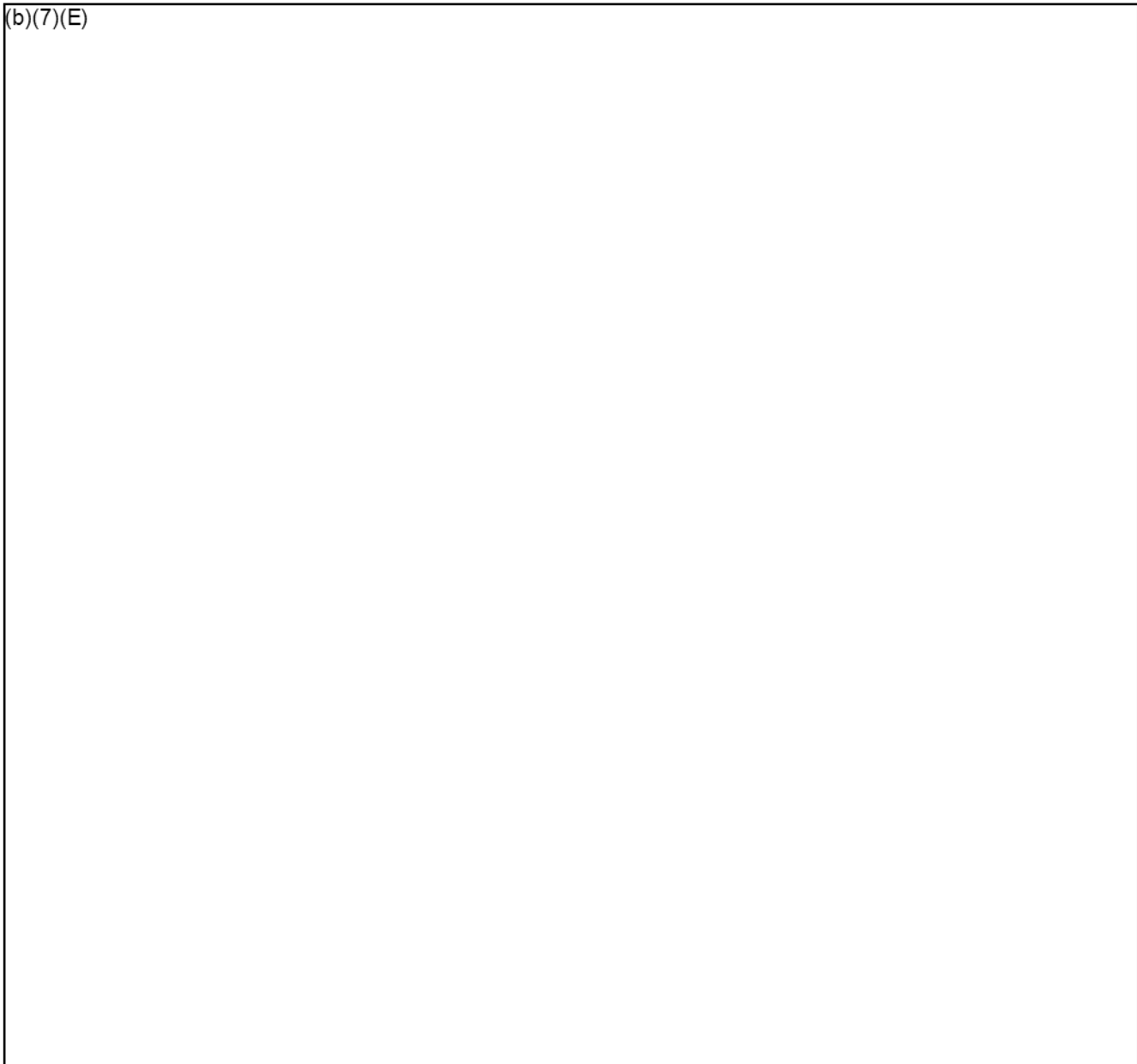
3.2 Chargé(e) d’Affaires

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.

(b)(7)(E)



(b)(7)(E)

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.)

3.12 Rewards Committees

INL manages the NRP in consultation with the Narcotics Rewards Committee (NRC), and the TOCRP in consultation with the Interagency Rewards Committee (IRC). The NRC members are the INL Assistant Secretary of State (Chair), representatives from the Department of Justice (DOJ), Department of the Treasury (Treasury), DHS, including ICE HSI, and other relevant federal law enforcement agencies and DOS regional bureaus. The IRC members are DOS (INL, the Office of the Legal Advisor's Office of Law Enforcement and Intelligence, and the Office of Emergencies in the Diplomatic and Consular Service), DHS, ICE HSI, DOJ, Federal Bureau of Investigation, Drug Enforcement Administration, Department of the Treasury, Internal Revenue Service, National Security Council, Office of the Director of National Intelligence, Central Intelligence Agency, and Department of Defense. In addition to these permanent members, other U.S. Federal agencies or DOS bureaus may be invited to participate on an *ad hoc* basis.

Eligible NRP or TOCRP nominations are submitted to the NRC or IRC, respectively, for concurrence. The IRC must unanimously recommend approval of both the reward offer and the amount requested; the IRC may agree to change the amount. For the NRP, the NRC makes specific reward payment recommendations to the Secretary of State, who, in turn, must obtain the concurrence of the Attorney General (in cases where there is U.S. criminal jurisdiction). For the TOCRP, once the IRC reaches a consensus, TOCRP seeks internal DOS clearance and forwards the nomination to the INL Assistant Secretary with a recommendation for approval or denial.

3.13 Reward Offer

A Reward Offer is an authorization from the Secretary of State to post and publicize a monetary reward. An authorized Reward Offer enables HSI SAs to offer a reward for information that can lead to the arrest and/or conviction of targets, identification or location of key leaders, dismantling of a major narcotics trafficking ring or transnational criminal organization, or disruption of financial mechanisms of networks in cases involving narcotics-related offenses committed primarily outside the United States, or, in cases of transnational organized crime, involving at least one jurisdiction outside the United States. This can be accomplished by HSI or DOS posting reward offers on the internet, social media (e.g., Twitter and Facebook) and/or advertising them through other means, such as TV, radio, and posters.

3.14 Reward Payment

A Reward Payment is a payment for information related to the target of a Reward Offer. The Secretary of State may approve a reward payment to an HSI CI in cases involving at least one jurisdiction outside the United States, based on the receipt of information that disrupts significant criminal activity or leads to the dismantling of a major narcotics trafficking ring or transnational criminal organization. Examples of outcomes that may merit a reward payment include, but are not limited to, the arrest and/or conviction of a key leader or the dismantling of a transnational criminal organization that pose a threat to U.S. national interests.

3.15 Sensitive But Unclassified Information

Sensitive But Unclassified Information (SBU) is an umbrella term used to refer to the many different types of information that both Congress and Federal agencies have determined require some form of protection from unauthorized disclosure. SBU includes information protected by statute (e.g., Sensitive Security Information (SSI) and Protected Critical Infrastructure Information (PCII)) and DHS policy (e.g., FOUO).

Chapter 4. AUTHORITIES/REFERENCES

- A. Title 22, U.S. Code, Chapter 38, Section 2708, Department of State Rewards Program.
- B. Title 32, Code of Federal Regulations, Part 2001, “Classified National Security Information” – contains supplemental requirements for identifying and safeguarding classified information.
- C. EO 13526, Classified National Security Information – contains requirements for identifying and safeguarding classified information.
- D. DHS Instruction 121-01-011, Administrative Security Program, dated April 25, 2011 – contains requirements for identifying and safeguarding classified information by DHS Components.
- E. DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, dated January 6, 2005 – contains requirements for identifying and safeguarding FOUO and LES information.
- F. ICE Directive 4003.2, Safeguarding Law Enforcement Sensitive Information, dated May 20, 2014, or as updated – contains requirements for identifying and safeguarding LES information.
- G. DOS, Narcotics Reward Payment Request Guidance, dated February 2013.
- H. DOS, Transnational Organized Crime Rewards Program Standard Operating Procedure, dated August 29, 2014.

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

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

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.

(b)(7)(E)

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.

(b)(7)(E)

Chapter 7. PREPARING AND TRANSMITTING PROPOSALS FOR REWARD PAYMENTS

The following procedures must be followed when requesting reward payments:

(b)(7)(E)

(b)(7)(E)

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.")

(b)(7)(E)

(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:

(b)(7)(E)

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

validation. The IRC must unanimously agree on the proposed reward amount in order for the case to move forward. DOS provides a criteria checklist to assist in determining the initial reward proposal. (Note: For more information about the criteria checklist, SAs should contact the Rewards Program NPM.)

Chapter 9. TRANSNATIONAL ORGANIZED CRIME REWARDS PROGRAM

Established by Congress in 2013, the TOCRP is a tool used by the U.S. Government to identify, locate, and bring to justice members of significant transnational criminal organizations. Under this program and subject to the availability of appropriated funds, the Secretary of State has statutory authority (22 U.S.C. § 2708) to offer rewards for information leading to the dismantling of transnational criminal organizations or the disruption of their finances, the identification or location of key leaders, or the arrest and/or conviction of significant members operating outside the United States.

Any U.S. federal agency may nominate an individual or organization for a TOCRP reward offer of up to \$25 million. Per DOS policy and for the purpose of this Handbook, HSI reward offers and payment requests may not exceed \$5 million. The IRC must unanimously recommend approval of both the reward offer and the amount requested; the IRC may determine that a different award amount is appropriate. Once the IRC reaches a consensus, TOCRP 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.

9.1 Reward Offer Proposal Format

The following format, including section headings, will be used for all Transnational Organized Crime reward offer proposals. All nomination proposals for reward offers must include the requestor's (SA) name, rank, office location, and contact information, including phone number and email address.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(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.

(b)(7)(E)

(b)(7)(E)

(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.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

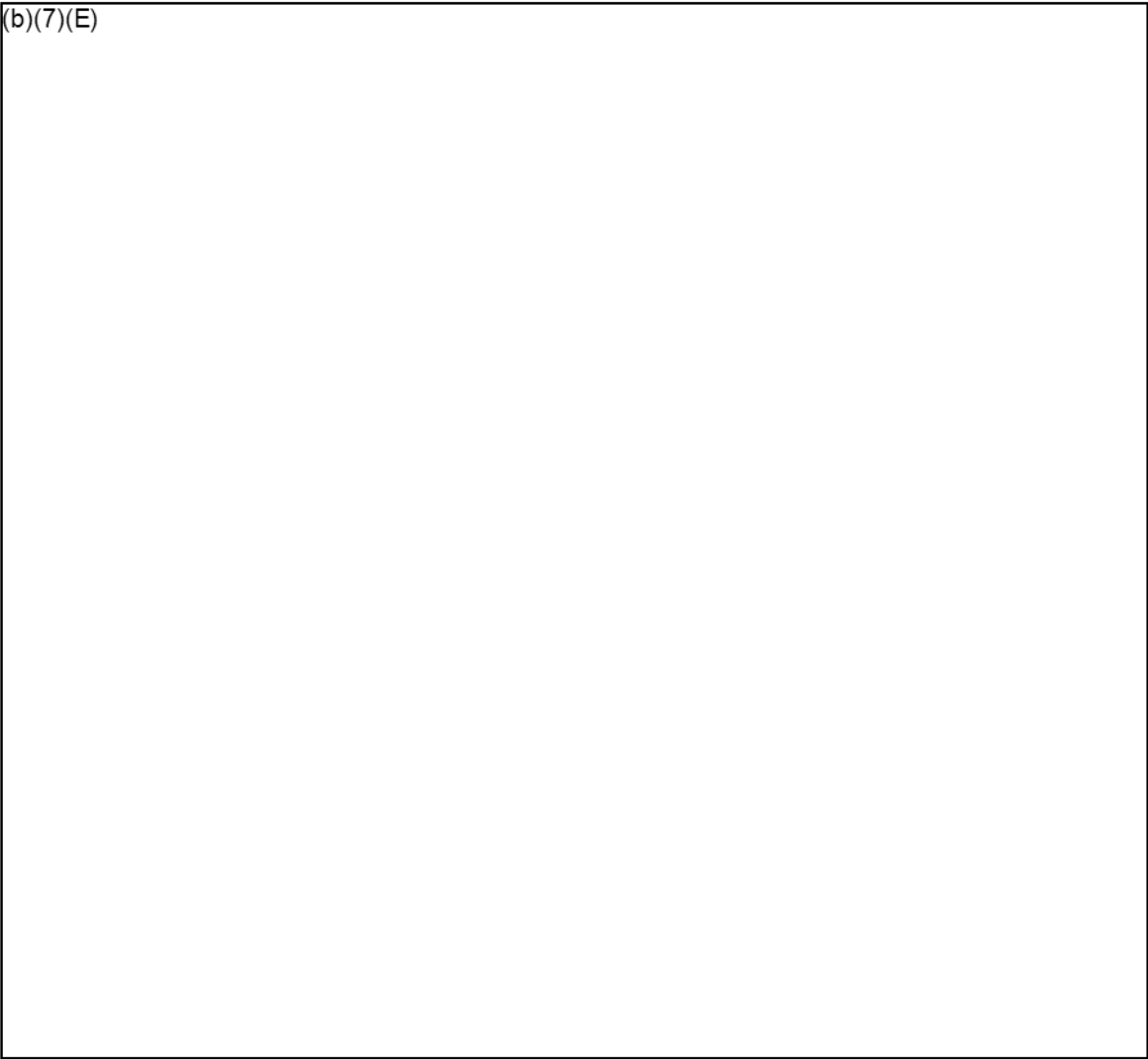
Chapter 11. DOS BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS MARKING REQUIREMENTS

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:

(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

(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.

(b)(7)(E)

(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)

(b)(7)(E)

12.2 DOS INL Transmission Requirements

The final proposal and supplemental e-mails must be transmitted to INL via (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

ACRONYMS

CI	Confidential Informant
CPOT	Consolidated Priority Organization Target
DAD	Deputy Assistant Director
DHS	U.S. Department of Homeland Security
DOJ	Department of Justice
DTO	Drug Trafficking Organization
DOS	Department of State
EO	Executive Order
FGI	Foreign Government Information
FOUO	For Official Use Only
GS	Group Supervisor
HB	Handbook
HSDN	Homeland Secure Data Network
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
INL	Bureau of International Narcotics and Law Enforcement Affairs
INTERPOL	International Criminal Police Organization
IRC	Interagency Rewards Committee
ISD	Investigative Services Division
LES	Law Enforcement Sensitive
NF	Not Releasable to Foreign Nationals
NOFORN	Not Releasable to Foreign Nationals
NPM	National Program Manager
NRC	Narcotics Rewards Committee
NRP	Narcotics Rewards Program
OPR	Office of Professional Responsibility
PCII	Protected Critical Infrastructure Information
RPP	Rewards Program Participant
SA	Special Agent
SAC	Special Agent in Charge
SBU	Sensitive But Unclassified
SCG	Security Classification Guide
SIPRNet	Secret Internet Protocol Router Network
SSI	Sensitive Security Information
TOCRP	Transnational Organized Crime Rewards Program
UOU	Undercover Operations Unit
U.S.C.	United States Code



Homeland Security Investigations

National Security Investigations Handbook

HSI HB 13-03 / April 26, 2013



U.S. Immigration
and Customs
Enforcement

~~FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE~~


Foreword

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

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

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

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


James A. Dinkins
Executive Associate Director
Homeland Security Investigations

4/26/2013
Date

**NATIONAL SECURITY INVESTIGATIONS
HANDBOOK**

Table of Contents

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

Chapter 2. INTRODUCTION1

Chapter 3. DEFINITIONS.....2

- 3.1 Automated Biometric Identification System2
- 3.2 Central Index System.....2
- 3.3 Electronic System for Travel Authorization2
- 3.4 Enforcement Integrated Database2
- 3.5 Foreign Terrorist Organizations.....2
- 3.6 Joint Vetting Unit.....3
- 3.7 National Security Entry/Exit Registration System3
- 3.8 National Security Interest3
- 3.9 Significant Event Notification3
- 3.10 Student and Exchange Visitor Information System.....3
- 3.11 (b)(7)(E)4
- 3.12 Triggering Event4
- 3.13 United States Visitor and Immigrant Status Indicator Technology4

Chapter 4. AUTHORITIES/REFERENCES4

- 4.1 Statutory Authorities Related to National Security Investigations4
- 4.2 Specific Criminal Charges Used in National Security Investigations6
- 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 Investigations10
- 5.2 Special Agents in Charge.....10
- 5.3 Special Agents10

Chapter 6. NATIONAL SECURITY INVESTIGATIVE PRIORITIES AND PROGRAMS10

- 6.1 National Security Investigative Priorities10
- 6.2 Post September 11, 2001, Congress Mandated Programs12
- 6.3 (b)(7)(E)13
- 6.4 National Security Law Section, Office of the Principal Legal Advisor16
- 6.5 Overseas Coordination in Support of National Security Investigations17

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

- 7.1 Field Coordination with Headquarters on National Security Investigations17
- 7.2 (b)(7)(E)18
- 7.3 Investigative Methods/Strategies Relating to National Security Investigations21
- 7.4 (b)(7)(E)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 Officers23
- 7.7 Identifying Potential Immigration Violations on National Security Investigations23
- 7.8 Managing Foreign Government-Related Information in Furtherance of a National Security Investigation23
- 7.9 (b)(7)(E)23
- 7.10 Engaging the U.S. Attorney’s Office and the Local Office of the Chief Counsel in National Security Investigations24
- 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 (b)(7)(E)25
- 7.14 JTF Cooperative Target Designation Protocol25
- 7.15 (b)(7)(E)26
- 7.16 Headquarters-Led Antiterrorism and National Disruptive Efforts26
- 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 OFFICE28

- 8.1 (b)(7)(E)28
- 8.2 Department of State Procedures for Designating a Group as a Foreign Terrorist Organization28
- 8.3 Legal Criteria for Designation as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act, as Amended29
- 8.4 Legal Ramifications of Designation as a Foreign Terrorist Organization.....29
- 8.5 Other Effects of Designation as a Foreign Terrorist Organization30
- 8.6 Terrorist Exclusion List30
- 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 List31

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

- 9.1 Evidence to Be Considered for Security-Related Administrative Removal Grounds33
- 9.2 Classified National Security Information/Evidence in Administrative Adjudicative Proceedings34
- 9.3 The Effect of the Real ID Act of 2005 on the Immigration and Nationality Act (INA) Relating to INA Definitions35
- 9.4 Section 212(a)(3)(B)(iii) of the Immigration and Nationality Act, Terrorist Activities35
- 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 COURT37

- 10.1 Relevant Definitions37
- 10.2 United States Foreign Intelligence Surveillance Court.....38
- 10.3 Foreign Intelligence Surveillance Act Applications38
- 10.4 Minimization Procedures38
- 10.5 Uses of Foreign Intelligence Information39
- 10.6 FISA Authority vs. Court-Overseen Criminal Investigatory Surveillance Techniques39
- 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 Investigations40

- 10.10 Emergency FISA Applications40
- 10.11 FISA Application in “Lone Wolf” Situations.....41

Chapter 11. BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC DEVICES41

- 11.1 Background.....41
- 11.2 Authorities.....42
- 11.3 Border Searches by HSI Special Agents.....42
- 11.4 Chain of Custody42
- 11.5 Demands for Assistance.....43
- 11.6 Information Sharing43

Chapter 12. JOINT TERRORISM TASK FORCE PARTICIPATION44

- 12.1 JTTF Background44
- 12.2 JTTF Commitment.....45
- 12.3 JTTF Reduction in Staffing Requests45
- 12.4 JTTF Investigations Predicated on ICE Information45
- 12.5 (b)(7)(E)45
- 12.6 MOUs and MOAs Pertaining to ICE’s Participation in the JTTF46
- 12.7 (b)(7)(E)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 Review47

APPENDICES

Appendix A	(b)(7)(E)	A-i
Appendix B	Designated Foreign Terrorist Organizations.....	B-i
Appendix C	Terrorist Exclusion List	C-i
Appendix D	(b)(7)(E)	D-i
Appendix E	Acronyms.....	E-i

NATIONAL SECURITY INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

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

Chapter 2. INTRODUCTION

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

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

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

Chapter 3. DEFINITIONS

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

3.1 Automated Biometric Identification System

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

3.2 Central Index System

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

3.3 Electronic System for Travel Authorization

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

3.4 Enforcement Integrated Database

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

3.5 Foreign Terrorist Organizations

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

3.6 Joint Vetting Unit

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

3.7 National Security Entry/Exit Registration System

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

3.8 National Security Interest

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

3.9 Significant Event Notification

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

3.10 Student and Exchange Visitor Information System

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

3.12 Triggering Event

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

3.13 United States Visitor and Immigrant Status Indicator Technology

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

Chapter 4. AUTHORITIES/REFERENCES

4.1 Statutory Authorities Related to National Security Investigations

- A. INA, Title 8, United States Code (U.S.C.), Sections 1101-1574, 1182 (2000), General Classes of Aliens Ineligible to Receive Visas and Ineligible for Admission;
- B. Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, 108 Pub. L. 458, §§ 1021-1023, 118 Stat. 3638, 3825-3832, National Counterterrorism Center (NCTC), National Counter Proliferation Center, and National Intelligence Centers;
- C. *Id.* at § 7215, Terrorist Travel Program;
- D. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 107 Pub. L. 56 §§ 411-418, 418, 115 Stat. 272 (2001) [enhanced immigration provisions];

- E. 8 U.S.C. § 1225, Inspection by Immigration Officers; Expedited Removal of Inadmissible Arriving Aliens;
- F. 8 U.S.C. § 1324, Bringing in and harboring certain aliens;
- G. 8 U.S.C. § 1357, Powers of Immigration Officers and Employees;
- H. 19 U.S.C. § 482, Search of vehicles and persons;
- I. 19 U.S.C. § 507, Assistance for Officers;
- J. 19 U.S.C. § 1401(i), Customs Officers;
- K. 19 U.S.C. § 1461, Inspection of merchandise and baggage;
- L. 19 U.S.C. § 1467, Special inspection, examination, and search;
- M. 19 U.S.C. § 1496, Examination of baggage;
- N. 19 U.S.C. § 1499, Examination of merchandise;
- O. 19 U.S.C. § 1581, Boarding vessels;
- P. 19 U.S.C. § 1582, Search of persons and baggage, regulations;
- Q. 19 U.S.C. § 1583, Examination of outbound mail;
- R. 19 U.S.C. § 1589a, Enforcement authority of customs officers;
- S. 19 U.S.C. § 1595, Searches and seizures;
- T. 31 U.S.C. § 5317, Search authority for compliance with Currency and Monetary Instruments Reporting Act;
- U. Title 8, Code of Federal Regulations (C.F.R.), Section 236.1(e), Privilege of Communication;
- V. 19 C.F.R. Part 145, Mail importations;
- W. 19 C.F.R. Part 162, Inspection, Search, and Seizure; and
- X. 31 C.F.R. § 594.201, Treasury Office of Foreign Assets Control (OFAC) regulations authorize the blocking and seizing of international cargo and goods being imported and exported to Specifically Designated Global Terrorists (SDGTs), companies, and entities of SDGTs.

4.2 Specific Criminal Charges Used in National Security Investigations

- A. 18 U.S.C. § 2332a, Use of weapons of mass destruction;
- B. 18 U.S.C. § 2332b, Acts of terrorism transcending national boundaries;
- C. 18 U.S.C. § 2332d, Financial transactions;
- D. 18 U.S.C. § 2332f, Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities;
- E. 18 U.S.C. § 2332g, Missile systems designed to destroy aircraft;
- F. 18 U.S.C. § 2332h, Radiological dispersal devices;
- G. 18 U.S.C. § 2339, Harboring or concealing terrorists;
- H. 18 U.S.C. § 2339a, Providing material support to terrorists, organizations involved in torture or the recruitment of child soldiers;
- I. 18 U.S.C. § 2339b, Providing material support to a designated foreign terrorist organization; and
- J. 18 U.S.C. § 2339d, Receiving military-type training from a foreign terrorist organization.

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

- A. 8 U.S.C. § 1304(e), Failure to carry proof of permanent residence;
- B. 8 U.S.C. § 1325, Improper Entry by Alien;
- C. 8 U.S.C. § 1325(c), Marriage Fraud;
- D. 8 U.S.C. § 1326, Re-entry after deportation/removal;
- E. 13 U.S.C. § 305, Penalties for unlawful export information activities;
- F. 18 U.S.C. § 371, Conspiracy;
- G. 18 U.S.C. § 542, Entry of goods by means of false statements;
- H. 18 U.S.C. § 545, Smuggling goods into the United States;

- I. 18 U.S.C. § 554, Smuggling goods from the United States;
- J. 18 U.S.C. § 641, Public money, property or records;
- K. 18 U.S.C. § 911, False claims to U.S. citizenship;
- L. 18 U.S.C. § 922(g)(5), Alien unauthorized to possess a firearm;
- M. 18 U.S.C. § 951, Agent of foreign governments;
- N. 18 U.S.C. § 1001, False statements;
- O. 18 U.S.C. § 1015, Fraud and statements regarding naturalization, citizenship or alien registry;
- P. 18 U.S.C. § 1028, Fraud and related activity in connection with identification documents, authentication features, and information;
- Q. 18 U.S.C. § 1425, Naturalization Fraud;
- R. 18 U.S.C. § 1543, Forgery or false use of passport;
- S. 18 U.S.C. § 1546, Visa/Immigration Fraud;
- T. 18 U.S.C. § 1956, Laundering of monetary instruments;
- U. 18 U.S.C. § 1957(a), Engaging in monetary transactions in property derived from specified unlawful activity;
- V. 18 U.S.C. § 1960, Prohibition of unlicensed money transmitting businesses;
- W. 18 U.S.C. § 1961, Racketeer Influenced and Corrupt Organizations;
- X. 18 U.S.C. § 2320, Trafficking in counterfeit goods or services;
- Y. 22 U.S.C. § 401, Shipping Export Declaration, Violation;
- Z. 22 U.S.C. § 611, Unregistered Agent of a Foreign Government;
- AA. 22 U.S.C. § 2778, Conspiracy to violate the Arms Export Control Act;
- BB. 31 U.S.C. § 5324, Structuring transactions to evade reporting requirement prohibited;
- CC. 31 U.S.C. § 5332, Bulk cash smuggling into or out of the United States;

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

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

4.4 National Security-Related Administrative Charges

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

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

4.5 References

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

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

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

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

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

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

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

- G. HSPD 19 establishes a national policy on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States. It mandates that the Secretary of Homeland Security coordinate with other federal agencies to maintain secure information-sharing systems.
- H. HSPD 24 establishes a framework to ensure that federal executive departments and agencies use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric information.
- I. IRTPA of 2004, 108 Pub. L. 458, §§ 1021-1023, 118 Stat. 3638, 3825-3832. NCTC, National Counter Proliferation Center, and National Intelligence Centers.
- J. *Id.* at § 7215. Terrorist Travel Program.
- K. ICE Directive 7-6.0, “Border Searches of Documents and Electronic Media” (July 16, 2008, or as updated). (Superseded by ICE Directive 7-6.1 only as it relates to electronic devices.)
- L. ICE Directive 10044.1 (former number: 7-6.1), “Border Searches of Electronic Devices” (August 18, 2009, or as updated).
- M. HSI Directive 12-02, “Terrorist Identities Datamart Environment” (October 19, 2012, or as updated).
- N. ICE Memorandum (Policy #10031.1), “Use of Joint Vetting Unit to Coordinate Terrorist Financing Investigations” (August 24, 2007, or as updated).
- O. ICE Memorandum (Policy #10068.1), “DHS Guidance Regarding Polygraph Examinations of ICE Officers Assigned to the FBI Joint Terrorist Task Forces” (January 22, 2007, or as updated).
- P. OI Memorandum, “Border Searches of Electronic Devices Directive” (August 31, 2009, or as updated).
- Q. OI Memorandum, “Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media” (December 12, 2008, or as updated).
- R. OI Memorandum, “Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry” (March 5, 2007, or as updated).

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

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

5.2 Special Agents in Charge

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

5.3 Special Agents

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

Chapter 6. NATIONAL SECURITY INVESTIGATIVE PRIORITIES AND PROGRAMS

(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 integrity (b)(7)(E) The

(b)(7)(E)

C. National Targeting Center

The ICE National Targeting Center (NTC), a Section in NSU, documents all

(b)(7)(E)

(b)(7)(E) The ICE NTC will notify the appropriate SAC or designee if it becomes aware of a subject of interest, investigative activity, or threat in the

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

(b)(7)(E)

D. National Security Integration Center

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

6.2 Post September 11, 2001, Congress Mandated Programs

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

A. National Security Entry/Exit Registration System

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

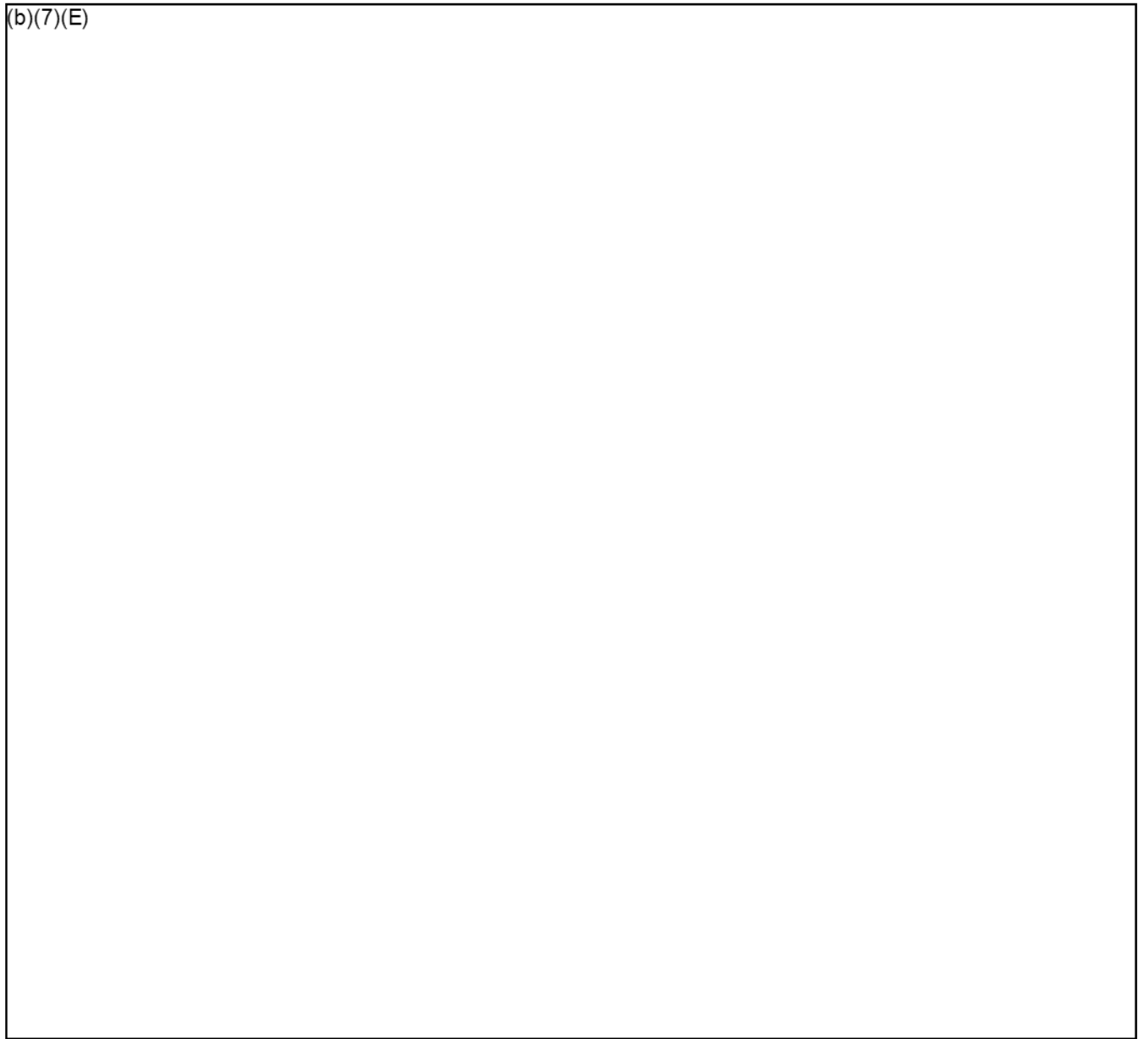
B. Student and Exchange Visitor Information System

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

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

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

(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

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

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

- A. The detention and removal of "special interest" aliens.
- B. The designation of terrorist entities under Title 8.
- C. The civil arrest authority of SAs.
- D. Criminal charges under Titles 8 and 18.
- E. Benefit eligibility.
- F. Denaturalization.

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

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

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

6.5 Overseas Coordination in Support of National Security Investigations

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

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

Chapter 7. CONDUCTING TERRORISM OR NATIONAL SECURITY INVESTIGATIONS

7.1 Field Coordination with Headquarters on National Security Investigations

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

The following categories are defined as national security matters:

- A. Terrorism-related cases/inquiries/allegations: Activity involving an individual who is suspected of being involved in terrorism or a direct or indirect supporter of a terrorist organization.
- B. Other national security cases/inquiries/allegations: Activity involving suspected espionage; engaging in illegal acts involving weapons of mass destruction; being an agent or officer of a hostile foreign intelligence service; or engaging in violations of the import and export laws relating to sensitive information or technology.

(b)(7)(E)

(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.

(b)(7)(E)

(b)(7)(E)

7.5 Information Security Considerations on a National Security Investigation

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

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

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

7.7 Identifying Potential Immigration Violations in National Security Investigations

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

(b)(7)(E)

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

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

(b)(7)(E)

(b)(7)(E)

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

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

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

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

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

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

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(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.

(b)(7)(E)

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

7.18 Investigative Tools to Consider in National Security Investigations

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

(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.)

(b)(7)(E)

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

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

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

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

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

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

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

- A. It must be a *foreign organization*; and
- B. The organization must *engage in terrorist activity*, as defined in section 212 (a)(3)(B) of the INA (8 U.S.C. § 1182(a)(3)(B)), or in *terrorism*, as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (22 U.S.C. § 2656f(d)(2)), *or retain the capability and intent to engage in terrorist activity or terrorism*; and
- C. The organization's terrorist activity must threaten the security of U.S. nationals *or* the national security (national defense, foreign relations, and/or the economic interests) of the United States.

8.4 Legal Ramifications of Designation as a Foreign Terrorist Organization

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

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

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

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

8.5 Other Effects of Designation as a Foreign Terrorist Organization

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

- A. Stigmatizes and isolates the designated terrorist organization internationally.
- B. Deters donations or contributions to, and economic transactions with, the named organization.
- C. Heightens public awareness and knowledge of the terrorist organization.
- D. Signals to other governments U.S. concerns about the designated organization.

8.6 Terrorist Exclusion List

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

8.7 Terrorist Exclusion List Designation Criteria

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

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

- B. Prepares or plans a terrorist activity.
- C. Gathers information on potential targets for terrorist activity.
- D. Provides material support for the commission of terrorist activity to an individual who has committed or plans to commit terrorist activity or to a terrorist organization.
- E. Soliciting funds for a terrorist activity or a terrorist organization.
- F. Soliciting individuals to engage in terrorist activity or for membership in a terrorist organization.

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

8.8 Terrorist Exclusion List Designation Process

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

8.9 Effects of Designation for Those on the Terrorist Exclusion List

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

A. Legal Ramifications for Those on the Terrorist Exclusion List

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

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

- 1) Membership in a TEL-designated organization.
- 2) Use of the alien's position of prominence within any country to persuade others to support an organization on the TEL.
- 3) Solicitation of funds or other items of value for an organization on the TEL.
- 4) Solicitation of any individual for membership in an organization on the TEL.
- 5) Commission of an act that the alien knows, or should have reasonably known, provides material support to an organization on the TEL. Such material support may include the provision of a safe house, transportation, communications, funds, transfer of funds, or other material to obtain financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training.

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

B. Other Effects for Those on the Terrorism Exclusion List

TEL-designation also:

- 1) Deters donation or contributions to the named organizations.
- 2) Heightens public awareness and knowledge of the terrorist organizations.
- 3) Alerts other governments to U.S. concerns about organizations engaged in terrorist activities.
- 4) Stigmatizes and isolates the designated terrorist organizations.

Chapter 9. IMMIGRATION AND NATIONALITY ACT

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

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

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

- A. any activity to violate any law of the United States relating to espionage or sabotage or to violate or evade any law prohibiting the export from the United States of goods, technology, or sensitive information;
- B. any other unlawful activity, such as criminal activity which endangers public safety or national security; or
- C. any activity whose purpose is the opposition to, or the control or overthrow of, the Government of the United States by force, violence, or other unlawful means.

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

- A. has engaged in a terrorist activity,
- B. is a member of a terrorist organization;
- C. has received military-type training from a terrorist organization.

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

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

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

(b)(7)(E)

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

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

9.2 Classified National Security Information/Evidence in Administrative Adjudicative Proceedings

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

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

(b)(7)(E)

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

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

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

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

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

- A. The hijacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle);
- B. The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a government organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained;
- C. A violent attack upon an internationally protected person (as defined in 18 U.S.C. § 1116(b)(4)) or upon the liberty of such a person;
- D. An assassination; and/or
- E. The use of any:
 - 1) Biological agent, chemical agent, or nuclear weapon or device;
 - 2) Explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with the intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property; and/or
- F. A threat, attempt, or conspiracy to do any of the foregoing.

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

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

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

(b)(7)(E)

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

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

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

10.1 Relevant Definitions

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

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

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

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

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

10.2 United States Foreign Intelligence Surveillance Court

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

10.3 Foreign Intelligence Surveillance Act Applications

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

(b)(7)(E)



10.4 Minimization Procedures

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

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

10.5 Uses of Foreign Intelligence Information

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

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

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

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

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

(b)(7)(E)

10.7 FISA, Counterintelligence, and Law Enforcement

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

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

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

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

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

10.9 FISA Usage in Domestic Terrorist or Racketeering Enterprise Investigations

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

10.10 Emergency FISA Applications

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

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

10.11 FISA Application in “Lone Wolf” Situations

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

Chapter 11. BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC DEVICES

11.1 Background

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

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

11.2 Authorities

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

11.3 Border Searches by HSI Special Agents

Border searches must be conducted by HSI SAs or other properly designated Customs Officers, such as law enforcement officers cross-designated by ICE as customs officers (e.g., TFOs), and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.

(b)(7)(E)

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

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

11.4 Chain of Custody

(b)(7)(E)

(b)(7)(E)

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

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

(b)(7)(E)

11.5 Demands for Assistance

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

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

(b)(7)(E)

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

11.6 Information Sharing

HSI SAs acting under border search authority may share information relating to national security with law enforcement and intelligence agencies consistent with the guidelines and applicable laws set forth in ICE Directive 7-6.0, Border Searches of Documents and Electronic Media, dated July 16, 2008, or as updated, and ICE Directive 10044.1 (former number: 7-6.1), Border Searches of Electronic Devices, dated August 18, 2009, or as updated.

(b)(7)(E)

(b)(7)(E)

Chapter 12. JOINT TERRORISM TASK FORCE PARTICIPATION

12.1 JTTF Background

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

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

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

HSI dedicates full-time and part-time SAs to the JTTFs to utilize their unique criminal and administrative authorities and resources in the investigation of national security threats.

(b)(7)(E)

SAs assigned to the JTTFs may be tasked to lead or assist in investigations based on information generated from the FBI or may open a JTTF investigation based on information predicated by ICE. (b)(7)(E)

(b)(7)(E)

12.2 JTTF Commitment

(b)(7)(E)

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

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

12.3 JTTF Reduction in Staffing Requests

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

12.4 JTTF Investigations Predicated on ICE Information

If SAs develop information, either through a lead or during the normal course of an investigation where a demonstrative nexus to terrorism exists, they should refer the investigation to the JTTF. (b)(7)(E)

(b)(7)(E)

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

(b)(7)(E)

(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.

(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

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

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

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

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

DESIGNATED FOREIGN TERRORIST ORGANIZATIONS

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

21. Islamic Movement of Uzbekistan (IMU)
22. Jaish-e-Mohammed (JEM) (Army of Mohammed)
23. Jemaah Anshorut Tauhid (JAT)
24. Jemaah Islamiya organization (JI)
25. Jundallah
26. Kahane Chai (Kach)
27. Kata'ib Hizballah (KH)
28. Kongra-Gel (KGGK, formerly Kurdistan Workers' Party, PKK, KADEK)
29. Lashkar-e Tayyiba (LT) (Army of the Righteous)
30. Lashkar i Jhangvi (LJ)
31. Liberation Tigers of Tamil Eelam (LTTE)
32. Libyan Islamic Fighting Group (LIFG)
33. Moroccan Islamic Combatant Group (GICM)
34. National Liberation Army (ELN)
35. Palestine Liberation Front (PLF)
36. Palestinian Islamic Jihad (PIJ)
37. Popular Front for the Liberation of Palestine (PFLP)
38. PFLP-General Command (PFLP-GC)
39. al-Qaida in Iraq (AQI)
40. al-Qa'ida (AQ)
41. al-Qa'ida in the Arabian Peninsula (AQAP)
42. al-Qaida in the Islamic Maghreb (formerly GSPC)
43. Real IRA (RIRA)

44. Revolutionary Armed Forces of Colombia (FARC)
45. Revolutionary Organization 17 November
46. Revolutionary People's Liberation Party/Front (DHKP/C)
47. Revolutionary Struggle (RS)
48. Shining Path (Sendero Luminoso (SL))
49. United Self-Defense Forces of Colombia (AUC)
50. Harakat-ul Jihad Islami (HUJI)
51. Tehrik-e Taliban Pakistan (TTP)

TERRORIST EXCLUSION LIST

1. Afghan Support Committee (a.k.a. Ahya ul Turas; a.k.a. Jamiat Ayat-ur-Rhas al Islamia; a.k.a. Jamiat Ihya ul Turath al Islamia; a.k.a. Lajnat el Masa Eidatul Afghania)
2. Al Taqwa Trade, Property and Industry Company Ltd. (f.k.a. Al Taqwa Trade, Property and Industry; f.k.a. Al Taqwa Trade, Property and Industry Establishment; f.k.a. Himmat Establishment; a.k.a. Waldenberg, AG)
3. Al-Hamati Sweets Bakeries
4. Al-Ittihad al-Islami (AIAI)
5. Al-Manar
6. Al-Ma'unah
7. Al-Nur Honey Center
8. Al-Rashid Trust
9. Al-Shifa Honey Press for Industry and Commerce
10. Al-Wafa al-Igatha al-Islamia (a.k.a. Wafa Humanitarian Organization; a.k.a. Al Wafa; a.k.a. Al Wafa Organization)
11. Alex Boncayao Brigade (ABB)
12. Anarchist Faction for Overthrow
13. Army for the Liberation of Rwanda (ALIR) (a.k.a. Interahamwe, Former Armed Forces (EX-FAR))
14. Asbat al-Ansar
15. Babbar Khalsa International
16. Bank Al Taqwa Ltd. (a.k.a. Al Taqwa Bank; a.k.a. Bank Al Taqwa)
17. Black Star

18. Continuity Irish Republican Army (CIRA) (a.k.a. Continuity Army Council)
19. Darkazanli Company
20. Dhamat Houmet Daawa Salafia (a.k.a. Group Protectors of Salafist Preaching; a.k.a. Houmat Ed Daawa Es Salifiya; a.k.a. Katibat El Ahoual; a.k.a. Protectors of the Salafist Predication; a.k.a. El-Ahoual Battalion; a.k.a. Katibat El Ahouel; a.k.a. Houmate Ed-Daawa Es-Salafia; a.k.a. the Horror Squadron; a.k.a. Djamaat Houmat Eddawa Essalafia; a.k.a. Djamaatt Houmat Ed Daawa Es Salafiya; a.k.a. Salafist Call Protectors; a.k.a. Djamaat Houmat Ed Daawa Es Salafiya; a.k.a. Houmate el Da'awaa es-Salafiyya; a.k.a. Protectors of the Salafist Call; a.k.a. Houmat ed-Daaoua es-Salafia; a.k.a. Group of Supporters of the Salafiste Trend; a.k.a. Group of Supporters of the Salafist Trend)
21. Eastern Turkistan Islamic Movement (a.k.a. Eastern Turkistan Islamic Party; a.k.a. ETIM; a.k.a. ETIP)
22. First of October Antifascist Resistance Group (GRAPO) (a.k.a. Grupo de Resistencia Anti-Fascista Premero De Octubre)
23. Harakat ul Jihad i Islami (HUJI)
24. International Sikh Youth Federation
25. Islamic Army of Aden
26. Islamic Renewal and Reform Organization
27. Jamiat al-Ta'awun al-Islamiyya
28. Jamiat ul-Mujahideen (JUM)
29. Japanese Red Army (JRA)
30. Jaysh-e-Mohammed
31. Jayshullah
32. Jerusalem Warriors
33. Lashkar-e-Tayyiba (LET) (a.k.a. Army of the Righteous)
34. Libyan Islamic Fighting Group
35. Loyalist Volunteer Force (LVF)

36. Makhtab al-Khidmat
37. Moroccan Islamic Combatant Group (a.k.a. GICM; a.k.a. Groupe Islamique Combattant Marocain)
38. Nada Management Organization (f.k.a. Al Taqwa Management Organization SA)
39. New People's Army (NPA)
40. Orange Volunteers (OV)
41. People Against Gangsterism and Drugs (PAGAD)
42. Red Brigades-Combatant Communist Party (BR-PCC)
43. Red Hand Defenders (RHD)
44. Revival of Islamic Heritage Society (Pakistan and Afghanistan offices -- Kuwait office not designated) (a.k.a. Jamia Ihya ul Turath; a.k.a. Jamiat Ihia Al- Turath Al-Islamiya; a.k.a. Revival of Islamic Society Heritage on the African Continent)
45. Revolutionary Proletarian Nucleus
46. Revolutionary United Front (RUF)
47. Salafist Group for Call and Combat (GSPC)
48. The Allied Democratic Forces (ADF)
49. The Islamic International Brigade (a.k.a. International Battalion, a.k.a. Islamic Peacekeeping International Brigade, a.k.a. Peacekeeping Battalion, a.k.a. The International Brigade, a.k.a. The Islamic Peacekeeping Army, a.k.a. The Islamic Peacekeeping Brigade)
50. The Lord's Resistance Army (LRA)
51. The Pentagon Gang
52. The Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs (a.k.a. Riyadus-Salikhin Reconnaissance and Sabotage Battalion, a.k.a. Riyadh-as-Saliheen, a.k.a. the Sabotage and Military Surveillance Group of the Riyadh al-Salihin Martyrs, a.k.a. Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Shahids (Martyrs))

53. The Special Purpose Islamic Regiment (a.k.a. the Islamic Special Purpose Regiment, a.k.a. the al-Jihad-Fisi-Sabililah Special Islamic Regiment, a.k.a. Islamic Regiment of Special Meaning)
54. Tunisian Combat Group (a.k.a. GCT, a.k.a. Groupe Combattant Tunisien, a.k.a. Jama'a Combattante Tunisien, a.k.a. JCT; a.k.a. Tunisian Combatant Group)
55. Turkish Hizballah
56. Ulster Defense Association (a.k.a. Ulster Freedom Fighters)
57. Ummah Tameer E-Nau (UTN) (a.k.a. Foundation for Construction; a.k.a. Nation Building; a.k.a. Reconstruction Foundation; a.k.a. Reconstruction of the Islamic Community; a.k.a. Reconstruction of the Muslim Ummah; a.k.a. Ummah Tameer I-Nau; a.k.a. Ummah Tameer E-Nau; a.k.a. Ummah Tameer-I-Pau)
58. Youssef M. Nada & Co. Gesellschaft M.B.H.

Appendix D

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

ACRONYMS

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

NCTC	National Counterterrorism Center
NSA	National Security Agency
NSEERS	National Security Entry/Exit Registration System
NSI	National Security Investigation
NSIC	National Security Integration Center
NSID	National Security Investigations Division
NSL	National Security Letter
NSLS	National Security Law Section
NSTTF	National Security Threat Task Force
NSU	National Security Unit
NTC	National Targeting Center
OCC	Office of the Chief Counsel
OFAC	Office of Foreign Asset Controls
OI	Office of Investigations
OIG	Office of the Inspector General
OPLA	Office of the Principal Legal Advisor
PDD	Presidential Decision Directive
POC	Point of Contact
POE	Port of Entry
SA	Special Agent
SAC	Special Agent in Charge
SAFM	Special Agent Field Manual
S/CT	Office of the Coordinator for Counterterrorism
SDGT	Specifically Designated Global Terrorists
SEACATS	Seized Asset and Case Tracking System
SEN	Significant Event Notification
SEVIS	Student and Exchange Visitor Information System
SEVP	Student and Exchange Visitor Program
SIPRNet	Secret Internet Protocol Router System
TAS	Threat Analysis Section
TEL	Terrorism Exclusion List
TFO	Task Force Officer
(b)(7)(E)	
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



Homeland Security Investigations

Counterterrorism and Criminal Exploitation Investigations Handbook

HSI HB 14-07 / November 12, 2014



U.S. Immigration
and Customs
Enforcement

~~FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE~~

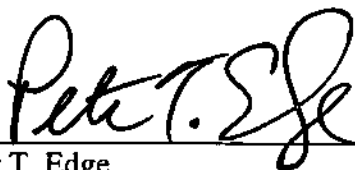
Foreword

The Counterterrorism and Criminal Exploitation Investigations Handbook provides a single source of national policies, procedures, responsibilities, guidelines, and controls to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents when conducting investigations relating to counterterrorism and criminal exploitation. This Handbook contains instructions and guidance to help ensure uniformity and operational consistency among all HSI field offices. Oversight over the national Counterterrorism and Criminal Exploitation Program resides with the Unit Chief, Counterterrorism and Criminal Exploitation Unit. (Note: HSI SAs must comply with "The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities," signed by Secretary Napolitano on April 26, 2013, and with ICE Directive 11062.2 entitled, "Sexual Abuse and Assault Prevention and Intervention," dated May 11, 2014.)

The Counterterrorism and Criminal Exploitation Investigations Handbook supersedes the Compliance Enforcement Handbook (Office of Investigations Handbook 10-01), dated January 25, 2010.

The Counterterrorism and Criminal Exploitation Investigations Handbook is an internal policy of HSI. It is not intended, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter, nor are any limitations hereby placed on otherwise lawful enforcement prerogatives of ICE. This Handbook is For Official Use Only (FOUO) – Law Enforcement Sensitive. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and the ICE Directive on Safeguarding Law Enforcement Sensitive Information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Records and Disclosure Unit, as well as the appropriate ICE Counsel and/or U.S. Attorney, should be consulted so that appropriate measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure pursuant to the law enforcement privilege. Any further request for disclosure of this Handbook or information contained herein should be referred to the HSI Records and Disclosure Unit.

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



Peter T. Edge
Executive Associate Director
Homeland Security Investigations

11/12/14
Date

COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS HANDBOOK

Table of Contents

Chapter 1. PURPOSE AND SCOPE		1
Chapter 2. INTRODUCTION		1
Chapter 3. DEFINITIONS		2
• 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	(b)(7)(E)	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 Program8
- 3.33 TECS.....8
- 3.34 Web-Based Commercial Databases8

Chapter 4. AUTHORITIES/REFERENCES8

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

Chapter 5. RESPONSIBILITIES15

- 5.1 Executive Associate Director, Homeland Security Investigations ...15
- 5.2 Deputy Assistant Director, National Security Program Division15
- 5.3 Unit Chief, Counterterrorism and Criminal Exploitation Unit16
- 5.4 Special Agents in Charge and Attachés16
- 5.5 Special Agents, Intelligence Research Specialists, and Investigative Assistants.....16

Chapter 6. CTCEU PROGRAMS AND RELATED RESOURCES16

- 6.1 Student and Exchange Visitor Information System.....16
- 6.2 Overstay Data Sources and Biometric Services.....20
- 6.3 Automated Biometric Identification System22
- 6.4 International Criminal Police Organization22
- 6.5 Visa Revocation Program24
- 6.6 International Military Student Absent Without Leave Program.....25
- 6.7 Lost and Stolen Passport Program25
- 6.8 Alien Flight Student Program25
- 6.9 Visa Waiver Enforcement Program26
- 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 Sentinel27
- 6.14 National Security Entry-Exit Registration System28
- 6.15 Compliance Enforcement Advisory Panel.....29
- 6.16 (b)(7)(E)30
- 6.17 FBI Counterterrorism Division30
- 6.18 (b)(7)(E)30
- 6.19 National Counterterrorism Center.....30
- 6.20 (b)(7)(E)30
- 6.21 (b)(7)(E)31
- 6.2231

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

- 7.1 Violator Identification.....31
- 7.2 Database Analysis.....32
- 7.3 School and Program Leads33
- 7.4 LeadTrac Database.....34
- 7.5 (b)(7)(E).....34
- 7.6 TECS Case Categories.....34
- 7.6.1 TECS Primary Program Codes35
- 7.6.2 TECS Secondary Program Codes35
- 7.7 Collateral Request Assignment.....36
- 7.8 Timely Assignment and Reporting Requirement36
- 7.9 Database Review.....36
- 7.10 Field Investigation and Interview37
- 7.11 Criminal and Administrative Charges39
- 7.12 Database Reporting/Management Notification.....40

Appendix

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

COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Counterterrorism and Criminal Exploitation Investigations Handbook establishes policy and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs), Investigative Research Specialists (IRs) and Investigative Assistants (IAs) when conducting or assisting counterterrorism and criminal exploitation investigations.

Chapter 2. INTRODUCTION

Prior to the events of September 11, 2001, there was no effective system in place to accurately track the status of nonimmigrants, especially foreign students and other visitors in the United States, which had disastrous consequences.

The 9/11 Commission wrote in its report: “We also found that had the immigration system set a higher bar for determining whether individuals are who or what they claim to be – and ensuring routine consequences for violations – it could potentially have excluded, removed, or come into further contact with several hijackers who did not appear to meet the terms of admitting short-term visitors” (The 9/11 Commission Report, July 22, 2004, page 401).

In June 2003, the ICE Office of Investigations (OI) established the Compliance Enforcement Unit (CEU) within the National Security Investigations Division, the first Unit dedicated to the enforcement of nonimmigrant visa violations. The pursuit of visa violators by CEU provided significant support on the “disrupt and deter” aspect of the counterterrorism strategy of the United States.

In September 2010, CEU’s responsibilities expanded and HSI established the Counterterrorism and Criminal Exploitation Unit (CTCEU). The mission of CTCEU is to proactively scrutinize known or suspected terrorists and their associates, identify and disrupt terrorist criminal enterprises, prevent terrorists and other criminals from exploiting the nation’s immigration system, and expand the resource equities within the various law enforcement agencies (LEAs) and the Intelligence Community (IC). CTCEU accomplishes its mission by reviewing the immigration status of known and suspected terrorists, combating criminal exploitations of the Student and Exchange Visitor Program (SEVP), and leveraging HSI’s capabilities in combination with partnering agencies to identify national security threats.

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 (b)(7)(E)

(b)(7)(E)

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. (b)(7)(E)

(b)(7)(E)

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. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

In addition to providing users access to the data via web pages,

(b)(7)(E)

(b)(7)(E)

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.

(b)(7)(E)

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.

(b)(7)(E)

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.

(b)(7)(E)

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 (DPICS²) 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),

(b)(7)(E)

(b)(7)(E)

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). (b)(7)(E)

(b)(7)(E)

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

(b)(7)(E)

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 (b)(7)(E)

(b)(7)(E)

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 (b)(7)(E)

(b)(7)(E)

(b)(7)(E) 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

information and event notifications, via the internet, to DHS and DOS throughout a student's or exchange visitor's stay in the United States.

3.32 Student and Exchange Visitor Program

SEVP is the HSI Unit that administers SEVIS and conducts outreach with the educational community. SEVP also approves schools for certification to enroll F and M nonimmigrant students and withdraws such certification when the school is determined to be no longer eligible.

3.33 TECS

TECS is an automated enforcement and inspection system designed to support DHS and other federal users. Case Management in TECS is the primary case management system used by HSI. Reports of Investigation (ROIs) are prepared and uploaded in TECS Case Management.

3.34 Web-Based Commercial Databases

Web-based commercial databases, such as Accurint, AutoTrack XP, and the Consolidated Lead Evaluation and Reporting (CLEAR) database, store millions of public source records such as state and local government records, information from public utilities, and driver's license and vehicle registration records. These commercial databases are available to the U.S. Government and the private sector, and special access to the information is available to law enforcement.

Chapter 4. AUTHORITIES/REFERENCES

4.1 Authorities

A. Enhanced Border Security and Visa Entry Reform Act (EBSVERA) of 2002

EBSVERA sets specific time frames for the implementation of SEVIS, strengthens the SEVIS requirements, and sets standards for the certification of schools and the designation of exchange visitor programs. The EBSVERA of 2002 also provides for DHS to recertify schools approved for attendance by F and/or M students every 2 years to confirm the schools' continuing eligibility for certification and compliance with recordkeeping and reporting requirements.

B. Family Educational Rights and Privacy Act (FERPA) of 1974

FERPA (20 U.S.C. § 1232g; Title 34, Code of Federal Regulations (C.F.R.), Part 99) is a Federal law that protects the privacy of students' education

records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

The Illegal Immigration Reform and Immigration Responsibility Act (IIRIRA) of 1996 (8 U.S.C. § 1372(c)(2) and 8 C.F.R. § 214.1(h)) states that nonimmigrant students are not covered by FERPA with respect to the collection and release of information to federal agencies.

C. Homeland Security Act of 2002

The Homeland Security Act of 2002 delegated responsibility for SEVIS to the Assistant Secretary of the Bureau of Border Security (BBS). Pursuant to section 1502 of the Homeland Security Act, BBS was renamed the “Bureau of Immigration and Customs Enforcement” (BICE) through the President’s “Reorganization Plan Modification for the Department of Homeland Security,” effective March 1, 2003. BICE was then renamed “U.S. Immigration and Customs Enforcement” (ICE) on March 31, 2007, as published in 72 Federal Register (FR) 20131.

D. Homeland Security Presidential Directive 2, Combating Terrorism Through Immigration Policies (October 29, 2001), 6 Integration and Use of Screening Information (September 16, 2003), and 11 Comprehensive Terrorist-Related Screening Procedures (August 27, 2004)

Directs the strengthening of information sharing, screening, and analysis programs to detect, identify, and interdict individuals entering or already within the United States who pose a terrorist threat to national security.

E. Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996, Section 641

IIRIRA required the creation of a program to collect student and exchange visitor information and monitor student and exchange visitors.

F. Immigration and Nationality Act (INA) of 1952, as amended

The INA stands alone as the basic body of immigration law. The INA is also contained in the United States Code.

G. Implementing Recommendations of the 9/11 Commission Act of 2007, Section 7; 8 U.S.C. § 1187(a)(11) and (h)(3) and 8 C.F.R. § 217.5

These references provide information relating to eligibility determinations under the Electronic System for Travel Authorization.

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.

(b)(7)(E)

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

(February 28, 2003); 13316 (September 17, 2003); 13385 (September 29, 2005); and 13652 (September 30, 2013).

N. EO 13354

EO 13354 established the National Counterterrorism Center (NCTC) to serve as the primary organization in the U.S. Government for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism, excepting purely domestic counterterrorism information.

National Counterterrorism Center, 69 FR, 53589, September 1, 2004.

O. EO 13388

EO 13388 provides that agencies shall give the highest priority to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, and establishes an information sharing council to achieve these goals.

Further Strengthening the Sharing of Terrorism Information to Protect Americans, 70 FR 62023, October 27, 2005.

P. 8 U.S.C. §§ 1103-1104

8 U.S.C. §§ 1103-1104 provide information relating to the powers and duties of the Secretary and Under Secretary of Homeland Security, and the Attorney General.

Q. 8 U.S.C. § 1202

8 U.S.C. § 1202 provides information relating to an application for a visa.

R. 8 U.S.C. § 1254a(c)(6) and 8 C.F.R. § 244.16

8 U.S.C. § 1254a(c)(6) and 8 C.F.R. § 244.16 provide information relating to temporary protected status claims.

S. 8 U.S.C. § 1255a(c)(4)-(5) and 8 C.F.R. §§ 210.2(e), 245a.2(t), 245a.3(n), and 245a.21

8 U.S.C. § 1255a(c)(4)-(5) and 8 C.F.R. §§ 210.2(e), 245a.2(t), 245a.3(n), and 245a.21 provide information related to legalization/seasonal agricultural worker claims.

T. 8 U.S.C. § 1357 and Section 287 of the INA

8 U.S.C. § 1357 provides statutory authority for immigration officers to interrogate and arrest aliens, board and search vessels for aliens, carry a firearm, and execute subpoenas and warrants. INA § 287(a)(5)(A) provides immigration officers with the statutory authority to make arrests without warrant for any offense against the United States, if the offense is committed in the officer's presence.

U. 8 U.S.C. §§ 1365a-1365a note

8 U.S.C. §§ 1365a and 1365a note provide information relating to an integrated entry and exit data system.

V. 8 U.S.C. § 1365b

8 U.S.C. § 1365b provides information relating to a biometric entry and exit data system.

W. 8 U.S.C. § 1372

8 U.S.C. § 1372 is the statutory authority for SEVIS and provides information relating to a program to collect information relating to nonimmigrant foreign students and other exchange program participants.

X. 8 U.S.C. § 1372(c)(2)

8 U.S.C. § 1372(c)(2) provides statutory authority for requesting information from schools for SEVP purposes.

Y. 8 U.S.C. § 1379

8 U.S.C. § 1379 provides information relating to a technology standard to confirm identity.

Z. 19 U.S.C. § 1401(i)

19 U.S.C. § 1401(i) defines "customs officers". HSI SAs retained their status as customs officers through 6 U.S.C. § 552 (Savings Provisions).

AA. 19 U.S.C § 1589a

19 U.S.C. 1589a grants enforcement authority to Customs officers to include the authority to carry a firearm, execute warrants, and make arrests.

BB. 19 U.S.C. § 1595

19 U.S.C. § 1595 grants Customs officers with probable cause to believe that merchandise upon which duties have not been paid or which is subject to forfeiture is located within a building, including a residence, the authority to make application for a search warrant to search such premises and seize the merchandise.

CC. 50 U.S.C. § 404o, 404o note, and 501 note

50 U.S.C. § 404o, 404o note, and 501 note provide information relating to the NCTC.

DD. 8 C.F.R. § 208.6

8 C.F.R. § 208.6 provides information relating to the disclosure to third parties of information contained in or pertaining to any asylum application.

EE. 8 C.F.R. § 214.1(f), Registration and false information

Nonimmigrant aliens' admission and continued stay in the United States are conditioned on compliance with any registration, fingerprinting, and photographing requirements upon arrival in the United States as described in 8 C.F.R. § 264.1(f). (Note: On April 28, 2011, through a notice published in the Federal Register, DHS removed the list of countries whose nationals had been subject to NSEERS registration and reporting requirements.)

FF. 8 C.F.R. § 214.2(f), (m), and (j)

8 C.F.R. § 214.2(f), (m), and (j) sets the rules for admission, extension, and maintenance of status for F, M, and J visa holders, respectively.

GG. 8 C.F.R. § 214.3

8 C.F.R. § 214.3 sets rules for the approval of schools seeking to enroll F and M nonimmigrant students, and for compliance post-approval.

HH. 8 C.F.R. § 214.3(g)

8 C.F.R. § 214.3(g) provides regulatory authority for school reporting requirements.

II. 8 C.F.R. § 214.4

8 C.F.R. § 214.4 sets rules for denial of certifications, denial of recertification, and withdrawal of SEVP certification.

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. (b)(7)(E)
- D. (b)(7)(E)
- E. (b)(7)(E)
- F. (b)(7)(E)
- G. (b)(7)(E)

- 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.

(b)(7)(E)
- O.

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

(b)(7)(E)

(b)(7)(E)

A. Student and Exchange Visitor Program

SEVP is responsible for the certification of schools wishing to enroll foreign students, the coordination of policies and regulations concerning foreign students, outreach with the academic community, and the operation and maintenance of the SEVIS database. CTCEU and SEVP share responsibility for school compliance, with SEVP focusing on administrative compliance and CTCEU focusing on criminal investigations. SEVP maintains information on schools that apply for certification and those that are currently certified by SEVP. This information includes the Petition for Approval of School for Attendance by Nonimmigrant Student (ICE Form I-17) and supporting documentation. Any requests for information or assistance from SEVP are to be coordinated through CTCEU.

B. Certification/Recertification of Schools

All academic institutions must be certified by SEVP in order to access SEVIS and issue the Certificate of Eligibility for Nonimmigrant F1 or M1 Student Status (ICE Forms I-20 A-B and I-20 M-N). In order to become certified, schools must file a Petition for Approval of School for Attendance by Nonimmigrant Student (ICE Form I-17). As of the date of issuance of this Handbook, there are no fines or penalties for administrative noncompliance with SEVIS regulations or the misuse of the SEVIS database, other than the decertification of schools or the revocation of a DSO's SEVIS access. Additionally, SEVP-certified institutions must recertify every 2 years.

C. Decertification of Schools

HSI field offices may request the withdrawal of a school's SEVP certification by contacting CTCEU. This request must be accompanied by supporting documentation outlining the justification for the withdrawal. Final authority

for the withdrawal of a school's certification is vested with SEVP's School Certification Branch (SCB).

8 C.F.R. § 214.4 sets forth the regulations concerning the withdrawal of a school's certification. CTCEU and HSI field offices will work closely with the SEVP SCB to provide information concerning schools that are subject to the withdrawal of SEVP certification. This will include timely reports of violations, documentation of incidents, and collection of evidence needed to support the withdrawal of certification.

D. Procedure for Obtaining Information from SEVP-Certified Schools

HSI's requests for information from schools for SEVP enforcement purposes are exempt from privacy requirements under the FERPA of 1974. Schools are legally bound to provide information requested by ICE. Statutory authority for requesting information from schools for SEVP purposes is found in 8 U.S.C. § 1372(c)(2). Regulatory authority for school reporting requirements is found in 8 C.F.R. § 214.3(g).

HSI SAs may obtain information needed for enforcement purposes from institutions by directly requesting the information from the DSOs. Many institutions will provide information informally (orally, by email, or via facsimile). If such a relationship exists with an institution, a formal written request does not need to be submitted. HSI has the authority to obtain the information without a subpoena; therefore, SAs shall not request information for SEVP enforcement purposes using an Immigration Enforcement Subpoena (DHS Form I-138).

Upon receiving a request for information, regulations require an institution to provide the information requested on an individual student within 3 workdays and within 10 workdays for a class of students (*i.e.*, all students in a particular major or of a certain nationality). For individuals in custody, the institution will provide the information orally on the same day when the request is made. Any oral request for information will be followed by a written notification if requested by the institution. Written requests, on ICE letterhead, will be made by certified mail, courier, or by other means so that receipt of the notification can be documented.

E. Contact with SEVP-Certified Institutions

8 C.F.R. § 214.3(I)(1)(ii) requires schools to designate one PDSO and 8 C.F.R. § 214.3(I)(1)(iii) authorizes each school to designate up to ten DSOs at any one time, including the PDSO. DSOs are responsible for updating SEVIS and issuing ICE Forms I-20 A-B or I-20 M-N to prospective and current students, as appropriate. PDSOs also serve as the principal POCs for HSI. These functions may not be delegated to any other person. If additional

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)

(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.

(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.

(b)(7)(E)



(b)(7)(E)

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)

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.

C. Biometric Exit

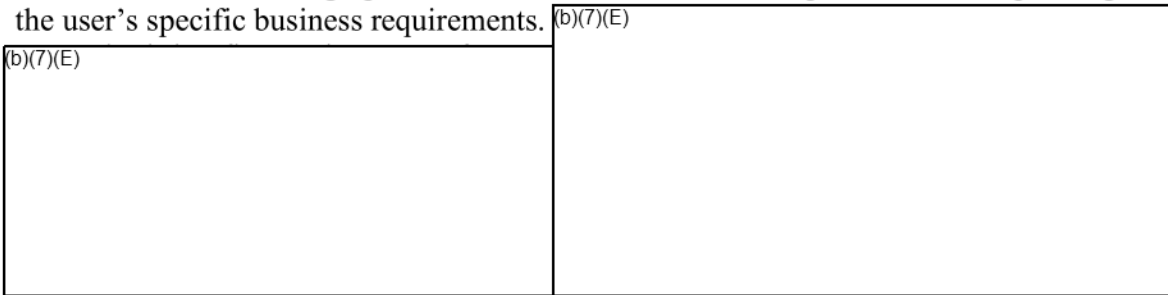
In 2006, US-VISIT piloted an automated biometric exit process to record the departure of foreign visitors. Exit procedures were put in place at 12 airports: Atlanta, Baltimore-Washington, Chicago, Dallas-Fort Worth, Denver, Detroit, Ft. Lauderdale, Newark, Philadelphia, San Francisco, San Juan, and Seattle; and 2 seaports: Miami and Los Angeles (Long Beach/San Pedro). Most foreign visitors, including nationals from Visa Waiver countries, were required to comply wherever exit procedures were established. Canadian citizens were not required to participate unless they fell under current US-VISIT enrollment criteria. Effective May 6, 2007, international visitors are no longer required to check out at a US-VISIT exit kiosk when they leave the United States.

CBP and DHS Science & Technology are currently analyzing updated solutions for implementing Biometric Exit. The exit mission was transferred from US-VISIT to CBP as part of the creation of OBIM and the CBP Entry/Exit Office.

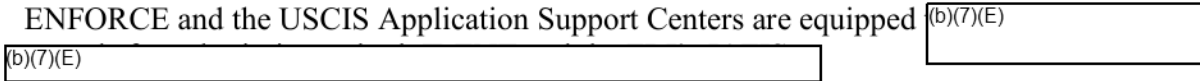
6.3 Automated Biometric Identification System

IDENT is a fingerprint matching system for rapid biometric identification of subjects. IDENT was developed in 1995 to assist the U.S. Border Patrol in identifying illegal aliens with multiple attempted illegal entries (recidivists). Since then, IDENT has grown from 5,000 subjects to millions of subjects. IDENT currently supports a variety of users for both law enforcement and immigration business processes.

IDENT users submit fingerprint transactions that search multiple databases depending on the user's specific business requirements.



User applications such as the ICE Enforcement Automated Booking Module within ENFORCE and the USCIS Application Support Centers are equipped



6.4 International Criminal Police Organization

In cooperation with the U.S. National Central Bureau (USNCB) of the International Criminal Police Organization (INTERPOL) and OBIM, CTCEU has developed a biometric-based program to identify foreign fugitives and criminals who have entered the

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.

(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. In circumstances where obtaining a provisional arrest warrant is necessary to take an individual into custody, the SA assigned to the case should work closely with CTCEU, INTERPOL, and/or the U.S. Marshals Service.

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).

(b)(7)(E)

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

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

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

6.6 International Military Student Absent Without Leave Program

CTCEU has been working closely with the U.S. military to identify, locate, and take appropriate action when a member of a foreign military present in the United States for training fails to report for training or goes absent from training. This program addresses International Military Students (IMS) who come to the United States on A-2 visas and then leave training without permission or go Absent Without Leave (AWOL), which is a violation of their immigration status.

(b)(7)(E)

(b)(7)(E)

6.7 Lost and Stolen Passport Program

Since November 2004, CTCEU has been responsible for initiating lost and stolen passport investigations. The CBP National Targeting Center (NTC) generates investigative lead information related to nonimmigrants who have entered the United States using a lost or stolen foreign passport. CTCEU also receives information from DOS on reported lost and stolen passports. These individuals may have entered the United States with fraudulent documents and were therefore inadmissible at entry.

(b)(7)(E)

6.8 Alien Flight Student Program

TSA is responsible for vetting all foreign flight candidates who seek to attend flight training in the United States. As a result of the September 11, 2001, terrorist attacks, the FBI implemented the AFSP. TSA assumed responsibility for this program in 2004. In

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

(b)(7)(E)

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. At SEVP-certified flight schools, the PDSO or DSO will be the POC. At non-SEVP-certified flight schools, the POC will be the Provider, typically the owner or manager. 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. (b)(7)(E)

(b)(7)(E)

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. This program entails the vetting of all foreign national students and their dependents in the United States

(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)

(b)(7)(E)

6.14 National Security Entry-Exit Registration System

In September 2002, DOJ developed and implemented NSEERS as the result of a Congressional mandate. Also known as “special registration,” NSEERS verified compliance with U.S. immigration laws through the implementation of a national registry for the entry and exit of nonimmigrants. NSEERS provided detailed information about the nonimmigrant, including background, purpose of the nonimmigrants’ visit to the United States, and departure confirmation.

In April 2011, DHS removed the list of countries whose nationals were required to register in NSEERS. DHS suspended all special registration and reporting requirements associated with the NSEERS program. The suspension applied to all aliens previously subject to NSEERS requirements whether or not the aliens were nationals of one of the previously designated countries and regardless of the underlying basis for the aliens’ inclusion in the NSEERS program.

Subsequently, on April 16, 2012, DHS issued guidance in its memorandum entitled, “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,” on how its components should treat an alien’s past failure to comply with special registration and reporting provisions associated with the NSEERS program and directing the DHS components to issue specific guidance consistent with it. That guidance clarified the limited circumstances under which negative immigration consequences, such as the denial of a benefit, finding of inadmissibility, or commencement of removal proceedings, would result from an alien’s prior failure to comply with NSEERS requirements. It explained that noncompliance, in and of itself, is not a sufficient basis for such consequences to adhere. Rather, negative immigration consequences may apply only where DHS personnel have determined, based on the totality of the evidence, that an alien’s NSEERS violation was willful.

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

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

6.15 Compliance Enforcement Advisory Panel

To better manage investigative resources, CTCEU relies on a prioritization framework established in consultation with interagency partners within the national intelligence and federal law enforcement communities. This partnership was formalized in 2009 with the creation of the Compliance Enforcement Advisory Panel (CEAP), which meets tri-

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)

(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. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

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.

(b)(7)(E)

(b)(7)(E)

A. System Leads

(b)(7)(E)

B. Specialized Leads

(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

(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)

(b)(7)(E)

7.3 School and Program Leads

CTCEU utilizes information from SEVIS, along with other analytical tools, to identify school and exchange visitor program anomalies. (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).

(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)

(b)(7)(E)

7.6.1 TECS Primary Program Codes

Per case management guidelines, each self-generated case must have one (except in limited circumstances) primary (b)(7)(E) program code. The below program codes are applicable to programs under CTCEU's purview:

(b)(7)(E)

7.6.2 TECS Secondary Program Codes

TECS contains many specific secondary program codes. For example, (b)(7)(E) refers to a specific school fraud investigation. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

7.7 Collateral Request Assignment

CTCEU consolidates all investigative referral information into an ROI. The ROI is used to initiate a collateral request to the designated field office. Field CTCEU coordinators review, assign, and ensure that all CTCEU collateral requests are investigated in a timely manner.

(b)(7)(E)

(b)(7)(E)

Detailed guidance on how collateral requests should be handled may be found in the Case Management Handbook (OI Handbook (HB) 08-02, dated February 1, 2008, or as updated) and in the OI memorandum signed by Marcy M. Forman, Director of OI, entitled “Minimum Standards on Compliance Enforcement Case Closures,” dated April 18, 2008, or as updated.

(b)(7)(E)

7.8 Timely Assignment and Reporting Requirement

CTCEU coordinators ensure the completion of collateral investigation requests in a timely manner.

(b)(7)(E)

(b)(7)(E)

7.9 Database Review

SAs shall review the information provided in the collateral ROI and conduct independent database queries as necessary.

(b)(7)(E)

(b)(7)(E)

7.10 Field Investigation and Interview

Prior to locating a nonimmigrant, SAs should conduct additional database queries, if deemed appropriate, and review all available documentation. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

SAs working CTCEU investigations with a terrorist nexus should consult with their local HSI JTTF liaison prior to taking enforcement action. If an office does not have a local HSI JTTF liaison, they should follow locally established procedures for deconfliction with the FBI. Additional reference and policy information is available in the National Security Investigations Handbook (HSI HB 13-03), dated April 26, 2013, or as updated. SAs should also consult with their local OCC prior to taking enforcement action in these cases so that NSLS can be put on notice as well as consulted, when appropriate.

7.11 Criminal and Administrative Charges

CTCEU investigations can result in criminal charges, administrative actions, or both. Careful consideration should be given to both charges and SAs should consult with the USAO or OCC.

A. Criminal Prosecution

Relevant criminal violations should be identified and prosecuted with the assistance of the USAO. Criminal arrests must be documented in EAGLE and TECS via a Seized Asset and Case Tracking System (SEACATS) Report.

Additionally, SAs should complete a SIR in the SEN system.

There are several violations that are commonly associated with compliance enforcement and school fraud investigations of SEVIS-certified schools and officials. They include:

- 1) 8 U.S.C. § 1324 (Harboring and Smuggling)
- 2) 8 U.S.C. § 1324c (Forging or counterfeiting false documents)
- 3) 8 U.S.C. § 1325 (Marriage Fraud)
- 4) 8 U.S.C. § 1328 (Importation for the purpose of prostitution or other immoral purposes)
- 5) 18 U.S.C. § 371 (Conspiracy)
- 6) 18 U.S.C. § 1001 (False Statements)
- 7) 18 U.S.C. § 1030 (Fraud in connection with computers)
- 8) 18 U.S.C. § 1341 (Mail Fraud)
- 9) 18 U.S.C. § 1343 (Wire Fraud)
- 10) 18 U.S.C. § 1546 (Visa Fraud)
- 11) 18 U.S.C. § 1426(b) (Uttering or selling false or counterfeit immigration documents)
- 12) 18 U.S.C. § 1621 (Perjury)
- 13) 18 U.S.C. § 1623 (False declarations before grand jury or court)

B. Administrative Proceedings

If administrative violations are substantiated, SAs should initiate administrative removal proceedings. Relevant charges can be found in the INA. Administrative arrests must be documented in EAGLE and in TECS via a SEACATS Incident Report. Prior to making administrative arrests or initiating administrative removal proceedings in any case where a national security charge or a bar pursuant to INA § 212(a)(3) or 237(a)(4) may be applicable, SAs must contact their local OCC so that NSLS may be alerted and/or consulted by the OCC where appropriate.

7.12 Database Reporting/Management Notification

Should a CTCEU-generated lead result in a significant arrest (*i.e.*, criminal alien, subject of a lookout, or INTERPOL subject, etc.), SAs should utilize the SEN system to create a SIR. Should a field investigation result in the arrest of an individual not identified as the subject of the investigation, SAs should include all qualifying information related to the incidental arrest. SAs should contact the appropriate CTCEU Program Manager if the

investigation identifies additional criminal violations or when proposed enforcement activities are forthcoming.

(b)(7)(E)

ACRONYMS

ADIS	Arrival Departure Information System
AFI	Analytical Framework for Intelligence
AFIT	Advanced Fingerprint Identification Technology
AFSP	Alien Flight Student Program
AOR	Area of Responsibility
ARO	Alternate Responsible Officer
ATS-P	Automated Targeting System – Passenger
AVALANCHE	Advanced Visual Abstracted Links and Name Collection Handler Engine
AWOL	Absent Without Leave
BBS	Bureau of Border Security
BICE	Bureau of Immigration and Customs Enforcement
BSC	Biometric Support Center
CBP	U.S. Customs and Border Protection
CCD	Consular Consolidated Database
CEAP	Compliance Enforcement Advisory Panel
CEU	Compliance Enforcement Unit
C.F.R.	Code of Federal Regulations
CI	Counterintelligence
CIS	Central Index System
CLAIMS	Computer-Linked Automated Information Management System
CLEAR	Consolidated Lead Evaluation and Reporting
CT	Counterterrorism
CTCEU	Counterterrorism and Criminal Exploitation Unit
CTD	Counterterrorism Division
CMAX	Common Mainframe Access
DACS	Deportable Alien Control System
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
DPICS ²	DHS Pattern Information and Collaboration Sharing System
DSO	Designated School Official
EAD	Executive Associate Director
EAGLE	Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement
EARM	ENFORCE Alien Removal Module
EBSVERA	Enhanced Border Security and Visa Entry Reform Act
EID	Enforcement Integrated Database
ENFORCE	Enforcement Case Tracking System
EO	Executive Order
ERO	Enforcement and Removal Operations

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



Homeland Security Investigations

Human Smuggling and Trafficking Investigations Handbook

HSI HB 15-04 / August 21, 2015



U.S. Immigration
and Customs
Enforcement

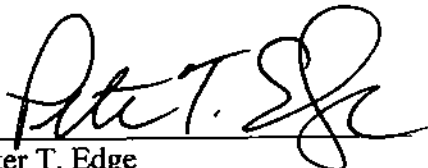
Foreword

The Human Smuggling and Trafficking Investigations Handbook provides a single source of national policies, procedures, responsibilities, guidelines, and controls to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents when conducting investigations relating to human smuggling and trafficking. This Handbook contains instructions and guidance to help ensure uniformity and operational consistency among all HSI field offices. Oversight over the National Human Smuggling and Trafficking Investigations Program resides with the Unit Chief, Human Smuggling and Trafficking Unit.

The Human Smuggling and Trafficking Investigations Handbook supersedes a number of policy documents issued by the former U.S. Immigration and Naturalization Service, the former ICE Office of Investigations, and HSI. See Appendix G for a detailed list of documents superseded by this Handbook.

The Human Smuggling and Trafficking Investigations Handbook is an internal policy of HSI. It is not intended, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter, nor are any limitations hereby placed on otherwise lawful enforcement prerogatives of ICE. This Handbook is For Official Use Only (FOUO) – Law Enforcement Sensitive. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and the ICE Directive on Safeguarding Law Enforcement Sensitive Information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Records and Disclosure Unit, as well as the ICE Office of the Principal Legal Advisor and/or the appropriate U.S. Attorney's Office, are to be consulted so that measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure in civil discovery. Any further request for disclosure of this Handbook or information contained herein should be referred to the HSI Records and Disclosure Unit.

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



Peter T. Edge
Executive Associate Director
Homeland Security Investigations

8/21/15
Date

HUMAN SMUGGLING AND TRAFFICKING INVESTIGATIONS HANDBOOK

Table of Contents

Chapter 1. PURPOSE AND SCOPE.....	1
Chapter 2. INTRODUCTION.....	1
Chapter 3. DEFINITIONS.....	1
• 3.1 Admission.....	1
• 3.2 Asylum	1
• 3.2.1 Affirmative Asylum Process	2
• 3.2.2 Defensive Asylum Process.....	2
• 3.3 Continued Presence	2
• 3.4 (b)(7)(E)	2
• 3.5 Debt Bondage.....	3
• 3.6 Deferred Action.....	3
• 3.7 Destination Country	3
• 3.8 Drop House.....	3
• 3.9 Forced Labor	3
• 3.10 Human Smuggling.....	3
• 3.11 Human Trafficking.....	3
• 3.12 Minor/Juvenile.....	4
• 3.13 Parole.....	4
• 3.14 Peonage	4
• 3.15 (b)(7)(E)	4
• 3.16	4
• 3.17 Refugee.....	5
• 3.18 Source Country.....	5
• 3.19 Special Interest Alien	5
• 3.20 Special Interest Country	5
• 3.21 Transit Country.....	5
• 3.22 Unaccompanied Child	5
Chapter 4. RESPONSIBILITIES.....	6
• 4.1 Executive Associate Director, Homeland Security Investigations.....	6
• 4.2 Assistant Director, Domestic Operations	6
• 4.3 Deputy Assistant Director, Transnational Crime and Public Safety Division	6
• 4.4 Unit Chief, Human Smuggling and Trafficking Unit.....	6
• 4.5 Special Agents in Charge and Attachés	6

- 4.6 Group Supervisors6
- 4.7 Special Agents7

Chapter 5. HUMAN SMUGGLING STATUTES AND REFERENCES7

- 5.1 Statutes7
- 5.1.1 8 U.S.C. § 1324 – Bringing in and Harboring Certain Aliens7
- 5.1.2 8 U.S.C. § 1327 – Aiding or Assisting Certain Aliens to Enter8
- 5.1.3 8 U.S.C. § 1328 – Importation of Alien for Immoral Purpose8
- 5.2 References.8

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

- 6.1 Accomplishing the Mission.....10
- 6.2 Identifying Human Smuggling Organizational Structures11
- 6.3 (b)(7)(E)13
- 6.3.1 (b)(7)(E)13
- 6.3.2 Assistance from U.S. Customs and Border Protection.....14
- 6.3.3 (b)(7)(E)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

(b)(7)(E)

Chapter 8. HUMAN TRAFFICKING STATUTES AND REFERENCES19

- 8.1 Statutes19
- 8.1.1 18 U.S.C. § 1581 – Peonage; Obstructing Enforcement19
- 8.1.2 18 U.S.C. § 1584 – Sale into Involuntary Servitude19
- 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 Labor19
- 8.1.5 18 U.S.C. § 1591 – Sex Trafficking of Children or by Force, Fraud, or Coercion19
- 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 Persons20

- 8.1.8 18 U.S.C. § 1594 – General Provisions.....20
- 8.1.9 Transportation for Illegal Sexual Activity and Related Crimes20
- 8.2 Human Trafficking Authorities/References20

Chapter 9. HUMAN TRAFFICKING INVESTIGATIVE GUIDANCE21

- 9.1 Indicators of Human Trafficking.....22
- 9.2 (b)(7)(E)23
- 9.3 Sex Trafficking.....25
- 9.4 Labor Trafficking25
- 9.5 Human Smuggling v. Human Trafficking.....25
- 9.6 Understanding Force, Fraud, and Coercion.....26
- 9.7 Responding to Trafficking Victims’ Leads27
- 9.8 Victim-Centered Approach29
- 9.9 Human Trafficking Computer-Based Training for Special Agents30

(b)(7)(E)

Chapter 11. APPLICABLE MONEY LAUNDERING LAWS IN SUPPORT OF HUMAN SMUGGLING AND HUMAN TRAFFICKING INVESTIGATIONS37

- 11.1 Money Laundering Laws.....38
- 11.2 Specified Unlawful Activities Related to Human Smuggling and Trafficking.....38
- 11.3 Forfeiture Laws38
- 11.4 (b)(7)(E)39

Chapter 12. (b)(7)(E)40

- 12.1 (b)(7)(E)40
- 12.2 Guidelines.....41

Chapter 13. IMMIGRATION RELIEF OPTIONS FOR HUMAN SMUGGLING AND HUMAN TRAFFICKING INVESTIGATIONS45

- 13.1 (b)(7)(E)45
- 13.246

• 13.3	(b)(7)(E)46
• 13.4	46
• 13.5	46
• 13.6	47
• 13.7	47
• 13.8	48
• 13.9	48

Chapter 14. CASE MANAGEMENT49

• 14.1	TECS Case Categories	49
• 14.2	TECS Program Codes	49

Chapter 15. INVESTIGATIVE RESOURCES50

• 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	(b)(7)(E)A
Appendix B	B
Appendix C	C
Appendix D	D
Appendix E	E
Appendix F	F
Appendix G	Superseded Documents.....	G
Appendix H	Acronyms.....	H

HUMAN SMUGGLING AND TRAFFICKING INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Human Smuggling and Trafficking Investigations Handbook establishes policies and procedures to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs) when conducting human smuggling and human trafficking investigations within the scope of their authority.

Chapter 2. INTRODUCTION

HSI is committed to protecting the United States by combatting the worldwide problem of human smuggling and human trafficking. The mission of HSI's Human Smuggling and Trafficking Unit (HSTU) is to identify criminal smuggling and trafficking organizations, prioritize investigations according to the degree of risk posed by each to national security and public safety, and coordinate field office investigations around targeted organizations with the goal of eliminating their ability to function.

Chapter 3. DEFINITIONS

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

3.1 Admission

The lawful entry of an alien into the United States after inspection and authorization by an immigration officer. *See* Title 8, United States Code (U.S.C.), Section 1101(a)(13)(A), Immigration and Nationality Act (INA), Section 101(a)(13)(A). Aliens lawfully admitted for permanent residence are not generally regarded as seeking an admission upon entry to the United States unless specific criteria enumerated in the INA has been met. 8 U.S.C. § 1101(a)(13)(C); INA § 101(a)(13)(C). Under Board of Immigration Appeals precedent, a procedurally regular, but otherwise unlawful, entry can still constitute an admission. For example, an alien who presents a fraudulent passport when entering the United States would be considered admitted. He or she would be placed in proceedings under chapter 237 of the INA, rather than under chapter 212.

3.2 Asylum

A discretionary form of protection available to aliens physically present in the United States who meet the definition of a refugee under 8 U.S.C. § 1101(a)(42), INA § 101(a)(42), and are not otherwise barred from receiving it. *See* 8 U.S.C. §§ 1158(a), (b), INA §§ 208(a), (b). Once an alien has been granted asylum, he or she may not be removed to his or her country of nationality or, in the case of an alien with no nationality, to his or her country of last habitual residence. *See*

8 U.S.C. § 1158(c)(1), INA § 208(c)(1). Once an alien has been granted asylum, he or she becomes eligible for other immigration benefits. *See* 8 U.S.C. §§ 1158(c)(1)(B), (C), INA §§ 208(c)(1)(B), (C).

3.2.1 Affirmative Asylum Process

The process whereby an alien seeks asylum by submitting an Application for Asylum and Withholding of Removal (U.S. Citizenship and Immigration Services (USCIS) Form I-589) to USCIS. There are seven steps in the affirmative asylum process: (1) the alien arrives in the United States, (2) the alien applies for asylum, (3) USCIS conducts fingerprinting and background/security checks, (4) the alien receives an interview notice, (5) a USCIS Asylum Officer (AO) conducts an interview with the alien, (6) the AO makes a determination on eligibility and the Supervisory Asylum Officer reviews the decision, and (7) the alien receives the decision. *See* USCIS Affirmative Asylum Procedures Manual, dated November 2007, revised July 2010, or as updated. If the AO does not approve the application of an alien who is inadmissible or deportable, the AO shall refer the application to an immigration judge for adjudication in removal proceedings. *See* Title 8, Code of Federal Regulations (C.F.R.), Section 1208.14(c)(1).

3.2.2 Defensive Asylum Process

The process whereby an alien who has not affirmatively applied for asylum with USCIS may nevertheless seek asylum before an immigration judge as a defense to, or relief from, removal. In such cases, the alien submits the application to the immigration judge who will determine whether the alien is eligible for relief during the course of the immigration proceedings. *See* 8 C.F.R. § 1208.2(b), (c).

3.3 Continued Presence

Continued Presence (CP) is a temporary immigration status provided to individuals identified by law enforcement as victims of human trafficking. This status allows eligible aliens to remain in the United States temporarily during the ongoing investigation into the human trafficking-related crimes committed against them. CP is initially granted for 1 year and may be renewed in 1-year increments. CP is authorized under provisions of section 107(c)(3) of the Trafficking Victims Protection Act (TVPA), which has since been reauthorized, and is codified at 22 U.S.C. § 7105(c)(3).

(b)(7)(E)

3.5 Debt Bondage

The status or condition of a debtor arising from a pledge by the debtor of his or her personal services or of those of a person under his or her control as a security for debt, if the value of those services as reasonably assessed is not applied toward the liquidation of the debt or the length and nature of those services are not respectively limited and defined. An individual will often pledge himself or someone under his or her control into debt bondage in exchange for passage into the United States. *See* 22 U.S.C. § 7102(4).

3.6 Deferred Action

An act of administrative convenience to the government which gives some cases lower priority. *See* 8 C.F.R. § 274a.12(c)(14).

3.7 Destination Country

The termination point or last country of the undocumented alien (UDA)'s journey and where the UDA intends to reside.

3.8 Drop House

A residence or building in the United States that is used to harbor a group of smuggled aliens after they entered the United States illegally. Typically, aliens are held at the "drop house" until their smuggling fee has been paid and/or while they await transport to another location.

3.9 Forced Labor

Labor or services of a person that is provided or obtained by threats of serious harm to, or physical restraint against, that person or another person, by means of any scheme, plan, or pattern intended to cause the person to believe that if he or she did not perform such labor or services, he or she or another person would suffer serious harm or physical restraint, or by means of the abuse or threatened abuse of law or the legal process. *See* 18 U.S.C. § 1589.

3.10 Human Smuggling

The facilitation and transportation of people into the United States by deliberately evading U.S. immigration laws. This offense includes bringing UDAs into the United States and unlawfully transporting and/or harboring aliens already present. (Note: The statute governing this range of offenses is 8 U.S.C. § 1324.)

3.11 Human Trafficking

There are two kinds of human trafficking: sex trafficking and labor trafficking.

- A. Sex trafficking is a commercial sex act that is induced by force, fraud, or coercion, or in which the person who is induced to perform such act has not attained 18 years of age.
- B. Labor trafficking involves the recruitment, harboring, transportation, provision, or obtaining of a victim by means of threat or use of force or coercion, thus subjecting the victim to involuntary servitude, peonage, debt bondage, or slavery. Involuntary servitude can be induced by means of:
 - 1) any scheme, plan, or pattern intended to cause a person to believe that, if the person did not enter into, or continue in, such condition, that person, or another person, would suffer serious harm or physical restraint; or
 - 2) the abuse or threatened abuse of the legal process.

See generally 18 U.S.C. §§ 1581-1596; 22 U.S.C. §§ 7101-7112; 42 U.S.C. § 14044; INA § 212(a)(2)(H).

3.12 Minor/Juvenile

A minor or juvenile is an individual who has not attained 18 years of age.

3.13 Parole

A grant of parole permits an otherwise inadmissible alien to be present in the United States temporarily due to urgent humanitarian concerns or to provide a significant benefit to the United States. *See* 8 U.S.C. § 1182(d)(5)(A); INA § 212(d)(5)(A). Parole does not confer any immigration status upon the alien.

3.14 Peonage

Peonage is the use of laborers bound to servitude due to debt. *See generally* 18 U.S.C. §§ 1581-1596; *see also* Section 3.11(B) above.

(b)(7)(E)

(b)(7)(E)

3.17 Refugee

- A. Any person who is outside of his or her country of nationality or, if he or she has no nationality, country of last residence, and is unable or unwilling to return to that country or avail himself or herself of that country's protection due to past persecution or a well-founded fear of persecution on account of race, religion, nationality, political opinion, or membership in a particular social group. *See* 8 U.S.C. §1101(a)(42)(A), INA § 101(a)(42)(A).
- B. In such circumstances as the President after appropriate consultation may specify, any person who is within the country of such person's nationality or, in the case of a person having no nationality, within the country in which such person is habitually residing, and who is persecuted or who has a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion. *See* 8 U.S.C. §1101(a)(42)(B), INA § 101(a)(42)(B).

3.18 Source Country

A source country is the UDA's country of origin. The term is also used in TECS to define the country/countries where the criminal activity originated. For example, where a Brazilian citizen or national is smuggled from Brazil, through Mexico, to the United States, the source country would be Brazil.

3.19 Special Interest Alien

A citizen or national of a country of current national security concern to the United States.

3.20 Special Interest Country

A country from which terrorism or national security threats to the United States originate or have been present.

3.21 Transit Country

A country, or countries, through which a UDA travels after departing his or her source country and prior to arriving at his or her destination country. Aliens may travel through multiple transit countries. For example, an alien from South Korea may be smuggled through France and Canada (in this case the transit countries) before arriving at his or her destination country, the United States.

3.22 Unaccompanied Child

An unaccompanied child is a minor who has no lawful immigration status in the United States, has not attained 18 years of age, has no parent or legal guardian in the United States, or has no parent or legal guardian in the United States who is available to provide care and physical

custody. *See* Homeland Security Act of 2002 § 462(g); 6 U.S.C. § 279(g); adopted by Trafficking Victims Protection Reauthorization Act (TVPRA) § 235(g). (Note: Not all unaccompanied children have been smuggled or trafficked.)

Chapter 4. RESPONSIBILITIES

4.1 Executive Associate Director, Homeland Security Investigations

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

4.2 Assistant Director, Domestic Operations

The Assistant Director (AD), Domestic Operations, is responsible for approving undercover investigations involving the domestic transportation and release of UDAs that are limited in scope (see Section 10.1). The AD, Domestic Operations, in consultation with the Deputy Assistant Director (DAD), Transnational Crime and Public Safety Division (TCPSD), is also responsible for resolving any disputes if the receiving Special Agent in Charge (SAC) does not concur with the release of UDAs within his or her area of responsibility (AOR) (see Section 10.3 (J)).

4.3 Deputy Assistant Director, Transnational Crime and Public Safety Division

The DAD, TCPSD, is responsible for ensuring overall compliance with the provisions of this Handbook. In addition, the DAD, TCPSD, will coordinate with the AD, Domestic Operations, to resolve any disputes if the receiving SAC does not concur with the release of UDAs within his or her AOR (see Section 10.3 (J)).

4.4 Unit Chief, Human Smuggling and Trafficking Unit

The Unit Chief, HSTU, has the overall responsibility for the implementation of the provisions of this Handbook.

4.5 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).

4.6 Group Supervisors

Group Supervisors are responsible for ensuring that the human smuggling and human trafficking related activities of the SAs they supervise, including reporting and case coding requirements, are in compliance with the provisions of this Handbook.

4.7 Special Agents

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

Chapter 5. HUMAN SMUGGLING STATUTES AND REFERENCES

The most commonly utilized criminal statutes when investigating human smuggling criminal activity are codified in Chapter 12 of Title 8 of the United States Code, entitled, “Immigration and Nationality.” This Chapter provides a brief summary of what each statute or subsection refers to in terms of the criminal committing the violation. SAs should consult with their local Office of the Chief Counsel (OCC) and U.S. Attorney’s Office (USAO) for a discussion of additional legal aspects of these or other related statutes.

8 U.S.C. § 1324 uses the term “alien smuggling.” Criminal organizations that violate the laws discussed in this Handbook are often called Human Smuggling Organizations (HSOs). (Note: For the purposes of this Handbook, the terms “alien smuggling” and “human smuggling” are used interchangeably.)

5.1 Statutes

5.1.1 8 U.S.C. § 1324 – Bringing in and Harboring Certain Aliens

This Section details the criminal penalties and elements of alien smuggling and accounts for the multiple individuals who may be involved in the scheme (e.g., foot guide, transporter, and harborer).

There are five distinct offenses that can be charged under 8 U.S.C. § 1324:

A. 8 U.S.C. § 1324(a)(1)(A)(i) – Bringing In

This section of the statute refers to the person who, knowing that a person is a UDA, brings or attempts to bring the UDA across the U.S. border.

B. 8 U.S.C. § 1324(a)(1)(A)(ii) – Transporting

This section of the statute refers to the person who, knowingly or in reckless disregard, transports or attempts to transport the UDA within the United States. The criminal need not know that the individuals are UDAs, but the circumstances dictate that the person should have known that the individuals entered the United States illegally and thus aided the violation.

C. 8 U.S.C. § 1324(a)(1)(A)(iii) – Harboring

This section of the statute refers to the person who, knowingly or in reckless disregard, provides or attempts to provide a location where a UDA can remain to assist him or her from detection.

D. 8 U.S.C. § 1324(a)(1)(A)(iv) – Encouraging

This section of the statute refers to the person who encourages or induces a UDA to come, enter, or reside in the United States knowing or in reckless disregard that such entry will be in violation of law.

E. 8 U.S.C. § 1324(a)(1)(A)(v) – Conspiring or Aiding and Abetting

This section refers to the person whose assistance and cooperation was integral to the execution of any criminal activity described in Subsections A, B, C, and D.

The maximum penalties for human smuggling are listed in 8 U.S.C. § 1324(a)(1)(B). SAs should consult with their local USAO on a case-by-case basis to determine how the individual's criminal history or other aggravating factors could impact sentencing.

5.1.2 8 U.S.C. § 1327 – Aiding or Assisting Certain Aliens to Enter

This statute refers to any person who facilitates the entry into the United States of a UDA, knowing that the UDA was previously convicted in the United States of an aggravated felony or a crime involving national security.

5.1.3 8 U.S.C. § 1328 – Importation of Alien for Immoral Purpose

This statute refers to any person who smuggles aliens into the United States for the purposes of prostitution.

5.2 References

- A. Intelligence Reform and Terrorism Prevention Act of 2004.
- B. Department of Justice (DOJ), “*Human Rights and Special Prosecution Section*,” dated September 12, 2012, or as updated <http://www.justice.gov/criminal/hrsp/>.
- C. “DHS Blue Campaign: Trafficking vs. Smuggling Brochure and Checklist” (undated).
- D. U.S. Customs and Border Protection (CBP) and ICE Policy, “Controlled Deliveries, Cold Convoys, and Pass-Through Operations at Ports of Entry,” dated February 18, 2010, or as updated.

- E. ICE Directive 10071.1, “Victim Assistance Program,” dated August 25, 2011, or as updated.
- F. 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.
- G. Detention and Removal Operations (DRO)/Office of Investigations (OI) memorandum, “DRO/OI Protocols and Handling Unaccompanied Alien Children,” dated October 1, 2007, or as updated.
- H. HSI “Human Smuggling Strategy,” dated January 2015, or as updated.
- I. HSI memorandum, “Role & Responsibilities of Field Coordinators in Support of the S-Nonimmigrant Visa (S-Visa) Program,” dated July 19, 2010, or as updated.
- J. HSI Memorandum, “Domestic and International Undercover Alien Smuggling Investigations,” dated March 23, 2012, or as updated.
- K. OI memorandum, “Interim Policy and Guidelines for Immediate Assumption of Significant Public Benefit Parole Responsibilities,” dated August 8, 2006, or as updated.
- L. OI memorandum, “Accountability of U.S. Immigration and Customs Enforcement (ICE) Significant Public Benefit Paroles,” dated June 27, 2006, or as updated.
- M. Financial Investigations Handbook (HSI Handbook (HB) 14-03), dated May 13, 2014, or as updated.
- N. Cyber Crimes Investigations Handbook (HSI HB 11-03), dated August 9, 2011, or as updated.
- O. Case Management Handbook (OI HB 08-02), dated February 1, 2008, or as updated.
- P. “HSTU TECS CODES Spreadsheet,” dated January 28, 2013, or as updated.
- Q. “ECT Brochure,” dated November 2012, or as updated.
- R. “Illicit Pathways Attack Strategy (IPAS) Brochure,” dated December 2012, or as updated.
- S. “Project Stamp Brochure,” dated May 2012, or as updated.
- T. “Extraterritorial Criminal Travel Strike Force Expansion and Institutionalization” (undated).

U. “Proposal to Enhance the ECT Strike Force” (undated).

V. Domestic and International Undercover Alien Smuggling Investigations Approval Guidance Chart (see Appendix A).

Chapter 6. HUMAN SMUGGLING INVESTIGATIVE GUIDANCE

Human smuggling is a transnational crime committed by violators whose ultimate goal is to make a financial profit. UDAs choose to enter other countries illegally for many reasons, such as religion, politics, employment, and/or education. In some cases, a UDA will enter into an agreement with a smuggler to illegally enter the United States. The human smuggler will in turn determine a set fee depending on the method or route used by the HSO or the individual. HSOs vary by the nationality of aliens smuggled, size of organization, levels of hierarchy, and sophistication of their method of operation.

HSOs operate by establishing a network that facilitates the undetected movement of UDAs from source countries through transit countries with the ultimate goal of successfully entering the United States in violation of U.S. law.

(b)(7)(E)

HSOs are ever-changing in their level of sophistication and have become increasingly violent by engaging in kidnapping, extortion, assault, and rape. Some of these activities have even resulted in the death of UDAs.

6.1 Accomplishing the Mission

HSI’s mission can be accomplished domestically and internationally by pursuing, identifying, investigating, disrupting, and dismantling HSOs in the United States and in transit countries, and by:

(b)(7)(E)

(b)(7)(E)

6.2 Identifying Human Smuggling Organizational Structures

HSOs can vary in several ways, including the number of co-conspirators, operating structure, financial structure, areas of operation, and nationality of the aliens the organization smuggles.

Human smuggling operations can be as small as an individual operating independently or as large as an organization. The individual or organization provides a guide, transportation, and temporary housing for aliens at points along the journey and/or once they arrive in the United States. HSOs are more organized in that they have defined roles for each member and a clear chain of command.

(b)(7)(E)

(b)(7)(E)

HSOs generally have the following operating structure:

A. Head of the Organization

The head of the organization is responsible for the oversight of the operation; he or she maintains continuous communication and coordinates the criminal activity with co-conspirators. This person shares in a major portion of the profits of the operation and, in many instances, escapes prosecution because he or she seldom participates directly in the actual smuggling activity.

B. Recruiters

The recruiters are the persons who are usually located outside the United States and are responsible for identifying aliens seeking to be smuggled into the United States. Recruiters are generally paid according to the number of UDAs who are successfully smuggled into the United States.

C. Guides

Guides, often referred to as “coyotes,” are the persons responsible for leading individual(s) illegally across the U.S. border. The guides are usually present for the border crossing but depart from the United States after delivering the UDAs to a designated location near the border. In some cases, there may be multiple sets of guides, for example one on each side of the border. In many instances, if guides are apprehended, they will attempt to assume the role of smuggled aliens.

D. Transporter

The transporter, often referred to as “the driver,” is the person who conveys aliens from one location to another in furtherance of the aliens’ illegal entry into the United States. Transporters often pick up UDAs at staging locations and transport them to drop houses in the United States. Transporters can use multiple types of conveyances, such as pickup trucks, vans, cars, boats, and tractor trailers to transport the UDAs. Alien smuggling offenses are not restricted to the time period immediately after entry.

E. Drop House Operators

A drop house operator is responsible for maintaining the drop house location(s) along the U.S. border and in interior U.S. cities, as well as running all facets of the drop house operations. The responsibilities of a drop house operator include, but are not limited to, detaining and maintaining the UDAs in the drop house until receipt of the smuggling fees, hiring and paying the guides and drivers, and coordinating travel arrangements to the next or final destination of the UDAs. The drop house operators also work with money collectors to coordinate the collection of smuggling fees or to collect money for themselves. The drop house operators also ensure that the UDAs are fed and that they do not leave the location until the smuggling fee is paid.

F. Facilitators

Most large HSOs obtain the assistance of facilitators. Facilitators are often individuals with lawful immigration or citizenship status (e.g., lawful permanent resident or U.S. citizen). Facilitators are responsible for renting properties to be used as drop houses in the United States, renting or purchasing means for transporting UDAs, obtaining cellular telephones, and recovering seized vehicles from impound lots. Some facilitators are hired for the purpose of providing false documents, which can be genuine, counterfeit, or altered documents.

G. Money Couriers

Most large HSOs include money couriers. Money couriers are responsible for collecting alien smuggling fees (b)(7)(E)

(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 harborer may be arrested. Therefore, the criminal organization may require that a transporter or guide take on the role of the harborer.)

(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)

(b)(7)(E)

(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 Responding to Human Smuggling Incidents

When responding to a human smuggling incident, SAs shall:

(b)(7)(E)

(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.)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Chapter 8. HUMAN TRAFFICKING STATUTES AND REFERENCES

The most commonly used human trafficking criminal statutes are codified in Chapter 77 of Title 18 of the United States Code. SAs should consult their local OCC and USAO for a discussion of additional legal aspects relating to these statutes.

8.1 Statutes

8.1.1 18 U.S.C. § 1581 – Peonage; Obstructing Enforcement

This statute refers to the criminal who maintains custody of the victim, physically or psychologically, for the purposes of peonage (defined in Section 3.14). *See* 18 U.S.C. § 1581(a). This statute also refers to criminals who attempt to obstruct justice related to this crime. *See* 18 U.S.C. § 1581(b). The statute includes the corresponding penalty.

8.1.2 18 U.S.C. § 1584 – Sale into Involuntary Servitude

This statute refers to the criminal who maintains custody of the victim, physically or psychologically, for the purposes of involuntary servitude as defined in Section 3.11. *See* 18 U.S.C. § 1584(a). This statute also refers to criminals who attempt to obstruct justice in relation to this crime. *See* 18 U.S.C. § 1584(b). The statute includes the corresponding penalty.

8.1.3 18 U.S.C. § 1589 – Forced Labor

This statute refers to criminals who provide or obtain the labor of a person, or benefit from providing or obtaining such labor by means such as force or threats of force, serious harm or threats of serious harm, or abuse or threats of abuse. *See* 18 U.S.C. § 1589(a). The employer(s) who engage in the providing or obtaining of the labor can also be charged. *See* 18 U.S.C. § 1589(b). The statute includes the corresponding penalty.

8.1.4 18 U.S.C. § 1590 – Trafficking with Respect to Peonage, Slavery, Involuntary Servitude, or Forced Labor

This statute refers to criminals who knowingly recruit, harbor, transport, provide, or obtain by any means any person for forced labor.

8.1.5 18 U.S.C. § 1591 – Sex Trafficking of Children or by Force, Fraud, or Coercion

This statute refers to trafficking with respect to sex trafficking of a minor or of any person by force, fraud, or coercion. It also refers to anyone who benefits financially or receives anything of value from the sex trafficking of any person. *See* 18 U.S.C. § 1591(a). The statute also outlines the corresponding punishment for sex trafficking depending on the age of the victim. *See* 18 U.S.C. § 1591(b).

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

This statute refers to criminals who knowingly destroy, conceal, remove, confiscate, or possess any actual or purported passports or other immigration document, or any other actual or purported government identification document of another person to further the trafficking of person(s). The statute includes the corresponding penalty.

8.1.7 18 U.S.C. § 1593A – Benefiting Financially from Peonage, Slavery, and Trafficking in Persons

This statute prohibits anyone from knowingly benefiting, financially or by receiving anything of value, from participation in a venture which has engaged in any act in violation of 18 U.S.C. §§ 1581(a), 1592, or 1595(a), knowing or in reckless disregard of the fact that the venture has engaged in these acts by any means.

8.1.8 18 U.S.C. § 1594 – General Provisions

This statute refers to the punishment of persons who attempt to violate or conspire with another to violate specific sections of Title 18 of the U.S. Code. Punishment includes civil forfeiture.

Subsection (f) of this section relates to witness protection; specifically, any violation of this chapter shall be considered an organized criminal activity or other serious offense for the purposes of application of chapter 224 (relating to witness protection). *See* 18 U.S.C. § 1594(f).

8.1.9 Transportation for Illegal Sexual Activity and Related Crimes

The following statutes, codified in 18 U.S.C. Chapter 117, Transportation for Illegal Sexual Activity and Related Crimes, are often utilized in human trafficking investigations, because the elements of these statutes frequently align with fact patterns similar to human trafficking investigations. These statutes, commonly known as the “Mann Act,” are detailed under 18 U.S.C. §§ 2421-2423. In general, these statutes prohibit anyone from knowingly transporting or attempting to transport a person in interstate or foreign commerce, or in any territory or possession of the United States, with the intent that the person engage in prostitution or any sexual activity.

8.2 Human Trafficking Authorities/References

- A. Intelligence Reform and Terrorism Prevention Act of 2004.
- B. Trafficking Victim Protection Act (TVPA) of 2000 and all subsequent TVPA Re-Authorizations.
- C. “Interagency Memorandum of Understanding between the Department of Health and Human Services, the Department of Homeland Security, and the Department of Justice,” dated July 12, 2004, or as updated.

- D. DOJ, “*Human Trafficking Prosecution Unit*,” dated September 12, 2012, or as updated <http://www.justice.gov/crt/about/crm/htpu.php>.
- E. DOJ, “*Human Rights and Special Prosecution Section*,” dated September 12, 2012 <http://www.justice.gov/criminal/hrsp/>.
- F. “DHS Blue Campaign: ICE Efforts to Combat Trafficking in Persons-Fact Sheet,” dated November 1, 2011, or as updated.
- G. “DHS Blue Campaign: Trafficking vs. Smuggling Brochure and Checklist” (undated).
- H. “DHS/DHS Human Trafficking Initiative from Senior Counselor Hill” (undated).
- I. ICE Directive 10071.1, “Victim Assistance Program,” dated August 25, 2011, or as updated.
- J. HSI Directive 10075.1, “Continued Presence,” dated April 6, 2011, or as updated.
- K. DRO/OI memorandum, “DRO/OI Protocols and Handling Unaccompanied Alien Children,” dated October 1, 2007, or as updated.
- L. HSI memorandum, “Role & Responsibilities of Field Coordinators in Support of the S-Nonimmigrant Visa (S-Visa) Program,” dated July 19, 2010, or as updated.
- M. OI memorandum, “Interim Policy and Guidelines for Immediate Assumption of Significant Public Benefit Parole Responsibilities,” dated August 8, 2006, or as updated.
- N. OI memorandum, “Accountability of U.S. Immigration and Customs Enforcement (ICE) Significant Public Benefit Paroles,” dated June 27, 2006, or as updated.

Chapter 9. HUMAN TRAFFICKING INVESTIGATIVE GUIDANCE

HSI conducts human trafficking investigations to combat the criminal exploitation and victimization of persons regardless of the persons’ manner of entry into the United States, citizenship, or immigration status. Victims of human trafficking may have entered the United States lawfully only to be subjected to exploitation at a later time. Although HSI primarily focuses on the investigation of human trafficking violations involving foreign nationals (perpetrators or victims), SAs have the jurisdiction to also target trafficking investigations involving domestic victims with no international nexus. Different groups or individuals may be involved in different phases of the process, such as the recruitment of victims in foreign countries, their cross-border transportation, and their exploitation in the United States. The globalization of economic systems and developments in transportation and communication

technologies has also created enormous opportunities for organized smuggling and human trafficking. Just as human trafficking organizations (HTOs) have gained sophistication by adopting modern transportation infrastructure and global communication technologies, HSI and its law enforcement partners must evolve and collaborate more effectively to combat human trafficking that is affecting countries around the world.

(b)(7)(E)

9.1 Indicators of Human Trafficking

The following are indicators of potential human trafficking situations:

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

9.3 Sex Trafficking

Sex trafficking is a type of human trafficking in which the victim is induced to engage in commercial sex acts, as defined in 18 U.S.C. § 1591(e)(3), or in which the person induced to perform such acts has not attained 18 years of age. The primary purpose behind this form of trafficking is to generate profits through the sexual exploitation of the victims. In some cases, victims may have initially been willing participants but were subsequently coerced, threatened, or forced to remain in the situation. Victims are often forced to perform in various roles which can eventually lead to sexual exploitation. These roles include, but are not limited to, prostitution and working in adult entertainment establishments such as strip clubs, cantina bars, or private call services known as “deliveries.” However, it is important to keep in mind that, for a violation to be considered sex trafficking, the victims must be engaged in, or have offered to engage in, commercial sex acts.

(b)(7)(E)

9.4 Labor Trafficking

Labor trafficking centers on the exploitation of a person’s production or ability to provide a service by means of force, fraud, or coercion. Similarly to sex trafficking, regardless of whether or not victims have a debt to be paid, victims are made to do manual labor or services thus generating profits for their exploiters. Slavery, peonage, debt bondage, and involuntary servitude fall under this form of labor trafficking and can involve work in areas such as agriculture, manufacturing, or service industries, such as domestic workers who work in-home, e.g., a maid or a caretaker.

9.5 Human Smuggling vs. Human Trafficking

Although trafficking victims are often found in sweatshops, service industries, residential homes (where they perform domestic work), agricultural labor, prostitution, or sex entertainment, they may be found anywhere in the United States doing anything that is profitable to their exploiters. Victims may not recognize that they have been victimized or may be forced into protecting their exploiters. As a result, self-identifying as a victim is not a requirement to be considered a victim of human trafficking. Both domestic and foreign victims are often lured into or within the United States with promises of legitimate employment, tourism, and educational opportunities, only to find themselves exploited in the commercial sex industry or in forced labor situations. Foreign victims find themselves in a foreign country and often they cannot speak the native language of the foreign country. Traffickers often take away the victims’ travel and identity documents and threaten victims by telling them that, if they attempt to escape, they or their families will be harmed or the victims’ families will assume the victims’ debt.

It may be difficult to distinguish between smuggling and trafficking in the initial phase of the investigation. (b)(7)(E)

(b)(7)(E)

9.6 Understanding Force, Fraud, and Coercion

The following are some examples of force, fraud, or coercion:

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

9.7 Responding to Trafficking Victims' Leads

The critical first steps in pursuing any human trafficking lead are the immediate rescue of any identified or potential victims from dangerous situations and the swift determination of any human trafficking indicators. When HSI receives a lead involving a potential human trafficking case or victim, SAs will proceed as follows:

(b)(7)(E)

(b)(7)(E)

(Note: For further guidance and requirements, see the TVPRA and “The Interagency Memorandum of Understanding Between the Department of Health and Human Services, the Department of Homeland Security, and the Department of Justice,” dated July 12, 2004, or as updated.)

9.8 Victim-Centered Approach

The enormous profits generated by human trafficking have attracted the interest of organized crime organizations and led to the significant involvement of such organizations into criminal human trafficking ventures. Traffickers exploit impoverished and vulnerable individuals seeking a better life by offering false hopes of economic enrichment or, at the very least, economic opportunity and steady employment. Once ensnared by traffickers, victims are trapped in a world of fear, cruelty, and misery that is extremely difficult to escape. Traffickers use threats,

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.

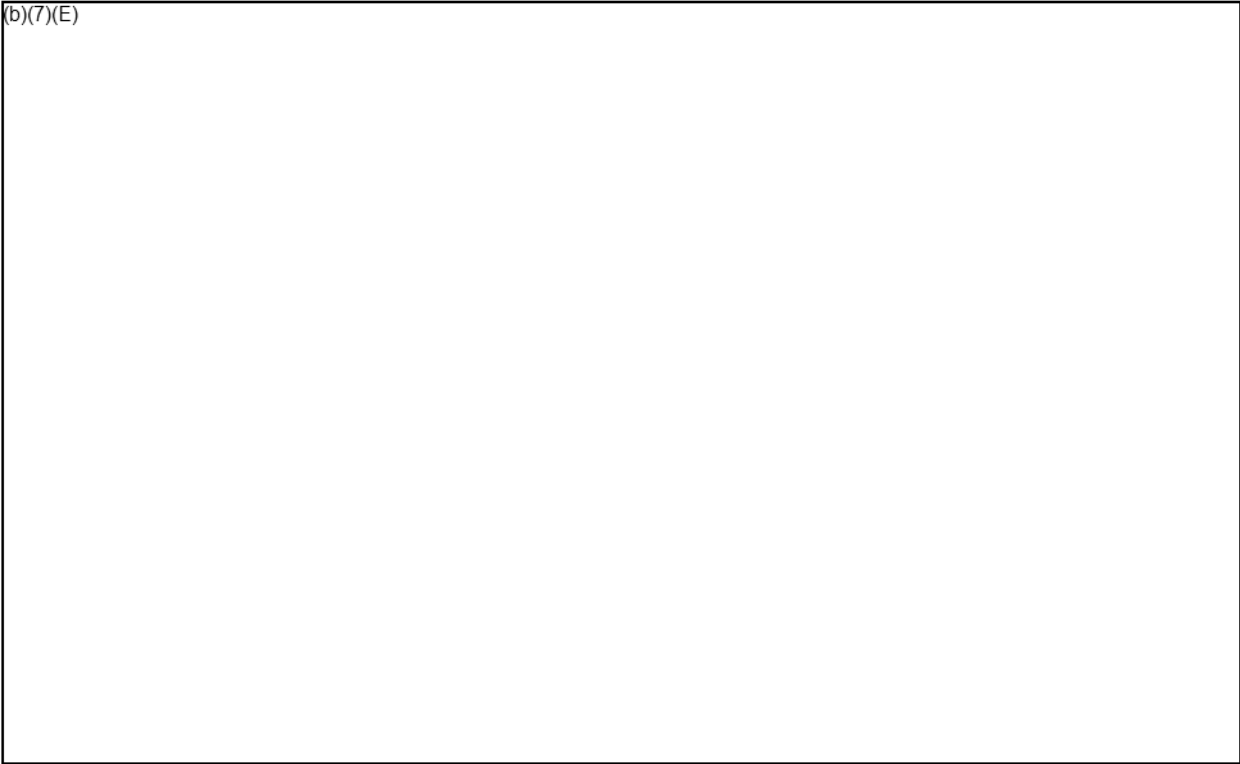
9.9 Human Trafficking Computer-Based Training for Special Agents

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.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)



(b)(7)(E)



(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(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.

(b)(7)(E)

11.1 Money Laundering Laws

Federal money laundering laws require that there be a financial transaction involving proceeds of a specified unlawful activity (SUA) with knowledge by the transactor that the funds are proceeds of some felony, but the transaction must be accomplished or undertaken for a particular purpose, e.g., promote some violation which is in fact an SUA; conceal some aspect (ownership, source, location, etc.) of proceeds derived from an SUA; avoid a reporting requirement; or engage in income tax violations prohibited by 26 U.S.C. §§ 7201, 7206.

- A. 18 U.S.C. § 1956 (a)(1) – Domestic Transactions
- B. 18 U.S.C. § 1956 (a)(2) – International Transactions
- C. 18 U.S.C. § 1956 (a)(3) – Sting operation
- D. 18 U.S.C. § 1957 – Transactions at Financial Institutions
- E. 18 U.S.C. § 1956 (h) – Money Laundering Conspiracy

11.2 Specified Unlawful Activities Related to Human Smuggling and Trafficking

- A. 8 U.S.C. § 1324 – Bring in and Harboring Certain Aliens
- B. 8 U.S.C. § 1327 – Aiding and Assisting Certain Aliens to Enter
- C. 8 U.S.C. § 1328 – Importation of Alien for Immoral Purpose
- D. 18 U.S.C. § 1581 – Peonage
- E. 18 U.S.C. § 1584 – Sale into Involuntary Servitude
- F. 18 U.S.C. §§ 2421-2423 – “Mann Act”
- G. 18 U.S.C. § 1591 – Sex Trafficking of Children or by Force, Fraud, or Coercion

(Note: SAs should seek more detailed guidance by consulting the Financial Investigations Handbook (HSI HB 14-03), dated May 13, 2014, or as updated.)

11.3 Forfeiture Laws

- A. 18 U.S.C. 981 – Civil Forfeiture

Civil forfeiture law embodies actions against a property in question with the requirement that the government establish probable cause that the property was

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.)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

12.2 Guidelines

Hostage situations can be dynamic and complex events; specific actions taken during a hostage situation need to be determined on a case-by-case basis. Exigent circumstances may require deviation from the following guidelines:

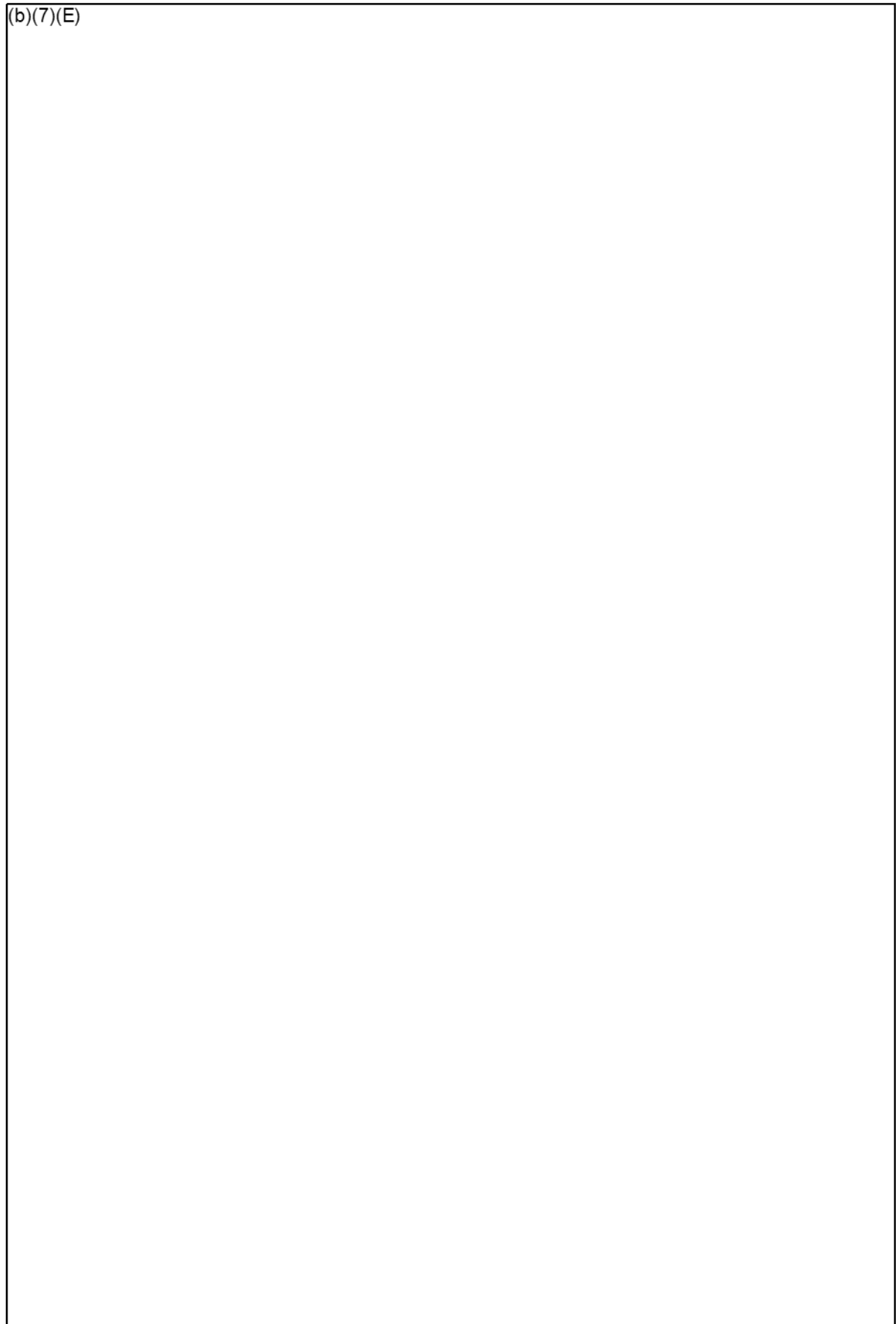
(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(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.

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Chapter 14. CASE MANAGEMENT

In order to appropriately document investigations, proper case management must be followed. It is important for SAC offices, and thus SAs, to properly categorize and code their cases in order to streamline the process of reporting, querying, intelligence gathering, and resource allocation.

(b)(7)(E)

14.1 TECS Case Categories

Case category (b)(7)(E) Human Smuggling/Trafficking, shall be utilized for all human smuggling and trafficking cases entered into TECS. Although there may be some overlap between these two criminal activities, they are two distinctly different federal violations and must be tracked accordingly. The primary program codes under this category are (b)(7)(E) for human smuggling investigations and (b)(7)(E) for human trafficking investigations. In addition, the subcategory program codes listed in Section 14.2 below shall be used to further classify each case.

14.2 TECS Program Codes

SAs should be aware that human smuggling and human trafficking cases sometimes cross over into other program areas (e.g., Worksite Enforcement, Identity and Benefit Fraud, etc.) and the secondary program codes for these areas should therefore be utilized in addition to the (b)(7)(E) and (b)(7)(E) primary program codes.

General program codes used in TECS for human smuggling and human trafficking investigations are as follows:

(b)(7)(E)

(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.

These groups provide SAs with invaluable forms of intelligence, organization, and victim assistance to what can become very complex cases. The following Sections detail some of the primary resources needed to help conduct human smuggling and human trafficking investigations effectively.

15.1 Human Smuggling and Trafficking Unit

HSTU can be contacted as follows:

U.S. Immigration and Customs Enforcement
Homeland Security Investigations
500 12th St. SW
Washington, DC 20536

Human Trafficking: (b)(7)(E)@ice.dhs.gov

Human Smuggling: (b)(7)(E)@ice.dhs.gov

(Note: SAs can access additional contact information for HSTU on (b)(7)(E))

15.2 Human Smuggling and Trafficking Center

HSTC was established by the Intelligence Reform and Terrorism Prevention Act of 2004 to provide greater coordination between state, federal, and international authorities involving human smuggling, human trafficking, and clandestine terrorist travel. HSTC facilitates the broad dissemination of all-source information, prepares strategic assessments, identifies issues for interagency coordination or attention, and coordinates and provides support for select initiatives. Participating federal agencies include the Department of State, DHS, DOJ, and the Office of the Director of National Intelligence. Further information regarding the HSTC may be found on HSI Net at the following address or website:

Human Smuggling and Trafficking Center
1800 G Street NW, (b)(7)(E)
Washington, DC 20223

(b)(7)(E)

15.3 National Human Trafficking Resource Center

The NHTRC is an HHS-funded program implemented for the purpose of providing a national, 24-hour human trafficking hotline in the United States. The NHTRC fields calls from potential victims, community members, and law enforcement agencies ranging from human trafficking tips and training requests to trafficking response situations. It also provides services including crisis calls from victims, tip reporting, training requests, urgent and non-urgent referrals, and general information requests. The NHTRC can be contacted at:

(b)(7)(E)

Email: (b)(7)(E)

15.4 Victim Assistance Program

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 linked to the VAP. The responsibility for ensuring that victims' needs are met lies with collateral-duty VACs working in HSI and ERO field offices, as well as with full-time VASs at HSI and ERO HQ and field offices. If VAC services are needed for an investigation, SAs should consult with their SAC office VAS or VAC for assistance. The HSI VAP is in the VAP/MO Unit, ISD, and can be contacted at:

HSI Victim Assistance Program:

Phone: (b)(7)(E)
Email: (b)(7)(E)@dhs.gov

15.5 Forensic Interview Program

The VAP has full-time forensic interview specialists available to support domestic and international investigations involving victims, particularly in the areas of child exploitation and human trafficking. The purpose of a forensic interview is to assist in the determination of whether or not a crime has occurred and to assess the victim's safety in his or her current situation. Forensic interview specialists are available to all victims, but their expertise is children.

(b)(7)(E)

(b)(7)(E)

(See the HSI memorandum, "The Forensic Interview Program," dated September 16, 2009, or as updated, for additional information.)

To request assistance with scheduling a forensic interviewer to aid their investigation, SAs should contact the VAP at HSI HQ which can be contacted at:

Forensic Interviews:

Phone: (b)(7)(E)
Email: (b)(7)(E)@ice.dhs.gov

15.6 Office of Refugee Resettlement

ORR is part of the Administration for Children and Families under HHS. ORR provides assistance through NGOs for victims of human trafficking by helping with resources like housing, living assistance, providing certifications for foreign adult victims of human trafficking, and eligibility letters to foreign minor victims of human trafficking. Certifications and eligibility letters grant foreign victims access to federal benefits and services to the same extent as refugees, including monetary and medical assistance, social services, health care, and foster care. ORR can be contacted at:

Office of Refugee Resettlement
Administration for Children and Families
U.S. Department of Health and Human Services
Aerospace Building
901 D Street, SW
Washington, DC 20447

(b)(7)(E)

15.7 Non-Governmental Organizations

NGOs are organizations that are not a part of a federal, state, or local government. For the purposes of HSI, NGOs are generally organizations or agencies that provide one or more social services to trafficking survivors and victims of other crimes. These service providers have an important role in the stabilization and long-term recovery of trafficking victims and often provide access to the following short-term and long-term services. Short-term services include, but are not limited to, shelter, food, clothing, medical care, and dental care. Long-term services include, but are not limited to, mental health, English language training, job skill training, and case management.

NGOs also provide or work with partner agencies that can provide immigration advocacy and legal services to trafficking victims which is a critical resource for victims who pursue civil cases or T or U nonimmigrant status. Many NGOs are community organizations, faith-based organizations, or agencies whose primary mission is to provide assistance to victims of domestic abuse or sexual assault. Since there is no organization with the capacity to meet the wide range of trafficking victims' needs single-handedly, NGOs usually work in collaboration with counterparts in a task force model. It should be noted that, while most trafficking victim service agencies are NGOs, there are many public agencies, especially at the local level, that also provide direct services to trafficking victims.

15.8 HSI Office of Intelligence

The HSI Office of Intelligence collects, analyzes, and shares timely and accurate intelligence on illicit trade, illicit travel, and illicit financial activity with a U.S. nexus. SAs are encouraged to utilize their local Intelligence Research Specialists to assist with investigative efforts, including

(b)(7)(E)

15.9 Human Trafficking Prosecution Unit

HTPU is part of the DOJ Civil Rights Division's Criminal Section and it serves to consolidate the expertise and resources of experienced human trafficking prosecutors. HTPU prosecutors work closely with the AUSAs and law enforcement agencies to streamline fast-moving trafficking investigations, ensure consistent application of trafficking statutes, and identify multijurisdictional trafficking networks. Early notification of any case with potential human trafficking angles allows HTPU to provide technical assistance, legal guidance, and coordination between districts prosecuting overlapping criminal network. (See the DOJ memorandum, "Human Trafficking Prosecution Unit," dated September 12, 2012, or as updated.) HTPU can be contacted through HSTU.

15.10 Human Rights and Special Prosecution Section

The DOJ Criminal Division's HRSP Section prosecutes members of international criminal networks who seek to evade U.S. immigration laws, such as smuggling persons into the United States. (See the DOJ memorandum, "Human Rights and Special Prosecution Section," dated September 12, 2012, or as updated.) <http://www.justice.gov/criminal/hrsp/>. HRSP also assists in the prosecution of ECT and IPAS investigations. HRSP can be contacted through HSTU.

15.11 International Organized Crime Intelligence and Operations Center

The International Organized Crime Intelligence and Operations Center (IOC2) utilizes existing resources and databases of the Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center and Special Operations Division (SOD) to share intelligence, deconflict operations, and produce actionable leads for investigators and prosecutors working nationwide. IOC2 can further help conduct case coordination in furtherance of the investigations. (Note: When requesting the telephone searches from IOC2, SOD results are automatically included. IOC2 can be contacted at:

National Program Manager
U.S. Immigration and Customs Enforcement
Homeland Security Investigations
OCDETF Fusion Center
International Organized Crime Intelligence and Operations Center (IOC2)

(b)(7)(E)

15.12 Special Operations Division

SOD can query telephone numbers to deconflict with other federal investigations. SOD can be contacted at:

Program Manager, Special Operations Division

Email: (b)(7)(E) @ice.dhs.gov

15.13 Undercover Operations

Undercover operations can be used to fund travel for SAs to follow victims outside their AOR. (Note: SAs should contact the Undercover Operations Unit for further information.)

15.14 Counterterrorism and Criminal Exploitation Unit

The Counterterrorism and Criminal Exploitation Unit (CTCEU) brings special skill sets to human smuggling and trafficking cases that involve certain visa classes such as F, M, and J visas.

CTCEU's SEVIS Exploitation Section may be contacted by SAs any time the smuggling scheme being used involves F, M, or J visas or academic, vocational and/or flight schools. CTCEU has the capability to analyze a large volume of data pertaining to schools, programs, and student and exchange visitor visa holders and compare them to current trends, intelligence, and law enforcement reporting to uncover human smuggling or trafficking.

(Note: CTCEU can be contacted at (b)(7)(E) dhs.gov; additional information can be found on HSI Net.)

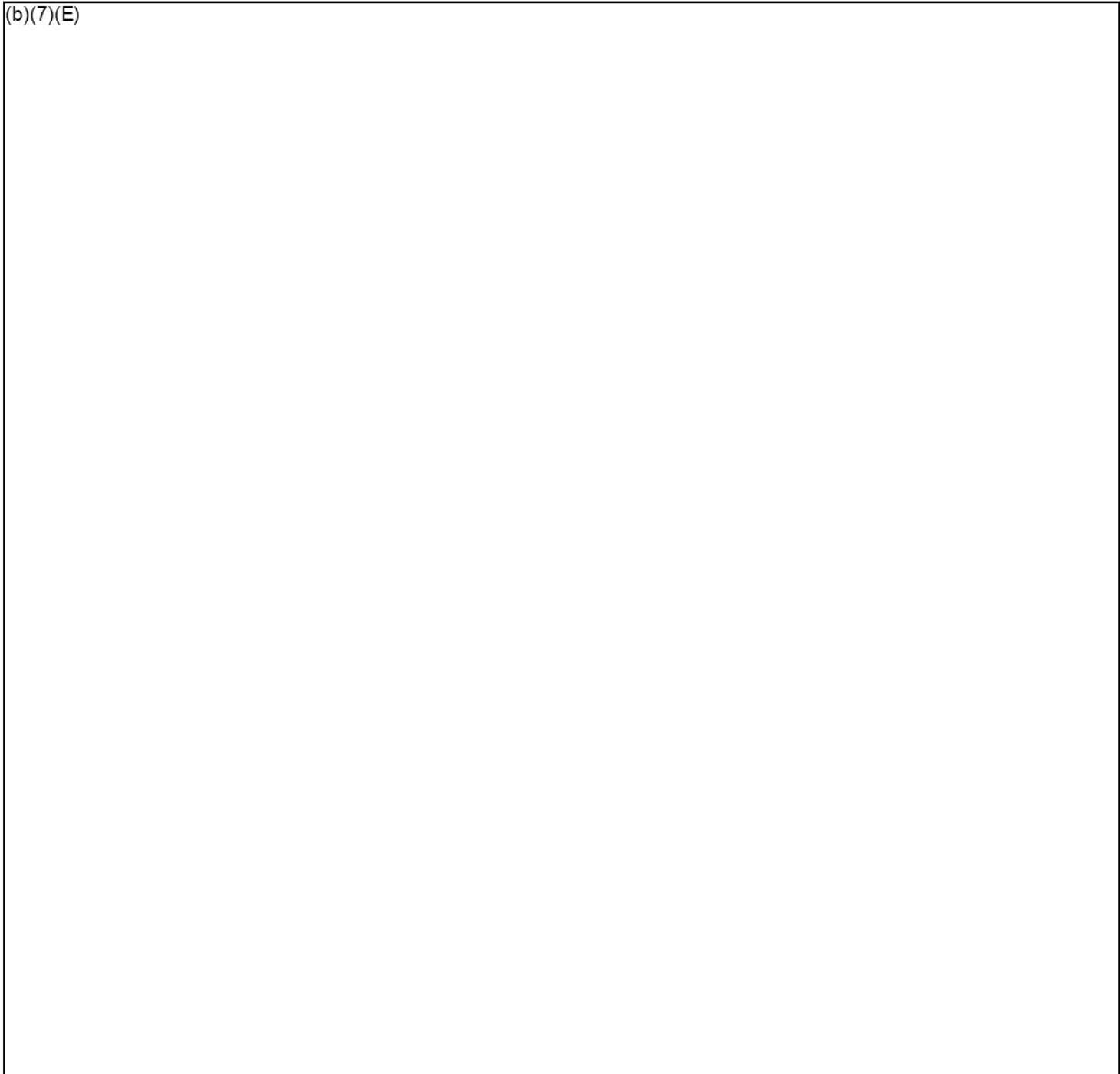
Appendix A

(b)(7)(E)

(b)(7)(E)

Appendix B

(b)(7)(E)



(b)(7)(E)

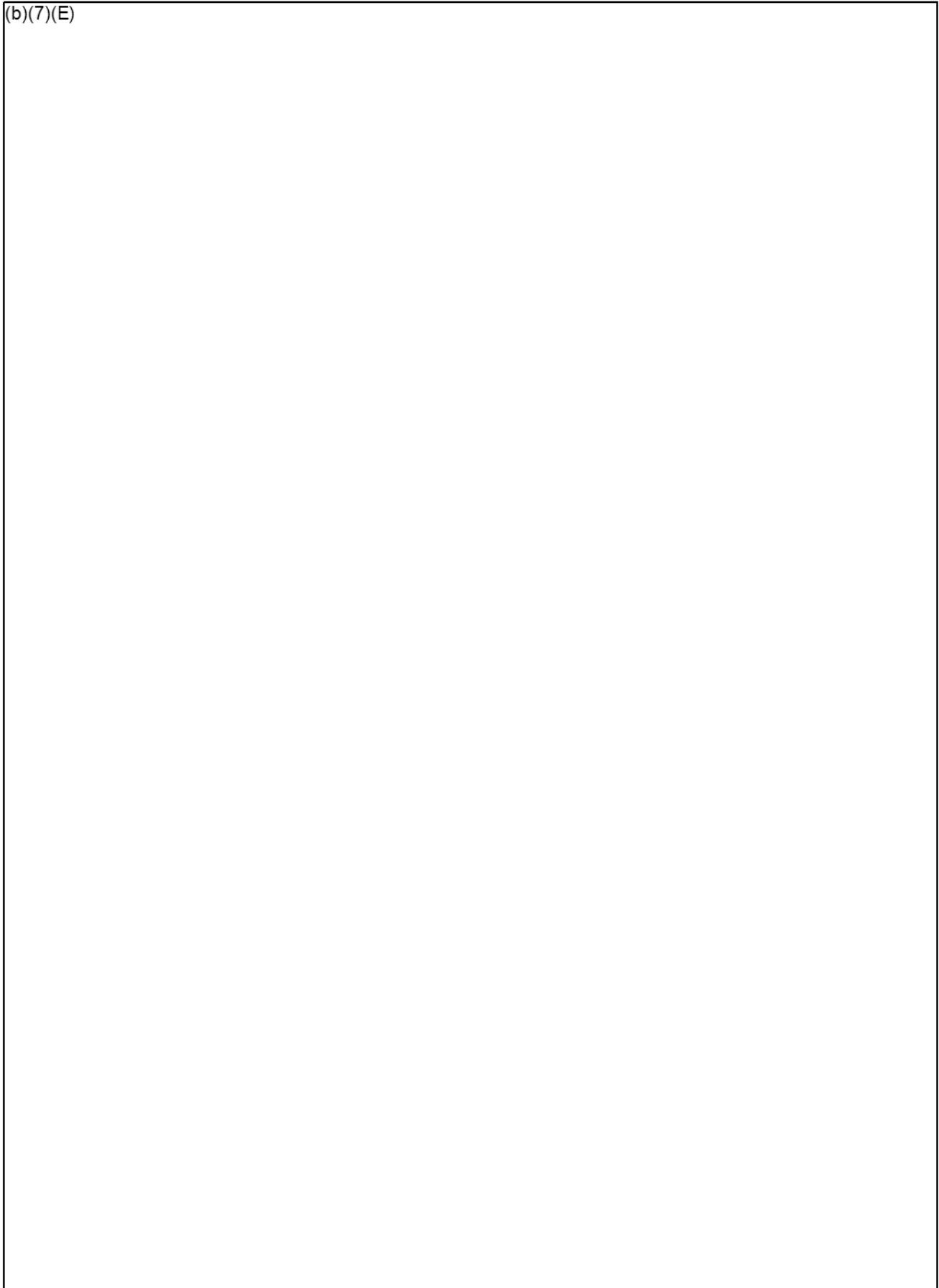
(b)(7)(E)

(b)(7)(E)

Appendix D

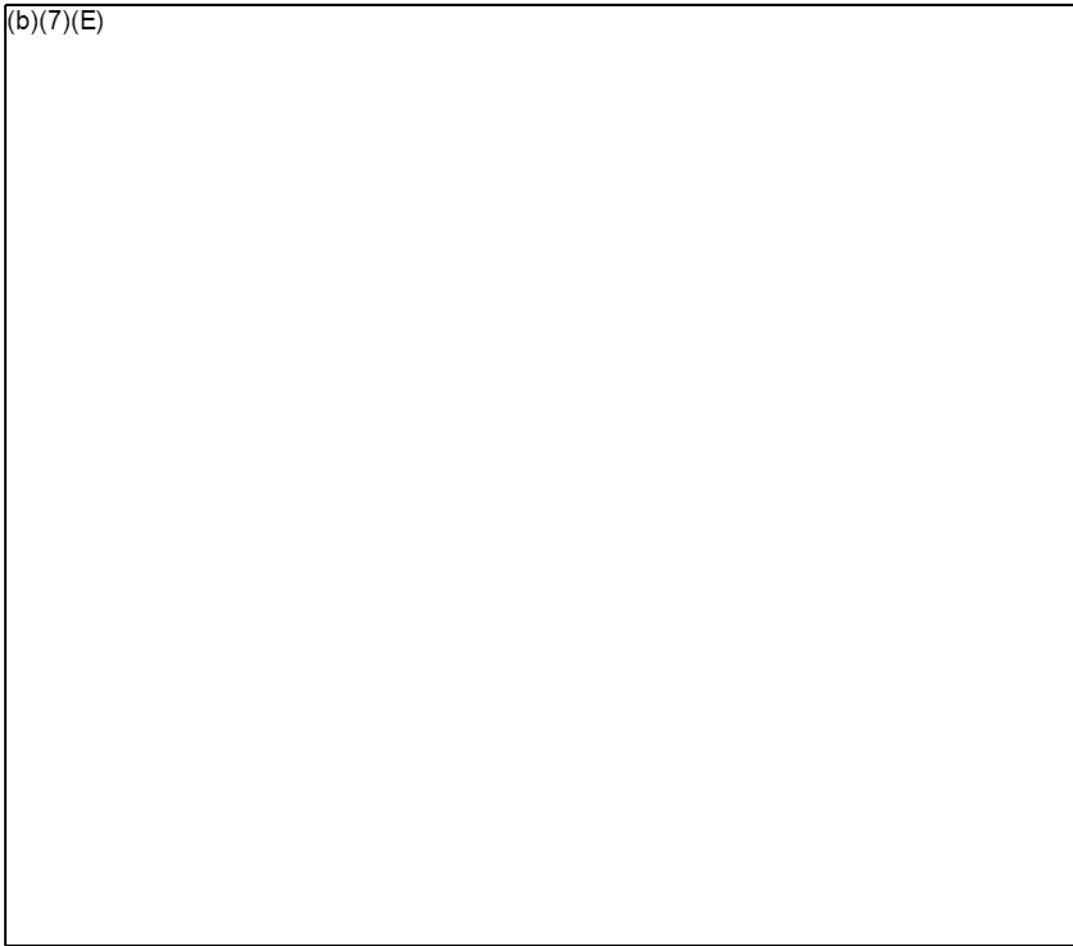
(b)(7)(E)

(b)(7)(E)



(b)(7)(E)


(b)(7)(E)



(b)(7)(E)

Appendix F

(b)(7)(E)



(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

2021-icli-00031 231

SUPERSEDED DOCUMENTS

The Human Smuggling and Trafficking Investigations Handbook supersedes the following documents:

Homeland Security Investigations Memorandum

1. Domestic and International Undercover Alien Smuggling Investigations (March 23, 2012)

Office of Investigations Memoranda

1. Human Trafficking Notification Requirements (April 30, 2010)
2. New Project Code 6AB for ICE HT Outreach Campaign (March 1, 2009)
3. Extraterritorial Criminal Strike Force (August 1, 2008)
4. Options and Forms of Immigration Relief for Victims and Witnesses in ICE Investigations (January 22, 2008)
5. ICE Trafficking in Persons Strategy (ICE TIPS): Responding to Trafficking Victims Leads (July 27, 2007)
6. Trafficking in Persons Assessment (December 17, 2006)
7. Definitions of “Human Smuggling” and “Human Trafficking” (December 13, 2004)
8. Standard Operating Procedure Domestic and International Transportation of Undocumented Aliens (December 3, 2004)
9. Standard Operating Procedure Human Smuggling Proprietary Safe House Operations (March 8, 2004)

U.S. Immigration and Naturalization Service Special Agent Field Manual

Chapter 27 of the U.S. Immigration and Naturalization Service Special Agent Field Manual entitled, “Smuggling Investigations,” was cancelled by the Human Smuggling and Trafficking Unit on August 12, 2010.

ACRONYMS

ACTeam	Anti-Trafficking Coordination Team
AD	Assistant Director
AIRG	Asset Identification and Removal Group
AO	Asylum Officer
AOR	Area of Responsibility
ASR	Administrative Stay of Removal
AUSA	Assistant United States Attorney
CBP	U.S. Customs and Border Protection
C.F.R.	Code of Federal Regulations
CI	Confidential Informant
CP	Continued Presence
CUC	Certified Undercover Operation
DAD	Deputy Assistant Director
DHS	Department of Homeland Security
DOJ	Department of Justice
DRO	Detention and Removal Operations
DUCS	Division of Unaccompanied Children's Services
EAD	Executive Associate Director
ECT	Extraterritorial Criminal Travel
ENFORCE	Enforcement Case Tracking System
EOIR	Executive Office for Immigration Review
ERO	Enforcement and Removal Operations
ESWP	Exigent Security for Witnesses Program
FOJC	Field Office Juvenile Coordinator
FOUO	For Official Use Only
HB	Handbook
HHS	Department of Health and Human Services
HQ	Headquarters
HRSP	Human Rights and Special Prosecutions
HSI	Homeland Security Investigations
HSO	Human Smuggling Organization
HSTC	Human Smuggling and Trafficking Center
HSTU	Human Smuggling and Trafficking Unit
HTO	Human Trafficking Organization
HTPU	Human Trafficking Prosecution Unit
ICE	U.S. Immigration and Customs Enforcement
INA	Immigration and Nationality Act
IOC2	International Organized Crime and Intelligence Operations Center
IP	Internet Protocol
IPAS	Illicit Pathways Attack Strategy
ISD	Investigative Services Division

ISP	Internet Service Provider
ISU	Investigative Support Unit
LEPS	Law Enforcement Parole Section
NGO	Non-Governmental Organization
NHTRC	National Human Trafficking Response Center
OAM	Office of Air and Marine
OBP	Office of Border Patrol
OCC	Office of the Chief Counsel
OCDETF	Organized Crime Drug Enforcement Task Force
OFO	Office of Field Operations
OI	Office of Investigations
ORR	Office of Refugee Resettlement
POE	Port of Entry
RFI	Request for Information
RICO	Racketeer Influenced and Corrupt Organization
ROI	Report of Investigation
SA	Special Agent
SAC	Special Agent in Charge
SCR	Significant Case Report
SEVIS	Student and Exchange Visitor Information System
SIA	Special Interest Alien
SIR	Significant Incident Report
SOD	Special Operations Division
SPBP	Significant Public Benefit Parole
SRT	Special Response Team
SUA	Specified Unlawful Activity
TOC	Transnational Organized Crime
TCPSD	Transnational Crime and Public Safety Division
TVPA	Trafficking Victims Protection Act
TVPRA	Trafficking Victims Protection Reauthorization Act
UCA	Undercover Agent
UDA	Undocumented Alien
USAO	U.S. Attorney's Office
U.S.C.	United States Code
USCIS	U.S. Citizenship and Immigration Services
VAC	Victim Assistance Coordinator
VAP	Victim Assistance Program
VAS	Victim Assistance Specialist

Homeland Security Investigations
Office of the Executive Associate Director

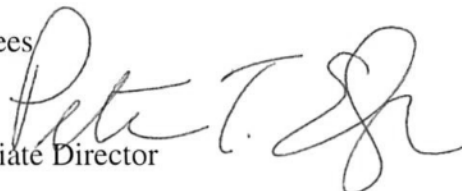
U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536



U.S. Immigration
and Customs
Enforcement

FEB 21 2017

MEMORANDUM FOR: All HSI Employees

FROM: Peter T. Edge 
Executive Associate Director

SUBJECT: ^{FEB 21 2017} Implementing the President's Border Security and Interior
Immigration Enforcement Policies

On February 21, 2017, Secretary Kelly issued the attached memoranda, "Implementing the President's Border Security and Immigration Enforcement Improvements Policies," and "Enforcement of the Immigration Laws to Serve the National Interest." These new polices outline the role of the Department of Homeland Security (DHS) in the implementation of Executive Order (E.O.) 13767, "Border Security and Immigration Enforcement Improvements," 82 Fed. Reg. 8793 (Jan. 25, 2017), and E.O. 13768, "Enhancing Public Safety in the Interior of the United States," 82 Fed. Reg. 8799 (Jan. 25, 2017). Effective immediately, Homeland Security Investigations (HSI) will implement this direction from the Secretary, with particular guidance as set forth below. Additionally, U.S. Immigration and Customs Enforcement (ICE) is reviewing all existing policies and guidance documents and will revise or rescind relevant policies in order to ensure consistency with the E.O.¹

A. Enforcement Policy

Effective immediately, HSI special agents may take enforcement action against all removable aliens encountered in the course of their duties. As always, special agents, in coordination with Enforcement and Removal Operations (ERO), must make an individualized custody determination in every case, prioritizing detention resources on aliens subject to expedited removal and aliens removable on any criminal ground, security or related ground, or for grounds related to fraud or material misrepresentation. Under the terms of the E.O., DHS will no longer exempt classes or categories of removable aliens from potential enforcement.

¹ With the exception of the June 15, 2012 memo, "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children," and the November 20, 2014 memo, "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children and with Respect to Certain Individuals Who Are the Parents of U.S. Citizens or Permanent Residents."

SUBJECT: Implementing the President's Border Security and Interior Immigration Enforcement Policies

Additionally, regardless of the basis of removability, HSI special agents should prioritize efforts to remove aliens who:

- (1) Have been convicted of any criminal offense;
- (2) Have been charged with any criminal offense that has not been resolved;
- (3) Have committed acts which constitute a chargeable criminal offense;
- (4) Have engaged in fraud or willful misrepresentation in connection with any official matter before a governmental agency;
- (5) Have abused any program related to receipt of public benefits;
- (6) Are subject to a final order of removal but have not complied with their legal obligation to depart the United States; or
- (7) In the judgment of an immigration officer, otherwise pose a risk to public safety or national security.

Aliens listed above do not necessarily have to be placed in removal proceedings based on a criminal ground of inadmissibility or removability. Instead, special agents should prioritize individuals within the above priorities for removal proceedings based on any lawfully available removal grounds.

(b)(7)(E)

SUBJECT: Implementing the President's Border Security and Interior Immigration Enforcement Policies

(b)(7)(E)

C. Detention Policy

The agency is currently expanding detention space to support the E.O.'s termination of "catch-and-release" policies.² HSI, in close consultation with ERO, will work to detain aliens pending a final determination of whether they will be removed from the United States, including a determination regarding eligibility for immigration relief and protection. HSI special agents should only release from detention an alien detained pursuant to section 235(b) of the Immigration and Nationality Act (INA) on a case-by-case basis, in accordance with applicable statutes and regulations, in the following situations:

- (1) When removing the alien from the United States pursuant to statute or regulation;
- (2) When the alien obtains an order granting relief or protection from removal or DHS determines that the individual is a U.S. citizen, national of the United States, or an alien who is a lawful permanent resident, refugee, asylee, holds temporary protected status, or holds a valid immigration status in the United States;
- (3) A Special Agent-in-Charge consents to the alien's withdrawal of an application for admission, and the alien contemporaneously departs from the United States;
- (4) When required to do so by statute, or to comply with a binding settlement agreement or order issued by a competent judicial or administrative authority;
- (5) A Special Agent-in-Charge authorizes the alien's parole pursuant to section 212(d)(5) of the INA with the written concurrence of the Deputy Director of ICE, except in exigent circumstances such as medical emergencies where seeking prior approval is not practicable. In those exceptional instances, any such parole will be reported to the Deputy Director as expeditiously as possible; or
- (6) When an arriving alien processed under the expedited removal provisions of section 235(b) has been found to have established a "credible fear" of persecution or torture by an asylum officer or an immigration judge, provided that such an alien affirmatively establishes to the satisfaction of an immigration officer his or her identity, that he or she presents neither a security risk nor a risk of absconding, and provided that he or she agrees to comply with any additional conditions of release imposed to ensure public safety and appearance at any removal hearings.

² The implementation of this provision may be dependent upon the deployment of a surge of immigration judges and asylum special agents and the acquisition of additional detention space, as determined by the Secretary.

SUBJECT: Implementing the President's Border Security and Interior Immigration Enforcement Policies

As the agency works to expand its detention capacity, detention of all such individuals may not be possible. Detention resources should be prioritized based upon potential danger and risk of flight if an individual alien is not detained.

D. Release and Parole Policy

HSI special agents should process requests for parole or other release sparingly, and only in individual cases where, after careful consideration of the circumstances, the officer or agent believes that the release would serve the best interests of the United States because of demonstrated urgent humanitarian reasons or significant public benefit. Parole or other release, with all available safeguards, may also be warranted in instances where detention capacity limits the agency's ability to detain the alien consistent with legal requirements, including court orders and settlement agreements.

Agency policy establishing standards and procedures for the parole of certain arriving aliens found to have a credible fear of persecution or torture will remain in full force and effect until further evaluation is completed and additional guidance is issued.³ HSI special agents are reminded, however, to apply ICE policy consistent with its plain language, and to ensure that the alien is held to his or her burden of establishing identity and that his or her release will not pose a danger or risk of flight. There is no presumption that an individual alien's release would not pose a danger or risk of flight.

E. Processing and Treatment of Unaccompanied Alien Minors

HSI special agents will continue to comply with the requirements of the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA) and the *Flores* Settlement Agreement, including all implementing policies and procedures, to ensure that all children, including unaccompanied alien children, are provided special protections to ensure that they are properly processed and receive appropriate care and placement when they are encountered by DHS agents and agents. Mexican and Canadian unaccompanied alien children may be permitted to withdraw their application for admission and return to Mexico or Canada after proper coordination with the Mexican or Canadian Consulate has been completed. Unaccompanied alien children who are permitted to withdraw may be repatriated at the nearest port of entry to Mexican or Canadian Consulate officials at a time designated by the consulate official.

³ Current agency policy is set forth in ICE Policy No. 11002.1: Parole of Arriving Aliens Found to Have a Credible Fear of Persecution or Torture, dated December 8, 2009, which is available [here](#). The policy is implicated by pending litigation before the U.S. Supreme Court in *Jennings v. Rodriguez*, No. 15-1204, and as noted in the Secretary's February 17, 2017 memorandum, "Implementing the President's Border Security and Immigration Enforcement Improvements Policies," is subject to further review and evaluation pending ongoing implementation of Executive Order 13767.

SUBJECT: Implementing the President's Border Security and Interior Immigration Enforcement Policies

F. No Private Right of Action

This document provides only internal ICE policy guidance, which may be modified, rescinded, or superseded at any time without notice. This guidance is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the otherwise lawful enforcement or litigation prerogatives of ICE.

In implementing these policies, I direct all HSI employees to consult with legal counsel through proper chain of command, to ensure compliance with all applicable laws, including the Administrative Procedure Act.

Page 240

Withheld pursuant to exemption

Duplicate

of the Freedom of Information and Privacy Act

Page 241

Withheld pursuant to exemption

Duplicate

of the Freedom of Information and Privacy Act

Page 242

Withheld pursuant to exemption

Duplicate

of the Freedom of Information and Privacy Act

(b)(7)(E)

www.ice.gov

(b)(7)(E)

(b)(7)(E)

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

ICE Directive 14019.1: Reporting Protocol Following a Designated National Security Event or U.S.-based International Terrorist Attack

Issue Date: December 3, 2019

Superseded: None.

Federal Enterprise Architecture Number: 306-112-002b

1. **Purpose/Background.** U.S. Immigration and Customs Enforcement (ICE) requires consistent processes and procedures to mitigate the after-effects of a designated national security event (NSE) or U.S.-based international terrorist (IT) attack. This Directive establishes a unified reporting protocol for law enforcement and intelligence information within ICE to eliminate duplication, minimize operational burdens in the field, and ensure accurate, timely, and comprehensive post-attack reporting to ICE Leadership.
2. **Policy.** It is ICE policy that an internal unified reporting protocol is followed in response to a designated NSE or IT attack. This protocol includes all ICE investigative efforts and entities, and all activities, actions, and initiatives performed in support of the post-attack response. The reporting protocol provides guidance for all information and intelligence that is gathered, investigative leads that are identified and/or pursued, and response activities that are conducted, whether they are directly or indirectly related to the associated Joint Terrorism Task Force (JTTF) investigation.

All information collected, recorded, and actioned by ICE Enforcement and Removal Operations (ERO) and/or Homeland Security Investigations (HSI) during a potential NSE or IT attack will be reported directly and exclusively to HSI, National Security Investigations Division (NSID), National Security Unit (NSU), Counterterrorism Section (CTS). CTS will lead the agency's post-attack reporting and vetting through the applicable command post in coordination with the Federal Bureau of Investigation's (FBI) Counterterrorism Division (CTD). The FBI will determine when an event is a U.S.-based IT attack. The Assistant Director (AD) of HSI/NSID will designate an event as a NSE, as appropriate.¹

3. **Definitions.** The following definitions apply for purposes of this Directive only:
 - 3.1. **ICE Leadership.** The Director and Deputy Director.
 - 3.2. **International Terrorism.** Acts of violence, terror, or intimidation perpetrated by individuals and/or groups inspired by or associated with designated foreign terrorist organizations or nations (state sponsored).

¹ A U.S.-based IT attack is always a designated NSE, but not all designated NSEs are U.S.-based IT attacks.

3.3. National Security Event. Any incident that involves potential or actual terrorist acts or terrorist threats, where such acts are within the federal criminal jurisdiction of the United States and require the FBI JTTF to coordinate the activities of the U.S. Government law enforcement community.

3.4. U.S.-based IT Attack. Any attack within the United States or any of its territories that has been determined to be, or is being investigated as, an act of international terrorism by the FBI.

4. Responsibilities.

4.1. The Executive Associate Director (EAD) for HSI is responsible for:

- 1) Ensuring compliance with the provisions of this Directive within his/her Directorate;
- 2) Notifying ICE Leadership when the AD for HSI/NSID has designated an event as a NSE;
- 3) Notifying ICE Directorates and Program Offices, including EADs, Program Heads, and the affected Special Agents in Charge (SACs) that the AD for HSI/NSID has designated an event as a NSE and/or to return to normal domestic reporting protocols when the investigative response reaches its natural conclusion; and
- 4) Reporting all post-attack or post-threat response activities within his/her Directorate to the ICE Director and, as directed by the ICE Director, to the applicable Department of Homeland Security (DHS) leadership.

4.2. The EAD for ERO is responsible for:

- 1) Ensuring compliance with the provisions of this Directive within his/her Directorate; and
- 2) Disseminating declaration of an event as a U.S.-based IT attack or designation as a NSE event, and all associated event information, within his/her respective Directorate, including to ERO Field Office Directors (FODs).

4.3. The AD for HSI/NSID is responsible for:

- 1) Serving as the primary ICE official responsible for coordination with FBI/CTD and for designating an event as a NSE, as appropriate;
- 2) Notifying the EAD for HSI when the FBI determines an event to be a U.S.-based IT attack or when an event is designated as a NSE by the AD for HSI/NSID;

- 3) Notifying and coordinating with the AD for HSI/Domestic Operations when the FBI determines an event to be a U.S.-based IT attack or when an event is designated as a NSE by the AD for HSI/NSID, to ensure that the unified reporting protocol is initiated;
- 4) Coordinating with the AD for the U.S. Citizenship and Immigration Services (USCIS)/Fraud Detection and National Security (FDNS) Directorate's Associate Director to invoke the procedures outlined in the USCIS' *Records Operation Handbook* associated with a NSE;² and
- 5) Determining and notifying the EADs for ERO and HSI when to return to normal domestic reporting protocols.

4.4. The **NSU Unit Chief** is responsible for implementing and coordinating the provisions of this Directive within the applicable area of responsibility (AOR), and reporting all activities of ICE Directorates and Program Offices to ICE Leadership through established reporting channels.

4.5. The **CTS Section Chief**, in coordination with the CTS Team Lead, is responsible for receiving, consolidating, and reporting all U.S.-based IT attack or designated NSE information, intelligence, and activities of ICE Directorates and Program Offices to ICE Leadership through established reporting channels.

4.6. The **CTS Team Lead** is responsible for handling post-attack/designated NSE communications, coordinating with ICE special agents and officers in their affected AORs, and serving as the primary point of contact for all A-Files maintained by USCIS.

4.7. **ICE Special Agents, ERO Officers, and Support Staff**³ are responsible for:

- 1) Documenting all unclassified U.S.-based IT attack or NSE-related information, intelligence, and activities in the HSI Investigative Case Management system;⁴ and
- 2) Disseminating all information to the HSI supervisor overseeing ICE JTTF equities within their AOR, as appropriate.

5. Procedures/Requirements.

² These procedures designate ICE HSI as the lead agency within DHS responsible for requesting, receiving, and disseminating all Alien File (A-File) information to the FBI, affected JTTFs, other law enforcement agencies, and the Intelligence Community.

³ Support Staff includes but is not limited to any intelligence, analytic, and logistical staff, as designated by ERO and HSI.

⁴ In the event that ERO personnel do not have access to ICM to document the identified unclassified information, HSI Special Agents will collect the related information from ERO and ensure that it is documented in ICM.

5.1. Post-Attack Procedures.

- 1) The AD for HSI/NSID will immediately notify the EADs for ERO and HSI when the FBI declares an event to be a U.S.-based IT attack or when an event is designated to be a NSE.
- 2) The EADs for ERO and HSI will immediately disseminate this event declaration or designation, and all associated event information, within their respective Directorates, including to ERO FODs and HSI SACs, respectively.
- 3) The EADs for ERO and HSI will provide the NSU Unit Chief and CTS Section Chief with all respective headquarters points of contact who will identify and/or receive any information during the investigative response.
- 4) HSI SAC office first-line supervisors and/or HSI special agents will report to the CTS Section Chief and/or Team Lead all JTTF-related investigative efforts and other activity associated with the post-attack response.
- 5) ERO Field Office first-line supervisors and/or ERO Deportation Officers will report all JTTF-related investigative efforts to their local JTTF HSI Group Supervisor and/or Resident Agent in Charge throughout the duration of the U.S.-based IT attack or designated NSE.⁵ In situations where ICE JTTF representation in the affected AOR does not exist, ICE personnel designated to assist in the response effort will comply with the above stated procedures.
- 6) Immediately upon notification that an event has been declared to be a U.S.-based IT attack or designated as a NSE, all related field reporting will transition to CTS for centralized reporting to ICE and DHS Leadership.
- 7) Any action by ICE Directorates or Program Offices related to the U.S.-based IT attack or designated NSE response effort must be coordinated with CTS. This includes any internal or external reporting requests.
- 8) In situations in which ICE Directorates or Program Offices develop information they deem important to the investigation and/or anticipate a need for Intelligence Information Reports (IIRs), press releases, or similar material, these offices will obtain prior concurrence from CTS, which will coordinate with the affected JTTF prior to action.
 - a) ICE-sourced information that relates to a U.S.-based IT attack or designated NSE that would require the HSI/Office of Intelligence to draft an IIR for the purposes

⁵ ICE Policy memo “U.S. Immigration and Customs Enforcement Reporting Following a Designated National Security Event/U.S.-based Terrorist Attack”, dated April 3, 2018.

of complying with mandates, public laws, and Presidential Executive Orders for a “Duty to Warn,” will be immediately provided to CTS for awareness and determination of any immediate operational action that may need to be taken by the JTTF.

- b) Prior to the release of any IIR(s) by the HSI/Office of Intelligence related to the U.S.-based IT attack or designated NSE, the HSI/Office of Intelligence will provide CTS with an advance copy of the pre-released IIR(s) and the amount of time available for deconfliction prior to publication.
- 9) CTS will obtain the name of an HSI Special Agent in the field who will receive hard copies of any USCIS A-Files deemed necessary by investigators and act as the Local A-File Point of Contact (POC), and CTS will provide this POC to USCIS.
- 10) The Local A-File POC will coordinate with the CTS Team Lead prior to ordering any hard copy A-Files from USCIS to ensure that a soft copy has been obtained in advance for immediate triage, and that production of comprehensive HSI subject reports can be initiated

5.2. Culmination of Investigative Response.


- 1) Once the investigative response culminates, and at the discretion of CTS, NSID will communicate to the EADs for ERO and HSI that the investigative response has reached its natural conclusion.
- 2) The EADs will then direct their respective Directorates to return to normal domestic reporting protocols.

6. Recordkeeping. All relevant communications disseminated by ICE Directorates and Program Offices through CTS will be memorialized, as appropriate, in accordance with established NSID post-attack reporting products and guidelines. Any records created or received as part of this directive must be maintained in accordance with a National Archives and Records Administration-approved retention schedule. If an applicable schedule does not exist the records must be treated as permanent until a retention schedule is developed and approved. Records will be stored/maintained within CTS holdings in accordance with established ICE records management procedures.

7. Authorities/References.

- 7.1.** Memorandum from Deputy Director and Senior Official Performing the Duties of the Director Thomas D. Homan, *U.S. Immigration and Customs Enforcement Reporting Following a Designated National Security Event/U.S.-based Terrorist Attack*, Apr. 3, 2018.

- 7.2. Memorandum from HSI Deputy Executive Associate Director (EAD) and Senior Management Official performing the Duties of the EAD Derek N. Benner, *HSI Domestic Field Office Reporting to NSID on a Designated NSE/U.S.-based Terrorist Attack*, Dec. 8, 2017.
- 7.3. Memorandum from USCIS Associate Director, Enterprise Services Division Soraya Correa, *Immigration File Sharing and Sequestration Procedures Used During a National Security Event*, Feb. 5, 2014.
- 7.4. ICE Directive 10086.1, *Oversight of ICE Personnel Serving on Federal Investigative Task Forces*, Mar. 25, 2016.
8. **Attachments.** None.
9. **No Private Right.** This document provides only internal ICE policy guidance, which may be modified, rescinded, or superseded at any time without notice. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the otherwise lawful enforcement or litigative prerogatives of ICE.

 12/3/19

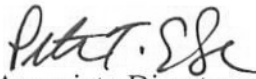
Matthew T. Albence
Deputy Director and Senior Official Performing the Duties of the Director
U.S. Immigration and Customs Enforcement



**U.S. Immigration
and Customs
Enforcement**

APR 03 2018

MEMORANDUM FOR: Thomas D. Homan
Deputy Director and
Senior Official Performing the Duties of the Director

THROUGH: Peter T. Edge 
HSI Executive Associate Director and
Senior Official Performing the Duties of the Deputy Director

FROM: Derek N. Benner /s/
HSI Deputy Executive Associate Director and
Senior Official Performing the Duties of the Executive Associate
Director

SUBJECT: U.S. Immigration and Customs Enforcement Reporting Following
a Designated National Security Event/U.S.-based Terrorist Attack

Purpose:

Homeland Security Investigations (HSI) proposes establishing a unified reporting protocol for the Deputy Director and Senior Official Performing the Duties of the Director following the declaration of a National Security Event (NSE)/U.S.-based terrorist attack that is deemed International Terrorism. This memorandum recommends having all entities within U.S. Immigration and Customs Enforcement (ICE) report directly to HSI National Security Investigations Division (NSID) Counter-Terrorism Section (CTS) if such an event occurs. This process will implement a unified command structure and ensure accurate and timely reporting to ICE leadership. Situational reporting will continue throughout the duration of the immediate investigative response, until directed to return to normal reporting protocol by NSID. This protocol does not change any other reporting requirements outside of a designated NSE. Further, this memorandum will be followed by an ICE-wide Directive memorializing this policy establishing a unified reporting protocol and outlining roles and responsibilities.

Background:

The United States has faced an increased threat posture as a result of numerous U.S.-based terrorist attacks. Following these attacks, ICE leadership requires a stream of timely and accurate reporting to make crucial decisions to protect American lives.

Subject: U.S. Immigration and Customs Enforcement Reporting Following a Designated National Security Event/U.S.-based Terrorist Attack

Page 2

NSID is uniquely situated to provide the most accurate real-time reporting, based on its placement and access within the International Terrorism Operations Section (ITOS) of the Federal Bureau of Investigation's (FBI) Counterterrorism Division (CTD). ITOS is the command and control center for all U.S.-based terrorism events; since 2001, NSID CTS has been embedded at ITOS to streamline coordination on all Joint Terrorism Task Force (JTTF) investigations, threat streams, and counter-terrorism responses.

Following several post-attack after-action reviews, HSI JTTF agents have expressed frustration about receiving redundant requests for similar information and updates from various entities within ICE in the aftermath of the attack. These redundancies create undue distractions in the field and can ultimately lead to inaccurate (and sometimes unvetted) reporting to ICE leadership.

Discussion:

(b)(7)(E)

(b)(7)(E)

The primary function of an HSI JTTF Special Agent or Enforcement and Removal Operations (ERO) officer is to mitigate threats and assist in the resulting investigation. Due to the massive volume of information gathered during the initial stages of an International Terrorism event, it is impractical to have nonlinear reporting to ICE leadership and concurrently conduct crucial investigative and enforcement activities in the midst of a terrorist attack. At present, both HSI

and ERO staff the JTTFs in the field and, per pre-established policy (ICE Directive 10086.1 paragraph 5), HSI is responsible for ICE consolidated reporting. To maintain the single flow of information, the HSI supervisor will provide updates to NSID CTS during these critical incidents.

In situations where ICE components develop information they deem important to the counter-terrorism investigation, including leads, and/or anticipate a need for possible production of Intelligence Information Reports or press releases, these offices will obtain prior concurrence from NSID CTS and the affected JTTF office prior to action. This includes the issuance of administrative subpoenas outside of the JTTF construct. Leads should be provided to CTS and the affected JTTF concurrently for review.

All events begin as a domestic investigation before being classified as an NSE/U.S.-based terrorist attack. For HSI, since the initial conduit for all reporting from the field is Domestic Operations, NSID will immediately advise HSI Domestic Operations, and all other ICE reporting components when NSID CTS is assuming reporting responsibilities following the declaration of an NSE. NSID CTS will continue to keep all ICE components advised of ICE JTTF field activity. Finally, NSID CTS will advise HSI Domestic Operations and all other ICE reporting components when the event will be managed under normal reporting protocols.

Recommendation:

I recommend that all entities within ICE report directly to HSI NSID CTS following the declaration of an NSE/U.S.-based terrorist attack that is deemed to be International Terrorism. This process will initiate a command structure and ensure accurate and timely reporting to ICE leadership. HSI NSID CTS will subsequently report all information through the HSI NSID Assistant Director to ICE leadership. Upon approval, these policies and procedures will be codified in an ICE Directive.

I respectfully request approval of this recommendation to ensure HSI, ICE, and ultimately U.S. Department of Homeland Security leadership is provided accurate, consistent, and timely reporting during, and in the immediate days following, responses to an NSE/U.S.-based terrorist attack.

Approve  Disapprove _____
Modify _____ Needs Discussion _____



Transnational Organized Crime Rewards Program (TOCRP)
Program Overview

(U) The TOCRP is one of five tools introduced in the President’s Strategy to Combat Transnational Organized Crime (TOC), which recognizes transnational criminal organizations (TCOs) are rapidly expanding in size and scope. The authority to offer rewards for TOC was signed into law on January 15, 2013 and complements the Narcotics Rewards Program (NRP) by authorizing rewards of up to \$25 million for information leading to the arrest and/or conviction of TCOs, including human trafficking, money laundering, cybercrime, and trafficking in arms, wildlife, counterfeits, and other goods. The program is managed by the Bureau of International Narcotics and Law Enforcement Affairs (INL).

(U) Eligibility

- Major international TCOs operating outside the United States and involved in transnational crimes, such as:
 - human trafficking;
 - money laundering;
 - maritime piracy;
 - cybercrime;
 - trafficking in arms;
 - counterfeits;
 - U.S. technology transfers; and
 - other illicit goods.

(SBU) Implementation Process Interagency Review Committee:

- An interagency rewards committee (IRC) must reach consensus in nominating targets and approving rewards amounts and payments with final approval by the Secretary of State.

(b)(7)(E)

- INL/GPP Director, or Division Chief, chairs the IRC review.

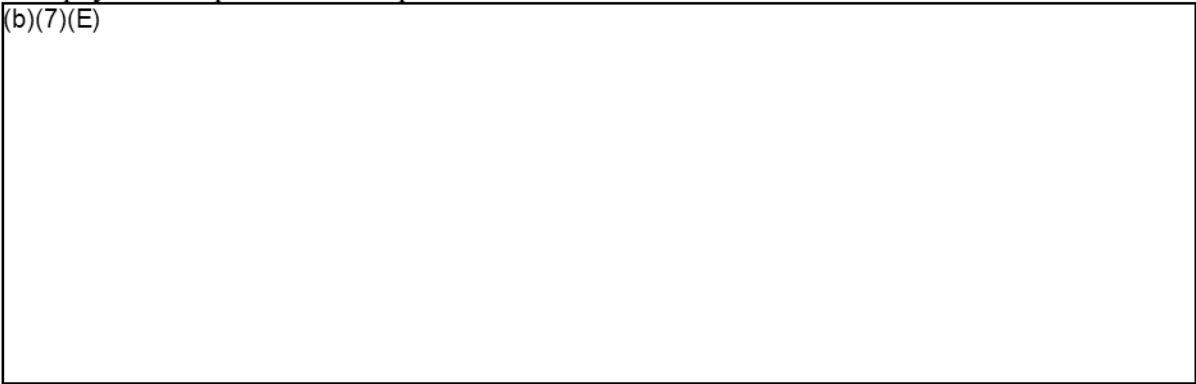
(SBU) Target Designation

(b)(7)(E)

(SBU) Rewards Payment

- If an informant(s) has provided information leading to the arrest and/or conviction of the approved target, a U.S. government agency or overseas post may then submit a reward payment request to the Department of State for consideration.

(b)(7)(E)



- Once nominating agency confirms payment, INL works with the K Fund manager in M/EDCS to complete the required congressional notifications. This concludes the TOCRP payment process.



Narcotics Rewards Program

Program Overview

The Narcotics Rewards Program (NRP) was established by Congress in 1986 as an important tool to assist U.S. law enforcement in identifying and bringing to justice the major violators of U.S. narcotics laws. Under this program, the Secretary of State has statutory authority (Title 22, United States Code, Section 2708) to pay rewards of up to \$25 million for information leading to the arrest and/or conviction of major narcotics traffickers who operate outside of the United States and send major quantities of drugs into the United States, causing death, addiction, and violence to spread throughout the United States. Generally, rewards are limited up to \$5 million per individual for this program.

The Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) manages this program. INL works in close coordination with the Department of Justice, Drug Enforcement Administration, Federal Bureau of Investigation, Homeland Security Investigations, and other interested U.S. agencies, such as the Department of Treasury and Central Intelligence Agency, to ensure that the program is responsive to priority regions and efforts and fully complements the U.S. National Drug Strategy.

Since its inception, the NRP has brought to justice 73 foreign major violators of United States narcotics laws, with more than \$130 million paid to 129 reward program participants.

Information through the NRP successfully contributed to operations against and/or arrests of Haji Bashir Noorzai, an Afghan heroin warlord and Taliban ally; Javier Arellano-Felix, the head of Mexico's largest and most violent trafficking organization, the Arellano-Felix Organization; Arturo Beltran-Levy, a major Mexican trafficker and leader of the Sinaloa Cartel responsible for importing tons of cocaine to the U.S.; key leaders of the Colombian Norte Valle Cartel; and violent narcotics trafficking networks operating in South America. There are currently reward offers for major narcotics traffickers including Mexican cartels, Asian heroin kingpins, and Colombian FARC leaders. All current NRP targets can be found at www.state.gov/j/inl/narc/rewards.



Narcotics and Transnational Organized Crime Rewards Programs

Targets Designation Request Paper

Submission: Agencies are strongly encouraged to consult with the rewards program coordinators (INL-Sanctions-DL@state.gov) during the drafting process to ensure all requirements are met. U.S. government agency headquarters should send a formal request on agency letterhead to the Assistant Secretary of State for International Narcotics and Law Enforcement Affairs (INL) Kirsten D. Madison requesting a reward offer. Posts may send nominations via cable, restricting distribution to the rewards program coordinators and using the “SNAR,” “KCRM,” and “KTOC” TAGS.

Approvals: INL chairs and coordinates the Interagency Rewards Committee (IRC) review and, when necessary, meetings with IRC members to ensure appropriate agency and bureau approval.

(b)(7)(E)

Contacts: NIPR: INL-Sanctions-DL@state.gov or SIPR: INL-Sanctions-DL@state.sgov.gov

(b)(7)(E)

Page 259

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

(b)(7)(E)

Questions

If you have any questions, need additional information, or would like to discuss any of the rewards programs, please contact the Rewards Program Manager at INL-Sanctions-DL@state.gov.

22 U.S. Code § 2708. Department of State rewards program

(a) Establishment

(1) In general

There is established a program for the payment of rewards to carry out the purposes of this section.

(2) Purpose

The rewards program shall be designed to assist in the prevention of acts of international terrorism, international narcotics trafficking, serious violations of international humanitarian law, transnational organized crime, and other related criminal acts.

(3) Implementation

The rewards program shall be administered by the Secretary of State, in consultation, as appropriate, with the Attorney General.

(b) Rewards authorized

In the sole discretion of the Secretary (except as provided in subsection (c)(2)) and in consultation, as appropriate, with the heads of other relevant departments or agencies, the Secretary may pay a reward to any individual who furnishes information leading to—

(1) the arrest or conviction in any country of any individual for the commission of an act of international terrorism against a United States person or United States property;

(2) the arrest or conviction in any country of any individual conspiring or attempting to commit an act of international terrorism against a United States person or United States property;

(3) the arrest or conviction in any country of any individual for committing, primarily outside the territorial jurisdiction of the United States, any narcotics-related offense if that offense involves or is a significant part of conduct that involves—

(A) a violation of United States narcotics laws such that the individual would be a major violator of such laws;

(B) the killing or kidnapping of—

(i) any officer, employee, or contract employee of the United States Government while such individual is engaged in official duties, or on account of that individual's official duties, in connection with the enforcement of United States narcotics laws or the implementing of United States narcotics control objectives; or

(ii) a member of the immediate family of any such individual on account of that individual's official duties, in connection with the enforcement of United States narcotics laws or the implementing of United States narcotics control objectives; or

(C) an attempt or conspiracy to commit any act described in subparagraph (A) or (B);

(4) the arrest or conviction in any country of any individual aiding or abetting in the commission of an act described in paragraph (1), (2), (3), (8), (9), or (10);

(5) the prevention, frustration, or favorable resolution of an act described in paragraph (1), (2), (3), (8), (9), or (10), including by dismantling an organization in whole or significant part;

(6) the identification or location of an individual who holds a key leadership position in a terrorist organization or transnational organized crime group;

(7) the disruption of financial mechanisms of a foreign terrorist organization or transnational organized crime group, including the use by such organization or group of illicit narcotics production or international narcotics trafficking—

(A) to finance acts of international terrorism or transnational organized crime; or

(B) to sustain or support any terrorist organization or transnational organized crime group;

(8) the arrest or conviction in any country of any individual for participating in, primarily outside the United States, transnational organized crime;

(9) the arrest or conviction in any country of any individual conspiring to participate in or attempting to participate in transnational organized crime;

(10) the arrest or conviction in any country, or the transfer to or conviction by an international criminal tribunal (including a hybrid or mixed tribunal), of any foreign national accused of war crimes, crimes against humanity, or genocide (including war crimes, crimes against humanity, or genocide committed in Syria beginning in March 2011), as defined under the statute of such tribunal;

(11) the identification or location of any person who, while acting at the direction of or under the control of a foreign government, aids or abets a violation of section 1030 of title 18; or

(12) the disruption of financial mechanisms of any person who has engaged in the conduct described in sections [1] 2914(a) or 2914(b)(1) of this title.

(c) Coordination

(1) Procedures

To ensure that the payment of rewards pursuant to this section does not duplicate or interfere with the payment of informants or the obtaining of evidence or information, as authorized to the Department of Justice, the offering, administration, and payment of rewards under this section, including procedures for—

(A) identifying individuals, organizations, and offenses with respect to which rewards will be offered;

(B) the publication of rewards;

(C) the offering of joint rewards with foreign governments;

(D) the receipt and analysis of data; and

(E) the payment and approval of payment,

shall be governed by procedures developed by the Secretary of State, in consultation with the Attorney General.

(2) Prior approval of Attorney General required

Before making a reward under this section in a matter over which there is Federal criminal jurisdiction, the Secretary of State shall obtain the concurrence of the Attorney General.

(d) Funding

(1) Authorization of appropriations

Notwithstanding section 102 of the Foreign Relations Authorization Act, Fiscal Years 1986 and 1987 (Public Law 99-93; 99 Stat. 408), but subject to paragraph (2), there are authorized to be appropriated to the Department of State from time to time such amounts as may be necessary to carry out this section.

(2) Period of availability

Amounts appropriated under paragraph (1) shall remain available until expended.

(e) Limitations and certification

(1) Maximum amount

No reward paid under this section may exceed \$25,000,000, except as personally authorized by the Secretary of State if he determines that offer or payment of an award of a larger amount is necessary to combat terrorism or defend the Nation against terrorist acts. Without first making such determination, the Secretary may authorize a reward of up to twice the amount specified in this paragraph for the capture or information leading to the capture of a leader of a foreign terrorist organization.

(2) Approval

A reward under this section of more than \$100,000 may not be made without the approval of the Secretary.

(3) Certification for payment

Any reward granted under this section shall be approved and certified for payment by the Secretary.

(4) Nondelegation of authority

The authority to approve rewards of more than \$100,000 set forth in paragraph (2) may not be delegated.

(5) Protection measures

If the Secretary determines that the identity of the recipient of a reward or of the members of the recipient's immediate family must be protected, the Secretary may take such measures in connection with the payment of the reward as he considers necessary to effect such protection.

(6) Forms of reward payment

The Secretary may make a reward under this section in the form of money, a nonmonetary item (including such items as automotive vehicles), or a combination thereof.

(f) Ineligibility

An officer or employee of any entity of Federal, State, or local government or of a foreign government who, while in the performance of his or her official duties, furnishes information described in subsection (b) shall not be eligible for a reward under this section.

(g) Reports

(1) Reports on payment of rewards

Not later than 30 days after the payment of any reward under this section, the Secretary shall submit a report to the appropriate congressional committees with respect to such reward. The report, which may be submitted in classified form if necessary, shall specify the amount of the reward paid, to whom the reward was paid, and the acts with respect to which the reward was paid. The report shall also discuss the significance of the information for which the reward was paid in dealing with those acts.

(2) Annual reports

Not later than 60 days after the end of each fiscal year, the Secretary shall submit a report to the appropriate congressional committees with respect to the operation of the rewards program. The report shall provide information on the total amounts expended during the fiscal year ending in that year to carry out this section, including amounts expended to publicize the availability of rewards.

(3) Advance notification for international criminal tribunal rewards

Not less than 15 days before publicly announcing that a reward may be offered for a particular foreign national accused of war crimes, crimes against humanity, or genocide, the Secretary of State shall submit to the appropriate congressional committees a report, which may be submitted in classified form if necessary, setting forth the reasons why the arrest or conviction of such foreign national is in the national interests of the United States.

(4) Reports on rewards authorized

Not less than 15 days after a reward is authorized under this section, the Secretary of State shall submit to the appropriate congressional committees a report, which may be submitted in classified form if necessary to protect intelligence sources and methods, detailing information about the reward, including the identity of the individual for whom the reward is being made, the amount of the reward, the acts with respect to which the reward is being made, and how the reward is being publicized.

(h) Publication regarding rewards offered by foreign governments

Notwithstanding any other provision of this section, in the sole discretion of the Secretary, the resources of the rewards program shall be available for the publication of rewards offered by foreign governments regarding acts of international terrorism which do not involve United States persons or property or a violation of the narcotics laws of the United States.

(i) Media surveys and advertisements

(1) Surveys conducted

For the purpose of more effectively disseminating information about the rewards program, the Secretary may use the resources of the rewards program to conduct media surveys, including analyses of media markets, means of communication, and levels of literacy, in countries determined by the Secretary to be associated with acts of international terrorism.

(2) Creation and purchase of advertisements

The Secretary may use the resources of the rewards program to create advertisements to disseminate information about the rewards program. The Secretary may base the content of such advertisements on the findings of the surveys conducted under paragraph (1). The Secretary may purchase radio or television time, newspaper space, or make use of any other means of advertisement, as appropriate.

(j) Determinations of Secretary

A determination made by the Secretary under this section shall be final and conclusive and shall not be subject to judicial review.

(k) Definitions

As used in this section:

(1) Act of international terrorism

The term "act of international terrorism" includes—

(A) any act substantially contributing to the acquisition of unsafeguarded special nuclear material (as defined in paragraph (8) of section 6305 of this title) or any nuclear explosive device (as defined in paragraph (4) of that section) by an individual, group, or non-nuclear-weapon state (as defined in paragraph (5) of that section); and

(B) any act, as determined by the Secretary, which materially supports the conduct of international terrorism, including the counterfeiting of United States currency or the illegal use of other monetary instruments by an individual, group, or country supporting international terrorism as determined for purposes of section 4605(j)(1)(A) [2] of title 50.

(2) Appropriate congressional committees

The term "appropriate congressional committees" means the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate.

(3) Member of the immediate family

The term "member of the immediate family", with respect to an individual, includes—

(A) a spouse, parent, brother, sister, or child of the individual;

(B) a person with respect to whom the individual stands in loco parentis; and

(C) any person not covered by subparagraph (A) or (B) who is living in the individual's household and is related to the individual by blood or marriage.

(4) Rewards program

The term "rewards program" means the program established in subsection (a)(1).

(5) Transnational organized crime

The term "transnational organized crime"—

(A) means—

(i) racketeering activity (as such term is defined in section 1961 of title 18) that involves at least one jurisdiction outside the United States; or

(ii) any other criminal offense punishable by a term of imprisonment of at least four years under Federal, State, or local law that involves at least one jurisdiction outside the United States and that is intended to obtain, directly or indirectly, a financial or other material benefit; and

(B) includes wildlife trafficking (as defined by section 7601(12) of title 16) and severe forms of trafficking in persons (as defined in section 7102 of this title) involving at least 1 jurisdiction outside of the United States.

(6) Transnational organized crime group

The term "transnational organized crime group" means a group of persons that includes one or more citizens of a foreign country, exists for a period of time, and acts in concert with the aim of engaging in transnational organized crime.

(7) United States narcotics laws

The term "United States narcotics laws" means the laws of the United States for the prevention and control of illicit trafficking in controlled substances (as such term is defined in section 802(6) of title 21).

(8) United States personThe term "United States person" means—

(A) a citizen or national of the United States; and

(B) an alien lawfully present in the United States.


(Aug. 1, 1956, ch. 841, title I, § 36, as added Pub. L. 98-533, title I, § 102, Oct. 19, 1984, 98 Stat. 2708; amended Pub. L. 99-399, title V, § 502, Aug. 27, 1986, 100 Stat. 869; Pub. L. 100-690, title IV, § 4602, Nov. 18, 1988, 102 Stat. 4287; Pub. L. 101-231, § 13(a), Dec. 13, 1989, 103 Stat. 1963; Pub. L. 101-246, title X, § 1001, Feb. 16, 1990, 104 Stat. 86; Pub. L. 103-236, title I, § 133(a)(1), title VIII, § 827, Apr. 30, 1994, 108 Stat. 395, 519; Pub. L. 104-134, title I, § 101[(a)] [title IV, § 406], Apr. 26, 1996, 110 Stat. 1321, 1321-45; renumbered title I, Pub. L. 104-140, § 1(a), May 2, 1996, 110 Stat. 1327; Pub. L. 105-277, div. G, subdiv. B, title XXII, § 2202, Oct. 21, 1998, 112 Stat. 2681-805; Pub. L. 105-323, title I, § 101, Oct. 30, 1998, 112 Stat. 3029; Pub. L. 107-56, title V, § 502, Oct. 26, 2001, 115 Stat. 364; Pub. L. 108-447, div. B, title IV, § 405(a)-(d), Dec. 8, 2004, 118 Stat. 2902, 2903; Pub. L. 110-181, div. A, title XII,

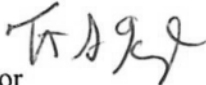
§ 1255(a), Jan. 28, 2008, 122 Stat. 402; Pub. L. 112–283, §§ 3, 4, Jan. 15, 2013, 126 Stat. 2493, 2494; Pub. L. 114–323, title VII, § 704(a)(1), (2), Dec. 16, 2016, 130 Stat. 1941; Pub. L. 115–44, title III, § 323, Aug. 2, 2017, 131 Stat. 954; Pub. L. 115–141, div. R, § 3, Mar. 23, 2018, 132 Stat. 1123; Pub. L. 115–232, div. A, title XII, § 1232(d), Aug. 13, 2018, 132 Stat. 2038; Pub. L. 116–94, div. J, title VI, § 603, Dec. 20, 2019, 133 Stat. 3069.)




U.S. Immigration
and Customs
Enforcement

MEMORANDUM FOR: Derek N. Benner
HSI Deputy Executive Associate Director (EAD) and Senior
Management Official performing the Duties of the EAD

THROUGH: Alysa Erichs 
Acting Deputy Executive Associate Director

FROM: Tatum King 
Assistant Director
Domestic Operations

Clark E. Settles 
Assistant Director
National Security Investigations Division

SUBJECT: HSI Domestic Field Office Reporting to NSID on a Designated
National Security Event / U.S. based Terrorist Attack

Purpose:

It is recommended HSI Deputy Executive Associate Director (EAD) and Senior Management Official performing the Duties of the EAD approve this memorandum to direct HSI domestic field offices to report Joint Terrorism Task Force (JTTF) investigative activity directly to the National Security Investigations Division (NSID) following a declaration of a National Security Event (NSE) / U.S. based terrorist attack that is deemed to be International Terrorism (IT). Such reporting will continue through the duration of the investigative response, until directed to return to normal reporting protocol by NSID. This protocol does not change any other reporting requirements outside of a designated NSE.

Background:

The U.S. has faced an increased threat posture as a result of numerous U.S. based terrorist attacks. During the response, HSI domestic field offices have internal reporting requirements, while continuing operations and investigations. As the Federal Bureau of Investigation (FBI)-led JTTFs are tasked with primary investigative responsibility for terrorism events, and most IT information is classified or originator controlled, HSI agents are faced with difficulty in reporting

classified information and filtering the operational “need to know”. Following many after action reviews, there is clearly a need for a more efficient mechanism for reporting. NSID is uniquely situated to provide reporting in real-time, based upon its placement and access within the International Terrorism Operations Section (ITOS) of the FBI HQ’s Counter-terrorism Division (CTD). ITOS is the command and control center for all U.S. based terrorism events, and NSID has embedded the Counterterrorism Section (CTS) of the National Security Unit into ITOS for the purpose of streamlined coordination of all JTTF IT investigations, threat streams and Counterterrorism (CT) responses following U.S. based terrorist attacks. CTS program managers and analysts are embedded within CTD teams which provide coverage of domestic regions. CTS supports HSI special agents (and their management) who are assigned to the JTTFs nationwide. This placement affords HSI NSID full visibility into JTTF operations. CTS personnel are the subject matter experts on CT operations, and provide the NSID Assistant Director a comprehensive picture of investigations and disruptions. CTS provides ICE and HSI strategic, National Security Law Section (NSLS) legal review, tactical capabilities, administrative immigration authority, and disruption options for ultimate decision making by JTTF/ITOS leadership.

Discussion

(b)(5)

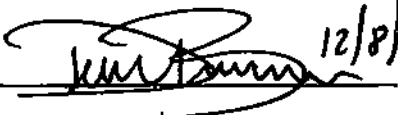
(b)(5)

(b)(7)(E)

Recommendation:

HSI domestic field office reporting on JTTF investigative activity and support following a designated NSE must flow directly and exclusively to NSID through CTS. NSID will subsequently report all such activity through the chain of command to HSI leadership. All events begin as a domestic investigation before being classified as an NSE. Since the initial conduit for all reporting from the field is Domestic Operations, NSID will immediately advise Domestic Ops when NSID is assuming reporting responsibilities. NSID will also advise Domestic Operations of ICE JTTF field activity resulting from such an event.

Respectfully request approval of this recommendation to ensure HSI, ICE, and ultimately DHS leadership is provided accurate, consistent, and timely reporting during responses to U.S. based terrorist attacks/NSE.

Approve  12/8/17 Disapprove _____
Modify _____ Needs more discussion _____

JUN 27 2019



U.S. Immigration
and Customs
Enforcement

MEMORANDUM FOR: Derek N. Benner
Executive Associate Director

THROUGH Alysa D. Erichs *Alys D Erichs*
Deputy Executive Associate Director

FROM: Louis A. Rodi, III *Louis A Rodi, III*
Acting Assistant Director

SUBJECT: Minimum Commitment and Requirements for Special Agent
Assignments to the Joint Terrorism Task Forces

Purpose:

To establish a Homeland Security Investigations (HSI) Directive requiring a minimum three-year (36 month) initial commitment for all HSI special agents (SAs) currently assigned to the Joint Terrorism Task Force (JTTF) and those who are selected to be assigned to the JTTF after the date of this Directive. In addition, the Directive would establish that all HSI JTTF SAs must be a GS-1811-13 at the time of assignment to the JTTF.

Background:

The Federal Bureau of Investigations (FBI) recognizes HSI as one of its most significant strategic partners in the execution of the counterterrorism mission. (b)(7)(E)

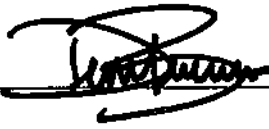
(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Recommendation:

It is recommended that the HSI Executive Associate Director implement a three-year minimum commitment for HSI SAs assigned to the JTTF and must be a GS-1811-13 to join and continue to build the partnership.

Approve  6/27/19 Disapprove _____
Modify _____ Needs more discussion _____