



*Homeland Security Investigations*

# Counterterrorism Investigations Handbook

HSI HB 23-01 / January 13, 2023



U.S. Immigration  
and Customs  
Enforcement

FOR OFFICIAL USE ONLY (U) (LAW ENFORCEMENT SENSITIVE)

REL0000025378

## Foreword

The Homeland Security Investigations (HSI) Counterterrorism Investigations Handbook provides a central source of policies, procedures, responsibilities, guidelines, and controls to be followed by U.S. Immigration and Customs Enforcement (ICE) HSI special agents and their supervisors when conducting or overseeing national security-related counterterrorism investigations. This handbook contains guidance to ensure uniformity and operational consistency across all HSI headquarters and field offices. Oversight of the Counterterrorism Investigations Program resides with the Unit Chief of the National Security Unit.

The Counterterrorism Investigations Handbook supersedes the National Security Investigations Handbook (HSI HB 13-03), dated April 26, 2013, and other documents listed in Appendix C.

The Counterterrorism 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 by 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. The information contained in this handbook 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 Information 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 Information 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 National Security Unit.



---

Steve K. Francis  
Acting Executive Associate Director  
Homeland Security Investigations

1/13/2023

---

Date

# COUNTERTERRORISM INVESTIGATIONS HANDBOOK

## Table of Contents

<b>Chapter 1. PURPOSE AND SCOPE</b> .....	<b>1</b>
<b>Chapter 2. INTRODUCTION</b> .....	<b>1</b>
<b>Chapter 3. DEFINITIONS</b> .....	<b>3</b>
• 3.1 8 U.S.C. § 1367 (VAWA, T Visa, U Visa, Continued Presence).....	3
• 3.2 Alien File .....	3
• 3.3 Asylum.....	3
• 3.4 Convention Against Torture .....	4
• 3.5 (b) (7)(E) .....	4
• 3.6 Denaturalization .....	4
• 3.7 Deportation or Removal.....	4
• 3.8 FBI Counterterrorism Division .....	5
• 3.9 FBI International Terrorism Operations Section (I & II).....	5
• 3.10 Foreign Terrorist Organizations.....	5
• 3.11 Joint Vetting Unit (historical reference only) .....	5
• 3.12 Known or Suspected Terrorist .....	6
• 3.13 Lawful Permanent Resident.....	6
• 3.14 Letterhead Memorandum.....	6
• 3.15 National Security Event .....	6
• 3.16 National Security Interest .....	7
• 3.17 Naturalization.....	7
• 3.18 Overstay .....	7
• 3.19 Parole .....	7
• 3.20 Passport .....	7
• 3.21 Persecution.....	8
• 3.22 Refugee Definition and Admission as a Refugee .....	8
• 3.23 Removal Proceedings.....	8
• 3.24 Significant Event Notification .....	8
• 3.25 Temporary Protected Status.....	9
• 3.26 Terrorism.....	9
• 3.27 (b) (7)(E) .....	9
• 3.28 (b) (7)(E) .....	9
• 3.29 (b) (7)(E) .....	9
• 3.30 Torture.....	10
• 3.31 Triggering Event .....	10

- 3.32 Visa .....10
- 3.33 Visa Revocation .....10

**Chapter 4. AUTHORITIES/REFERENCES .....11**

- 4.1 Statutory and Regulatory Authorities Related to Counterterrorism Investigations .....11
- 4.2 Criminal Charges Used in Counterterrorism Investigations.....12
- 4.3 General and DHS-Specific Ancillary Criminal Charges Used in Counterterrorism Investigations.....13
- 4.4 National Security-Related Administrative Charges.....14
- 4.5 Customs Officer and Immigration Officer Authorities.....15
- 4.6 Statutory Authority to Revoke Naturalization .....15
- 4.7 Civil Denaturalization Statute.....15
- 4.8 Criminal Denaturalization Statute.....16
- 4.9 References.....16

**Chapter 5. RESPONSIBILITIES .....19**

- 5.1 Executive Associate Director, Homeland Security Investigations .....19
- 5.2 Assistant Director, National Security Division.....19
- 5.3 Unit Chief, National Security Unit .....20
- 5.4 Section Chiefs, Counterterrorism Sections .....20
- 5.5 Special Agents in Charge.....20
- 5.6 Resident Agents in Charge and Group Supervisors.....20
- 5.7 Special Agents.....20

**Chapter 6. COUNTERTERRORISM INVESTIGATIVE PRIORITIES AND PROGRAMS .....20**

- 6.1 National Security Division.....20
- 6.2 National Security Programs .....21
- 6.3 Office of the Principal Legal Advisor.....22

**Chapter 7. HSI FIELD OFFICE JOINT TERRORISM TASK FORCE PARTICIPATION AND ROLES.....23**

- 7.1 HSI’s JTTF Commitment and Functions .....23
- 7.2 HSI JTTF Special Agents’ Role .....23
- 7.3 HSI Supervisors of HSI JTTF Special Agents.....26

**Chapter 8. HSI HEADQUARTERS OPERATIONAL AND PROGRAMMATIC SUPPORT TO COUNTERTERRORISM EFFORTS.....27**

- 8.1 HSI CTS Mission Statement and Field Support .....27
- 8.2 Counterterrorism Operations Section Goals .....29
- 8.3 Counterterrorism Investigative Priorities.....29
- 8.4 (b) (7)(E) .....30

**Chapter 9. CONDUCTING COUNTERTERRORISM INVESTIGATIONS.....31**

- 9.1 Field Coordination with HSI CTS Related to Investigations.....31
- 9.2 Investigative Case Management .....31
- 9.3 Predicating Information and Intelligence.....36
- 9.4 JTTF Investigations Predicated on HSI Information .....37
- 9.5 JTTF Investigations Predicted on FBI Information or Investigations in Which ICE Violations Are Predicate Offenses .....37
- 9.6 Initiating a Counterterrorism Investigation.....37
- 9.7 Information Security Considerations .....39
- 9.8 Collaboration with Federal, State, and Local Law Enforcement and Other Government Agencies .....39
- 9.9 Identifying Potential Immigration Violations.....39
- 9.10 Managing Foreign Government-Related Information .....39
- 9.11 Use of Other Agency Informants in Furtherance of Counterterrorism Investigations .....40
- 9.12 Engaging the U.S. Attorney’s Office and the Local OPLA Field Location in Counterterrorism Investigations .....40
- 9.13 Considerations When Interviewing and Taking Statements on Information in Counterterrorism Investigations .....40
- 9.14 Considerations on Counterterrorism Investigations Regarding Individuals Who Are Nonimmigrants .....40
- 9.15 Other Investigative Activities in Furtherance of a Counterterrorism Investigation.....41
- 9.16 (b) (7)(E) .....41
- 9.17 Immigration or Document Fraud Schemes and Counterterrorism Investigations .....42
- 9.18 Headquarters-Led Counterterrorism and National Disruptive Efforts.....42
- 9.19 Classified Information in Counterterrorism Investigations .....43
- 9.20 Tools to Consider in Counterterrorism Investigations.....44
- 9.20.1 Use of Databases in Counterterrorism Investigations.....44
- 9.21 CTS Investigative Partnership Functions.....47
- 9.22 Visa Security Program .....50
- 9.23 CBP Tactical Terrorism Response Teams .....51
- 9.24 Oversight of ICE Personnel Serving on Federal Investigative Task Forces .....51

**Chapter 10. DEPARTMENT OF STATE COUNTERTERRORISM OFFICE .....52**

- 10.1 Identification and Designation of Foreign Terrorist Organizations.....52
- 10.2 Department of State Procedures for Designating a Group as a Foreign Terrorist Organization.....52
- 10.3 Legal Criteria for Designation as a Foreign Terrorist Organization Under Section 219 of the Immigration and Nationality Act, as Amended.....53
- 10.4 Legal Ramifications of Designation as a Foreign Terrorist Organization.....53
- 10.5 Other Effects of Designation as a Foreign Terrorist Organization .....54
- 10.6 (b) (7)(E) .....54
- 10.7 (b) (7)(E) .....55
- 10.8 (b) (7)(E) .....55
- 10.9 (b) (7)(E) .....55

**Chapter 11. IMMIGRATION AND NATIONALITY ACT .....56**

- 11.1 Evidence to Be Considered for Security-Related Administrative Removal Grounds .....56
- 11.2 (b) (7)(E) .....59
- 11.3 Evidence to Be Considered for Administrative Removal Proceedings .....60

**Chapter 12. FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) AND THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC).....61**

- 12.1 Relevant Definitions .....61
- 12.2 U.S. Foreign Intelligence Surveillance Court .....62
- 12.3 Foreign Intelligence Surveillance Act Applications .....62
- 12.4 Minimization Procedures .....62
- 12.5 Uses of Foreign Intelligence Information .....63
- 12.6 FISA Authority vs. Court-Overseen Criminal Investigatory Surveillance Techniques .....63
- 12.7 FISA, Counterintelligence, and Law Enforcement .....64
- 12.8 Considerations of FISA Implications for U.S. Persons and Non-U.S. Persons .....64
- 12.9 FISA Usage in Domestic Terrorist or Racketeering Enterprise Investigations .....64
- 12.10 Emergency FISA Applications .....64
- 12.11 FISA Application in “Lone Wolf” Situations .....65

<b>Chapter 13. BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC DEVICES .....</b>	<b>65</b>
• 13.1 Background .....	65
• 13.2 Authorities and Policies .....	66
• 13.3 Border Searches by HSI Special Agents.....	66
• 13.4 Chain of Custody .....	67
• 13.5 Demands for Assistance.....	67
• 13.6 Information Sharing.....	68
<b>Chapter 14. HSI RESPONSE PROTOCOL FOLLOWING DESIGNATED NATIONAL SECURITY EVENT .....</b>	<b>68</b>
• 14.1 HSI JTTF and CTS Post Attack Management.....	68
<b>Chapter 15. GUIDANCE FOR COMMON FIELD ISSUES .....</b>	<b>70</b>
• 15.1 JTTF Reduction in Staffing Requests.....	70
• 15.2 MOUs and MOAs Pertaining to HSI Participation in the JTTF .....	71
• 15.3 Deputation of HSI Special Agents Assigned to the JTTF .....	72
• 15.4 Polygraph Examination of HSI Special Agents Assigned to the JTTF .....	72
• 15.5 National Security Letters .....	73
• 15.6 FBI National Security Requests for Alien File Review.....	73
• 15.7 Disclosure of Asylum or Refugee Related Information .....	74
• 15.8 Disclosure of 8 U.S.C. § 1367 Information .....	74

**APPENDICES**

Appendix A	Counterterrorism Investigations Development Worksheet.....	A-i
Appendix B	Joint Terrorism Task Force Membership Designation Criteria .....	B-i
Appendix C	Superseded Documents.....	C-i
Appendix D	Acronyms.....	D-i

# COUNTERTERRORISM INVESTIGATIONS HANDBOOK

## Chapter 1. PURPOSE AND SCOPE

The Counterterrorism Investigations Handbook establishes policy and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs) and their supervisors when conducting or overseeing national security-related counterterrorism (CT) investigations. This Handbook also provides guidance governing investigations conducted by HSI SAs using ICE authorities and jurisdiction in support of the Federal Bureau of Investigation (FBI)-led Joint Terrorism Task Forces (JTTFs); this helps SAs and their supervisors better understand HSI's integral role in national security CT investigations, beginning in the wake of the terrorist attacks of September 11, 2001, through HSI's current operational and intelligence capabilities both within the Department of Homeland Security (DHS) and as part of the JTTFs.

## Chapter 2. INTRODUCTION

Prior to the events of September 11, 2001, neither immigration nor customs authorities were widely recognized as effective and powerful CT tools in the United States. With the creation of DHS in 2003, ICE became an integral part of the U.S. Government's approach to CT investigations and operations, and HSI's immigration and customs investigative expertise and role became valued assets in pursuit of terrorists and transnational criminal organizations.

HSI SAs are uniquely trained and resourced to initiate and support complex, multidisciplinary investigations by leveraging HSI's unique immigration and customs authorities. In addition to conducting investigations, gathering law enforcement intelligence, and conducting enforcement operations within HSI's jurisdiction, HSI's role and placement within DHS uniquely positions HSI SAs to understand the functions and workings of, and liaise with, other DHS agencies such as the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS), and within ICE, Enforcement and Removal Operations (ERO). In other instances, HSI provides guidance within its jurisdiction and adds value to important CT mechanisms, such as TSA's "No-Fly List." HSI's capabilities are equally significant in proactive and reactive CT investigations.

Given HSI's responsibility and jurisdiction to investigate, disrupt, and dismantle transnational criminal organizations and terrorist networks that threaten or seek to exploit the customs and immigration laws of the United States, HSI partners with the FBI's Counterterrorism Division (CTD) and assigns SAs to JTTFs nationwide to ensure that HSI's authorities are leveraged to most effectively execute the shared national security mission of the FBI and ICE, and to safeguard the security of the United States. HSI SAs substantially contribute to JTTFs by enforcing the authorities entrusted to ICE, which span a broad set of investigative areas including, among others, immigration, money laundering, smuggling, trafficking, trade



violations, and cyber security. HSI's support of and commitment to the JTTF structure is evidenced by the fact that HSI is the largest federal contributor of personnel (outside of the FBI) to the JTTFs in the field and to the FBI CTD's International Terrorism Operations Section (ITOS) at Headquarters (HQ).

The FBI is the designated coordinating agency, through the JTTFs, for all federal CT investigations. *See* Title 28, United States Code (U.S.C.), Section 533; Title 28, Code of Federal Regulations (C.F.R.), Section 0.85; Presidential Decision Directive (PDD) 39, U.S. Policy on Counterterrorism, issued on June 21, 1995; PDD 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, issued May 22, 1998. This neither diminishes HSI's equities in the national security arena nor precludes investigations predicated on ICE's authorities and jurisdiction; instead, it provides for a uniform approach within which HSI SAs assigned to JTTFs may conduct CT investigations in compliance with applicable statutes, policies, and guidelines.

The JTTFs were established by the FBI to utilize the collective authorities and 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 first JTTF was established in 1980 in the FBI New York field office. As of the date of issuance of this Handbook, there are 184 JTTFs throughout the United States.

The FBI maintains operational oversight of the JTTFs; however, the groups, organizations, and individuals to be investigated are specifically identified and agreed upon by the JTTF participating agencies, in accordance with Attorney General (AG) Guidelines. HSI SAs assigned to the JTTFs may be tasked to open, lead, or assist in investigations based on information generated from the FBI, another agency/component, or information predicated by HSI. It is critical that SAs lead JTTF investigations where ICE's authorities and jurisdiction are viewed as the most likely legal avenue to disrupting a terrorist attack or dismantling a terrorist organization. HSI SAs should strive to be designated as case managers, co-case managers, or case participants in the FBI's case investigative systems (Sentinel and/or Guardian) on investigations in which they are substantially engaged. This is most appropriate and in line with HSI's mission where ICE authorities can potentially be utilized against targets to disrupt or dismantle a terrorist organization or national security threat.

SAs and their supervisors should always remain cognizant of the diverse information, methods, and goals inherent in CT investigations, which at times differ from those used for criminal investigations. HSI SAs must remain cognizant that working with the FBI on a CT investigation or matter does not augment HSI's authorities. CT investigations are often predicated on classified information, employ Intelligence Community (IC) collection techniques, and may contain foreign government information. These methods may at times include criminal investigations and at other times may not result in a criminal arrest, but CT investigations are pursued to deter, disrupt, and prevent terrorists from achieving their goals both within the United States and around the world.

## Chapter 3. DEFINITIONS

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

### 3.1 8 U.S.C. § 1367 (VAWA, T Visa, U Visa, Continued Presence)

ICE personnel are generally prohibited from using or disclosing information protected by 8 U.S.C. § 1367 to anyone other than an employee of DHS, the Department of State (DOS), or the Department of Justice (DOJ), to include any information related to any noncitizen who has, or who ICE personnel has reason to believe may have, a pending or approved application for (1) Victims of battery or extreme cruelty perpetrated by certain qualifying relatives (applicants for Violence Against Women Act (VAWA) benefits); (2) Victims of certain qualifying crimes who help law enforcement (applicants for U nonimmigrant status); and (3) Victims of certain forms of trafficking (applicants for T nonimmigrant status and Continued Presence). Information about derivative relatives of the individuals referenced in the above categories is protected as well.

### 3.2 Alien File

An Alien File (A-File) is an official file owned by USCIS that documents all immigration and naturalization records created or consolidated for a noncitizen. (Note: The term “noncitizen” as used in this document is intended to refer to any individual defined in section 101(a)(3) of the Immigration and Nationality Act (INA) [8 U.S.C. § 1101(a)(3)]<sup>1</sup> and does not include noncitizen nationals of the United States.) An A-File may include a noncitizen’s history of interactions with USCIS, CBP, and ICE, as prescribed by the INA and regulations regarding immigration benefits. Information in an A-File is used as a reference for DHS to approve or deny immigration-related benefits, or to support enforcement actions initiated against those who violate U.S. immigration laws. A-Files may be classified or unclassified and must be handled accordingly. Each A-File folder is labeled with a unique Alien Number (A number), also referred to as Alien Registration Number (ARN), that is assigned to individuals who are not U.S. citizens and should match the barcode label on the folder.

### 3.3 Asylum

Asylum is a discretionary form of relief available to any noncitizen who is physically present in the United States or who arrives in the United States, irrespective of such noncitizen’s status, if the noncitizen meets the definition of a refugee under INA § 101(a)(42) and is not otherwise ineligible for such relief. *See* INA § 208(a) and (b). The core requirements are that noncitizens

---

<sup>1</sup> This Handbook will generally cite to sections of the INA when discussing matters involving immigration court and administrative litigation in removal proceedings, including an initial cite to the U.S.C. where needed for clarity. Various sections of the INA are also codified at Title 8 of the U.S.C. Criminal statutes related to immigration enforcement, such as 8 U.S.C. §§ 1324-1326, are typically referred to with their U.S.C. citations. References to those statutes will include citations to the U.S.C. throughout this Handbook, consistent with common usage. For a comprehensive table which cross references parallel citations between the INA and U.S.C., *see* USCIS, Immigration and Nationality Act, available at <https://www.uscis.gov/laws-and-policy/legislation/immigration-and-nationality-act>.

must establish either that they were persecuted in the past or have a well-founded fear of future persecution based on one of five specified grounds (race, religion, nationality, membership in a particular social group, or political opinion.). Once noncitizens have been granted asylum, they may not be removed, absent termination of asylum. *See* 8 C.F.R. §§ 208.22 and 1208.22. Once noncitizens have been granted asylum, they become eligible to apply for employment authorization and to travel abroad if they obtain a proper travel document. *See* INA § 208(c)(1)(B) and (C).

### **3.4 Convention Against Torture**

The United States is a signatory to the United Nations (U.N.) Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT) signed in New York on December 10, 1984. Because CAT is not self-executing, the United States promulgated regulations for the implementation of the immigration-related aspects of our treaty obligations. These regulations set forth standards for a noncitizen to establish in immigration court that it is “more likely than not” that the individual would be subjected to torture. *See* 8 C.F.R. §§ 208.16(c) - .18, 1208.16(c) - .18; Foreign Affairs Reform and Restructuring Act of 1998, Pub. L. No. 105-277, div. G, § 2242, 112 Stat. 2681, 2681-822. A grant of CAT protection, which comes in two forms, CAT withholding of removal and CAT deferral of removal, only precludes removal to the country where it is more likely than not that the noncitizen would be tortured, but not removal from the United States per se.

### **3.5 Counterterrorism Operations**

FBI Counterterrorism Operations consist of Assessments (formerly known as Guardians), Preliminary Investigations (PIs), Full Investigations (FIs), Threat Streams, Source Opportunities, Continental United States (CONUS)-based attacks, and other HQ initiatives.

### **3.6 Denaturalization**

Denaturalization is a judicial order revoking and setting aside the order granting citizenship to a person and cancelling the Certificate of Naturalization. Denaturalization can be pursued criminally, with the U.S. Attorney’s Office (USAO) filing criminal charges against the subject, or civilly, with the USAO filing an action for revocation of naturalization. *See* 18 U.S.C. § 1425; INA § 340(a), (e). (*Note: See* the Denaturalization Investigations Handbook (Office of Investigations (OI) Handbook (HB) 08-01), dated January 15, 2008, or as updated.)

### **3.7 Deportation or Removal**

Noncitizens ordered deported or removed and who have left the United States shall be considered to have been deported or removed in pursuance of law, irrespective of the source from which the expenses of their transportation were defrayed or of the place to which they departed. Deportation or removal of noncitizens from the United States occurs after the noncitizens have been found removable based on the INA grounds of inadmissibility or deportability and are not eligible for any benefits or protection from removal. Deportation or

removal is often ordered by an Immigration Judge (IJ) without any criminal punishment being imposed or contemplated. Deportation or removal may also occur based on expedited removal proceedings before an immigration officer. (*See* Section 3.23.)

### **3.8 FBI Counterterrorism Division**

The FBI CTD is a component of the National Security Branch of the FBI. CTD investigates terrorism threats inside the United States, provides information on terrorists outside the country, and tracks known terrorists worldwide. ITOS is a section within the FBI CTD.

### **3.9 FBI International Terrorism Operations Section (I & II)**

The FBI's ITOS is a unique HQ element serving as a global command and control element for CT. ITOS is divided into two sections: ITOS I and ITOS II.

ITOS I supports, coordinates, and provides oversight of all FBI CONUS-based international terrorism investigations. ITOS I also provides guidance, approvals, financial and technical support, and coordination with other HQ entities for all JTTF field offices.

ITOS II supports the FBI's law enforcement mission abroad to prevent terrorist attacks against U.S. citizens and to protect the interests of the United States, and also supports intelligence efforts to eliminate the external threat of terrorism to the homeland, U.S. citizens, and U.S. interests.

### **3.10 Foreign Terrorist Organizations**

Foreign Terrorist Organizations (FTOs) are foreign organizations that are designated by the Secretary of State in accordance with INA § 219, as amended. FTO designations play a critical role in the U.S. Government'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 and abroad. It should also be noted that, under the INA, a "terrorist organization" is defined more broadly to include organizations designated by DOS in consultation with DOJ and the Department of the Treasury, as well as a group of two or more individuals who engage in terrorist activity. *See* INA § 212(a)(3)(B)(vi) ("Terrorist organization" defined).

### **3.11 Joint Vetting Unit (historical reference only)**

Created in 2005, the Joint Vetting Unit (JVU) was responsible for the deconfliction of HSI investigative leads with the FBI CTD's Terrorism Financing Operations Section (TFOS) or the FBI section within CTD which assumes TFOS's responsibilities. The JVU was previously staffed by HSI and FBI personnel. However, in 2019, the FBI restructured its resources assigned to TFOS to better maintain its ability to support terror finance operational efforts across all CT areas; as a result, TFOS as a Section within the FBI's CTD no longer exists.

(Note: The JVU has been disbanded and is no longer staffed by HSI and the FBI. SAs should contact the Counterterrorism Operations Sections I and II (collectively CTS) of the HSI National Security Unit (NSU) for all guidance related to terror finance investigations. Proper deconfliction methods for investigations should be addressed to the FBI at the local HSI Special Agent in Charge (SAC) office level.)

### **3.12 Known or Suspected Terrorist**

Pursuant to the FBI's definition, Known or Suspected Terrorists (KSTs) are individuals about whom, based on the totality of the circumstances, there is a reasonable suspicion that they are engaged, have been engaged, or intend to engage, in conduct constituting, in preparation for, in aid or furtherance of, or related to, terrorism. "Frequently Asked Questions," FBI Terrorist Screening Center (TSC) (Apr. 11, 2016), *available at* <https://ucr.fbi.gov/nsb/tsc/terrorist-screening-center-frequently-asked-questions-032416.pdf>. This definition includes the following:

- A. A Known Terrorist is an individual who has been (a) charged by criminal complaint, information, arrested, or indicted for or convicted of a crime related to terrorism or terrorist activities by U.S. Government or foreign government authorities; or (b) identified as a terrorist or member of a terrorist organization pursuant to a U.N. Security Council Resolution.
- B. A Suspected Terrorist is an individual who is reasonably suspected to be engaging in, has been engaged in, or intends to engage in conduct constituting, in preparation for, in aid of, or related to terrorism or terrorist activity.

### **3.13 Lawful Permanent Resident**

A Lawful Permanent Resident (LPR) is a noncitizen who has been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with the INA. *See* INA § 101(a)(20). LPR status terminates upon the entry of a final administrative order of exclusion, removal, or deportation. 8 C.F.R. § 1.2. An LPR may also be referred to as a "Permanent Resident Alien," "Resident Alien Permit Holder," and "Green Card Holder."

### **3.14 Letterhead Memorandum**

In the context of CT investigations, a Letterhead Memorandum (LHM) is a written summary, typically issued by the FBI, of derogatory information. The FBI may prepare an unclassified LHM and provide the authority to ICE to use the LHM as evidence during immigration proceedings. Alternatively, the FBI may also prepare a classified LHM, although such LHMs are less useful, as approval to file such classified documents in immigration proceedings is rare.

### **3.15 National Security Event**

Pursuant to ICE policy, a National Security Event (NSE) is defined as "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 with the other members of the law enforcement community.” See ICE Directive 14019.1, Reporting Protocol Following a Designated National Security Event or U.S.-based International Terrorist Attack, dated December 3, 2019, or as updated. The Assistant Director (AD) for HSI’s National Security Division (NSD) serves as the primary ICE official responsible for designating an event as an NSE and coordinating with the FBI’s CTD. *Id.*; see also *infra* Chapter 14.

### **3.16 National Security Interest**

National Security Interest is a determination that an individual is someone for whom sufficient information exists to warrant opening an investigation in accordance with applicable AG Guidelines. 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 AG, consistent with Executive Order 12333 or any successor order.

### **3.17 Naturalization**

Naturalization is the conferring of the nationality of a state upon a person after birth by any means whatsoever. See INA § 101(a)(23).

### **3.18 Overstay**

An overstay is an individual admitted to the United States as a nonimmigrant, with authorization to remain for a temporary period, who has not departed the United States upon the conclusion of the authorized period of stay. See INA § 237(a)(1)(B).

### **3.19 Parole**

Pursuant to INA § 212(d)(5), DHS has the discretionary authority to parole into the United States, temporarily and only on a case-by-case basis, an otherwise inadmissible noncitizen for urgent humanitarian reasons or significant public benefit. Parole does not constitute a formal admission to the United States and confers temporary permission only, requiring parolees to leave when the conditions supporting their parole cease to exist, when the parole expires, or when the parole is otherwise terminated. Further, parole does not waive any applicable grounds of inadmissibility. Although not defined by statute, types of parole include, but are not limited to, deferred inspection, silent parole, humanitarian parole, advance parole, conditional parole, and significant public benefit parole (which includes law enforcement paroles).

### **3.20 Passport**

A passport is an official document issued by the government of a country to one of its citizens. Passports authorize travel to foreign countries and authenticate the bearer’s identity, citizenship, right to protection while abroad, and right to reenter the bearer’s country of citizenship.

### **3.21 Persecution**

Persecution is the infliction of severe harm or suffering by a government or by persons whom or entities that a government is unable or unwilling to control. The United States may grant refugee admission to a noncitizen abroad or may grant asylum to a noncitizen physically present in or who arrives in the United States, based on either past persecution or a well-founded fear of future persecution. *See* INA §§ 101(a)(42), 207, and 208. In addition, statutory withholding of removal may be granted to a noncitizen in removal proceedings to preclude removal to a country where it is more likely than not that the noncitizen would be persecuted. *See* INA § 241(b)(3). The persecution must be based on the individual's actual or imputed race, religion, nationality, membership in a particular social group, or political opinion.

### **3.22 Refugee Definition and Admission as a Refugee**

A refugee is defined as any person who is outside his or her country of nationality who is unable or unwilling to return to that country because of persecution or a well-founded fear of future persecution on account of race, religion, nationality, membership in a particular social group, or political opinion. The term "refugee" does not include any person who ordered, incited, assisted, or otherwise participated in the persecution of any person on account of race, religion, nationality, membership in a particular social group, or political opinion. *See* INA § 101(a)(42). The definition of "refugee" forms the core requirement not only for asylum under INA § 208, but also for admission of refugees from overseas under INA § 207. In the latter regard, overseas noncitizens who believe they meet the definition of "refugee" and are included in a refugee group identified in INA § 207(a) may apply for admission to the United States. *See* INA § 207; 8 C.F.R. § 207.

### **3.23 Removal Proceedings**

Removal proceedings are administrative proceedings held to determine an individual's removability and/or eligibility for relief or protection from removal under U.S. immigration law. Removal proceedings are typically conducted in immigration court by DOJ's Executive Office for Immigration Review and presided over by an IJ.

### **3.24 Significant Event Notification**

The Significant Event Notification (SEN) system is an ICE transactional Intranet application and reporting system designed to facilitate the seamless entry, query, and modification of Significant Incident Reports (SIRs) and Significant Prospective Enforcement Action Reports (SPEARs) that contain indicators and warnings. These reports may contain information of such significance that they warrant immediate notification to the National Operations Center.

### 3.25 Temporary Protected Status

Pursuant to INA § 244, the Secretary of Homeland Security may designate a foreign country for temporary protected status (TPS) due to conditions in the country that temporarily prevent the country's nationals from returning safely or, in certain circumstances, where the country is unable to handle the return of its nationals adequately. TPS may be granted to eligible nationals of certain countries (or parts of countries) who are already in the United States. Eligible individuals without nationality who last resided in the designated country may also be granted TPS.

### 3.26 Terrorism

Terrorism is defined as activities that would constitute terrorism, international terrorism, or terrorist activities as defined by law, including, but not limited to, the following provisions: 6 U.S.C. § 101; 18 U.S.C. §§ 2331 and 2332b(g)(5); INA § 212(a)(3)(B) [8 U.S.C. § 1182(a)(3)(B)]. For example, terrorism, as defined in 6 U.S.C. § 101(16), means an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources; is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and appears to be intended (i) to intimidate or coerce a civilian population, (ii) to influence the policy of a government by intimidation or coercion, or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.

### 3.27 Terrorism Financing Operations Section

Until 2019, the FBI's TFOS led law enforcement and domestic IC efforts to defeat terrorism through the application of financial investigative techniques, the exploitation of financial intelligence, and the disruption of terrorist financing operations. (Note: As stated in Section 3.11 above, in 2019 the FBI restructured its resources assigned to TFOS to better maintain its ability to support terror finance operational efforts across all CT areas; as a result, TFOS as a Section within the FBI's CTD no longer exists.)

### 3.28 (b) (7)(E)

(b) (7)(E)

### 3.29 (b) (7)(E)

(b) (7)(E)



(b) (7)(E)

### **3.30 Torture**

In terms of its criminal law definition, torture is an act committed by a person acting under the color of law specifically intended to inflict severe physical or mental pain or suffering (other than pain or suffering incidental to lawful sanctions) upon another person within his or her custody or physical control. *See* 18 U.S.C. § 2340(a). For immigration law purposes, in terms of qualifying for withholding or deferral of removal under the CAT regulations, the definition of torture is more detailed. *See* 8 C.F.R. §§ 208.18(a), 1208.18(a).

### **3.31 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.

### **3.32 Visa**

A visa is an endorsement made by an authorized representative of one country upon a passport issued by another, permitting the passport holder entry into or transit through the country making the endorsement.

## **3.3 Visa Revocation**

Pursuant to INA § 221(i), DOS has the authority to revoke a visa that it previously granted to a noncitizen. For noncitizens admitted to the United States, the overwhelming majority of DOS visa revocations are effective upon departure, meaning the revocation is not effective until the noncitizen's departure from the United States. DOS can revoke a visa effective upon departure when, after issuance of a visa, information surfaces that questions either the noncitizen's eligibility at the time of visa issuance or the noncitizen's continued eligibility for the visa. This may be based on an ineligibility ground under INA § 212(a) or a lack of entitlement to the visa classification. Visa revocations that are effective upon a noncitizen's departure generally do not constitute permanent findings of visa ineligibility. If a noncitizen is admitted to the United States while the noncitizen is within a period of authorized stay and the noncitizen's visa is revoked effective upon departure by DOS, DHS may not use the visa revocation as a basis to place the noncitizen in removal proceedings or for purposes of issuance of a Notice to Appear (NTA) (DHS Form I-862) if no other viable removal charges exist.

The majority of visa revocations by DOS take place when the noncitizen is outside the United States, in which case such revocation takes effect immediately.

In very few cases, after a noncitizen's admission into the United States, DOS may issue a revocation "effective immediately" and render the noncitizen subject to removal under INA §

237(a)(1)(B). If this is the only charge of removability, however, the IJ has the authority, pursuant to INA § 221(i), to review the underlying visa revocation. This is one of the only exceptions to the doctrine of consular non-reviewability, so DOS considers such revocations only in extraordinary circumstances at the request of DHS or another federal agency. Therefore, prior to issuance of an NTA solely on this ground, these cases must be coordinated through the Office of the Principal Legal Advisor (OPLA) and DOS to find another viable basis of removability.

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

### **4.1 Statutory and Regulatory Authorities Related to Counterterrorism Investigations**

- A. INA § 101(a)(15) [8 U.S.C. § 1101], Definitions of classes of noncitizens;
- B. INA § 212 [8 U.S.C. § 1182], General classes of noncitizens ineligible to receive visas and ineligible for admission, as well as waivers of inadmissibility;
- C. Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, 108 Pub. L. No. 458, §§ 1021-1023, 118 Stat. 3638, 3825-832, National Counterterrorism Center (NCTC), National Counter Proliferation Center, and National Intelligence Centers;
- D. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 107 Pub. L. No. 56 §§ 411-418, 418, 115 Stat. 272 (enhanced certain immigration provisions);
- E. INA § 235 [8 U.S.C. § 1225], Inspection by immigration officers; expedited removal of inadmissible arriving aliens<sup>2</sup>;
- F. INA § 274 [8 U.S.C. § 1324], Bringing in and harboring certain aliens;
- G. INA § 287 [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;

---

<sup>2</sup> The term “alien” is defined in INA § 101(a)(3) [8 U.S.C. § 1101(a)(3)] as any person not a citizen or national of the United States. For purposes of this Handbook, the term “noncitizen” will use the same definition as the term “alien” in INA § 101(a)(3) [8 U.S.C. § 1101(a)(3)].

- 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 and forfeiture of monetary instruments;
- U. 8 C.F.R. § 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;
- X. 31 C.F.R. § 594.201, U.S. Department of the Treasury's 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; and
- Y. 28 C.F.R. § 0.85, General functions of the FBI Director.

#### **4.2 Criminal Charges Used in Counterterrorism Investigations**

- A. Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Division C of Pub. L. 104-208, 110 Stat. 3009-546, enacted September 30, 1996 (multiple statutes);
- B. 18 U.S.C. § 2332a, Use of weapons of mass destruction;
- C. 18 U.S.C. § 2332b, Acts of terrorism transcending national boundaries;
- D. 18 U.S.C. § 2332d, Financial transactions;
- E. 18 U.S.C. § 2332f, Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities;
- F. 18 U.S.C. § 2332g, Missile systems designed to destroy aircraft;

- G. 18 U.S.C. § 2332h, Radiological dispersal devices;
- H. 18 U.S.C. § 2339, Harboring or concealing terrorists;
- I. 18 U.S.C. § 2339a, Providing material support to terrorists, organizations involved in torture or the recruitment of child soldiers;
- J. 18 U.S.C. § 2339b, Providing material support to a designated foreign terrorist organization; and
- K. 18 U.S.C. § 2339d, Receiving military-type training from a foreign terrorist organization.

#### **4.3 General and DHS-Specific Ancillary Criminal Charges Used in Counterterrorism Investigations**

- A. INA § 264(e) [8 U.S.C. § 1304(e)], Failure to carry proof of permanent residence;
- B. INA § 275 [8 U.S.C. § 1325], Improper entry by alien;
- C. INA § 275(c) [8 U.S.C. § 1325(c)], Marriage fraud;
- D. INA § 276 [8 U.S.C. § 1326], Re-entry of removed noncitizens;
- 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, 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;
- EE. 50 U.S.C. § 4819, Export controls, violation; and
- FF. 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) [8 U.S.C. § 1182(a)(3)], Security and related inadmissibility grounds; and

B. INA § 237(a)(4) [8 U.S.C. § 1227(a)(4)], Security and related deportation grounds.

#### **4.5 Customs Officer and Immigration Officer Authorities**

ICE designates HSI SAs who have completed the necessary training as customs officers under 19 U.S.C. § 1401(i) and immigration officers under 8 C.F.R. § 1.2. The law enforcement authorities for these positions are set forth at 19 U.S.C. § 1589a and 19 C.F.R. Parts 161-162, and 8 U.S.C. § 1357 and 8 C.F.R. § 287.5, respectively. These authorities were transferred from the former U.S. Customs Service and the former Immigration and Naturalization Service to the Secretary of Homeland Security through the Homeland Security Act of 2002, in conjunction with the Department of Homeland Security Reorganization Plan of November 25, 2002, the Reorganization Plan Modification for the Department of Homeland Security of January 30, 2003, and DHS delegation orders.

Some enforcement authorities granted to customs officers and immigration officers are similar to those granted to other federal criminal investigators, including, but not limited to, carrying firearms, executing and serving warrants and subpoenas, and making certain arrests without warrant. *See* 19 U.S.C. § 1589a; INA § 287. Other authorities were granted to ensure that HSI (and HSI's predecessors) had the necessary tools to execute its unique and expansive mission to enforce and investigate the laws under its jurisdiction. As customs officers under 19 U.S.C. § 1401(i), HSI SAs enforce the customs laws of the United States by searching for merchandise at the border, functional equivalent of the border, and extended border, among other reasons to protect the revenue of the United States, to ensure that proper duties are paid, and to prevent prohibited merchandise from being imported into or exported from the United States. By statute and case precedent, HSI SAs are granted broad authorities to investigate violations of federal law at and away from the border. This includes authority for enforcement of provisions under numerous titles of the United States Code, including Titles 18, 19, 21, 22, 31, and 50. Additionally, HSI has primary jurisdiction to investigate violations of law involving the movement of merchandise (including currency and other monetary instruments) into and out of the United States. *See* 19 U.S.C. § 1401(i).

#### **4.6 Statutory Authority to Revoke Naturalization**

The laws in effect as of the date of issuance of this Handbook provide procedures for the revocation of U.S. citizenship of a naturalized immigrant by judicial order through civil proceedings or a criminal conviction for naturalization fraud. *See* INA § 340(a) [8 U.S.C. § 1451(a)] (providing authority for civil denaturalization); 18 U.S.C. § 1425 (providing authority for criminal denaturalization); and Sections 4.7-4.8 below; *see also* the Denaturalization Investigations Handbook (OI HB 08-01), dated January 15, 2008, or as updated.

#### **4.7 Civil Denaturalization Statute**

The civil denaturalization statute, INA § 340(a), states that U.S. Attorneys for the respective districts have the duty, upon an affidavit showing good cause, to institute proceedings to revoke

citizenship and cancel the certificate of naturalization on the grounds that naturalization was “illegally procured” or was “procured by concealment of a material fact or by willful misrepresentation.” Revocation on these bases is also covered by 8 C.F.R. § 340.2. There is no statute of limitations for bringing a civil denaturalization action. *See* INA § 340(a); *see also United States v. Nuñez-Garcia*, 262 F. Supp. 2d 1073, 1087 (C.D. Cal. 2003). There is also no right to a jury trial in civil denaturalization proceedings. *See Luria v. United States*, 231 U.S. 9, 27-28 (1913).

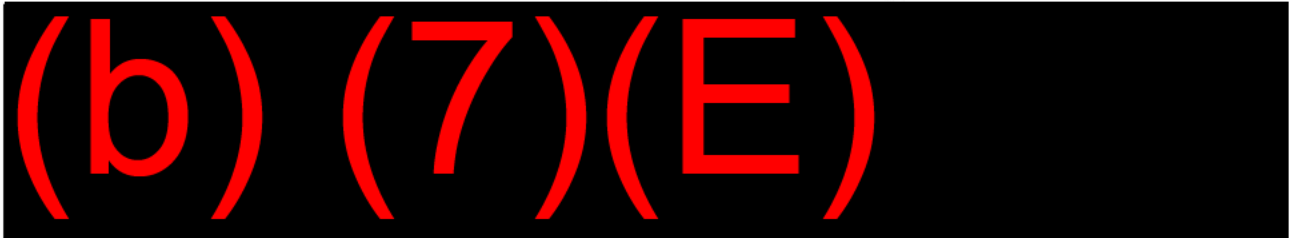
#### **4.8 Criminal Denaturalization Statute**

Authority for the criminal prosecution of unlawful procurement of citizenship or naturalization is found in 18 U.S.C. § 1425. When a person has been convicted of a violation of 18 U.S.C. § 1425, the court where the conviction occurred shall “revoke, set aside, and declare void the final order admitting such person to citizenship, and shall declare the certificate of naturalization of such person to be canceled.” *See* 8 U.S.C. § 1451(e).

#### **4.9 References**

- A. PDD 39, U.S. Policy on Counterterrorism, issued June 21, 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, Protection Against Unconventional Threats to the Homeland and Americans Overseas, issued May 22, 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 CT 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, Combating Terrorism through Immigration Policies, issued October 29, 2001 (as amended by HSPD 5), 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 noncitizens associated with, suspected of being engaged in, or supporting terrorist activity, and to locate, detain, prosecute, or deport any such noncitizens already present in the United States.
- D. HSPD 6, Integration and Use of Screening Information to Protect Against Terrorism, issued September 16, 2003, provides a consolidated approach to proactively target terrorist travel. It establishes the TSC to consolidate terrorist names and identifiers into a single database. Furthermore, it mandates that all international terrorist information be provided to the NCTC. Under HSPD 6, agencies are prohibited from maintaining a separate terrorist watchlist.

- E. HSPD 7, Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003, 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 set forth the responsibilities for CIKR partners.



- G. HSPD 19, Combating Terrorist Use of Explosives in the United States, issued on February 12, 2007, 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, Biometrics for Identification of Screening to Enhance National Security, issued June 5, 2008, 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. DHS Directive 262-02, Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes, dated November 15, 2016, or as updated, and DHS Instruction 262-02-011, Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes, dated November 21, 2016, or as updated.
- K. DHS Directive 215-01, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes, dated November 6, 2013, or as updated, and DHS Instruction 215-01-001, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes, dated November 7, 2013, or as updated.
- L. ICE Directive 10086.1, Oversight of ICE Personnel Serving on Federal Investigative Task Forces, dated March 25, 2016, or as updated.
- M. ICE Directive 10044.1 (former number: 7-6.1), Border Searches of Electronic Devices, dated August 18, 2009, or as updated. (Supersedes ICE Directive 7-6.0 only as it related to electronic devices. *See* Subsection O below.)



- N. ICE Directive 14019.1, Reporting Protocol Following a Designated National Security Event or U.S.-based International Terrorist Attack, dated December 3, 2019, or as updated.
- O. ICE Directive 7-6.0, Border Searches of Documents and Electronic Media, dated July 16, 2008, or as updated or superseded. (Superseded by ICE Directive 10044.1 (former number: 7-6.1) only as it relates to electronic devices. *See* Subsection M above.)

(b) (7)(E)

- Q. ICE Memorandum, Proper usage of FBI Time Utilization Record Keeping (TURK) system by ICE Joint Terrorism Task Force (JTTF) agents, dated May 5, 2010, or as updated.

(b) (7)(E)

- S. ICE Memorandum (Policy #10068.1), DHS Guidance Regarding Polygraph Examinations of ICE Officers Assigned to the FBI Joint Terrorist Task Forces, dated January 22, 2007, or as updated.
- T. ICE Memorandum, U.S. Immigration and Customs Enforcement Reporting following a Designated National Security Event/U.S.-Based Terrorist Attack, dated April 3, 2018, or as updated.

(b) (7)(E)

- V. HSI Memorandum, Minimum Commitment and Requirements for Special Agent Assignments to the Joint Terrorism Task Forces, dated June 27, 2019, or as updated.

(b) (7)(E)

- X. OI Memorandum, Border Searches of Electronic Devices Directive, dated August 31, 2009, or as updated.
- Y. OI Memorandum, Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media, dated December 12, 2008, or as updated.
- Z. 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.

- AA. USCIS Memorandum, Immigration File Sharing and Sequestration Procedures Used During a National Security Event, dated February 5, 2014, or as updated.
- BB. 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.
- CC. 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.
- DD. Memorandum of Understanding between the U.S. Customs Service and the Federal Bureau of Investigation, dated January 6, 2000, or as updated.
- EE. Memorandum of Understanding between the Immigration and Naturalization Service and the Federal Bureau of Investigation, dated June 18, 1999, or as updated.
- FF. Case Management Handbook (HSI HB 20-04), dated July 1, 2020, or as updated.
- GG. Asset Forfeiture Handbook (HSI HB 20-01), dated January 28, 2020, or as updated.
- HH. Arrest Procedures Handbook (HSI HB 15-03), dated July 21, 2015, or as updated.
- II. Search and Seizure Handbook (HSI HB 12-04), dated September 14, 2012, or as updated.
- JJ. Denaturalization Investigations Handbook (OI HB 08-01), dated January 15, 2008, 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 oversight of the policies and procedures set forth in this Handbook.

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

The AD, NSD, is responsible for the programmatic oversight over the production, interpretation, and modification of the policies and procedures set forth in this Handbook.

### **5.3 Unit Chief, National Security Unit**

The NSU Unit Chief is responsible for the development, production, and implementation of the provisions of this Handbook throughout HSI.

### **5.4 Section Chiefs, Counterterrorism Sections**

The Section Chiefs for CTS are responsible for serving as the points of service and coordination for all JTTF International Terrorism investigations and threat streams.

### **5.5 Special Agents in Charge**

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

### **5.6 Resident Agents in Charge and Group Supervisors**

Resident Agents in Charge (RACs) and Group Supervisors (GSs) who are tasked with managing SAs assigned to JTTFs are responsible for complying with relevant provisions of this Handbook.

### **5.7 Special Agents**

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

## **Chapter 6. COUNTERTERRORISM INVESTIGATIVE PRIORITIES AND PROGRAMS**

### **6.1 National Security Division**

NSD leads HSI's efforts to identify, disrupt, and dismantle transnational criminal enterprises and terrorist organizations that threaten the security of the United States. NSD protects the United States by enhancing national security through criminal investigations; preventing acts of terrorism by targeting the people, money, and materials that support terrorist and criminal activities; and identifying and eliminating vulnerabilities in the security of the nation's border, economy, transportation networks, and infrastructure.

NSD executes its mission using the unique investigative authorities that HSI commands. HSI's combined authorities for enforcing immigration and customs laws serve as a powerful tool in national security investigations – a tool that no other law enforcement agency holds.

NSD is comprised of two programs:

- A. National Security Programs (NSP); and
- B. Student and Exchange Visitor Program (SEVP).

## **6.2 National Security Programs**

NSP's mission is to protect our nation against terrorists, foreign intelligence entities, and transnational criminal organizations that threaten national security, public safety, and U.S. trade, travel, and financial systems. NSP is comprised of three Units and a cadre of National Security Liaisons who assist with the larger mission of protecting the United States:

- A. The Counter Threat Lead Development Unit (CTLTD) investigates nonimmigrant visa holders who violate their immigration status. CTLTD places the highest priority on monitoring the activities of suspected terrorists and combating criminal exploitation of the nation's student visa system. CTLTD accomplishes its mission through research and analysis, targeted operations, special initiatives, and leveraging of expertise with partner agencies. (*See the CTLTD page on HSI Net for more information.*)
- B. The Human Rights Violators and War Crimes Unit (HRVWCU) pursues foreign war criminals, persecutors, and human rights abusers who seek shelter from justice in the United States. The Unit also oversees the Human Rights Violators and War Crimes Center, which consists of HSI SAs and Criminal Analysts, USCIS Liaisons, SAs and intelligence analysts from the FBI's International Human Rights Unit, DOS Liaisons, and attorneys and historians from OPLA and DOJ's Human Rights and Special Prosecutions Section and Office of Immigration Litigation. (Note: *See the HRVWCU page on HSI Net for more information.*)
- C. NSU integrates and synchronizes operational equities, intelligence information, support elements, and policy efforts to mitigate and combat threats to national security. NSU maintains programmatic oversight of all HSI engagement on the JTTFs and the Counterintelligence Task Forces (CITFs) nationwide, manages HSI's core and advanced National Security Professional Development training (CT and counterintelligence), and provides operational coordination and support to all JTTF-led international terrorism and CITF-led counterintelligence investigations and threat streams within ICE. NSU is also responsible for developing, coordinating, facilitating, and implementing policies in support of HSI's and the U.S. Government's national security efforts.

NSU is comprised of three sections: Counterterrorism Operations Sections I and II (collectively CTS) and the Mission Development Section. NSU personnel utilize their placement and access within partner agencies' CT and counterintelligence elements to ensure that HSI's equities and broad range of investigative authorities and capabilities

are considered and infused into operational objectives and strategies to identify, investigate, and disrupt national security threats against the United States.

- D. National Security Liaisons are senior HSI personnel who coordinate investigative activity under assignments to various federal agencies and departments. As part of NSD, Liaisons are essential to establishing partnerships and developing close and cooperative working relationships with HSI's partner agencies.

### **6.3 Office of the Principal Legal Advisor**

OPLA, consisting of a team of HQ attorneys based in Washington, D.C., along with field attorneys in OPLA field locations nationwide, manages the litigation of national security cases in removal proceedings. OPLA HQ, in consultation with OPLA field locations, provides legal advice and guidance to all ICE Directorates and Program Offices responsible for cases involving terrorism, espionage, sabotage, and other immigration issues related to national security, including:

- A. The detention and removal of noncitizens described in INA § 212(a)(3) and INA § 237(a)(4);
- B. The designation of terrorist organizations under INA § 219 and as defined in INA § 212(a)(3)(B)(vi);
- C. The civil arrest authority of SAs;
- D. Criminal charges under Titles 8 and 18;
- E. Benefit eligibility; and
- F. Denaturalization.

Because of the variety of considerations involved in national security cases, lodging of security and terrorism-related charges of inadmissibility (INA § 212(a)(3)), deportability (INA § 237(a)(4)), and/or raising certain national security bars to relief requires the approval of OPLA HQ.

OPLA HQ provides assistance (in the form of training, legal review of DHS and ICE policies and procedures, and reviews of press and congressional responses) to ICE Directorates and Program Offices, including HSI, ERO, the Office of Congressional Relations, the Office of Regulatory Affairs and Policy, and the Office of Public Affairs. OPLA also provides litigation support to DOJ on immigration aspects of criminal prosecution cases involving noncitizens of national security concern. OPLA HQ serves as a liaison in national security matters to the FBI, DOS, the Central Intelligence Agency (CIA), and various DOJ Offices and Divisions, such as the Office of International Affairs, the Civil Division's Office of Immigration Litigation, the Criminal Division's Counterterrorism Section, and the local USAOs.

## **Chapter 7. HSI FIELD OFFICE JOINT TERRORISM TASK FORCE PARTICIPATION AND ROLES**

### **7.1 HSI's JTTF Commitment and Functions**

HSI is fully partnered with the FBI at CTD and at JTTFs nationwide to ensure that HSI's authorities are leveraged to most effectively execute the shared national security mission to safeguard the security of the United States. HSI SAs substantially contribute to the JTTFs by enforcing the authorities entrusted to ICE which span a diverse set of investigative areas relating to, among others, immigration, money laundering, smuggling and trafficking, trade violations, and cyber security. HSI remains committed to the JTTF structure, evidenced by the fact that HSI is the largest federal contributor of personnel at both the JTTFs and ITOS.

SAs assigned to the JTTF conduct CT investigations, intelligence, and enforcement operations within the scope of HSI's well-established abilities to engage in investigations that leverage broad authorities, grounded in immigration/customs authorities that center on the movement of people, goods, and information into and throughout the United States. Furthermore, SAs are, in most cases, statutorily authorized to concurrently perform the functions of other DHS components as "Customs Officers" and "Immigration Officers."

In other instances, HSI provides input and expertise, and adds value to CT investigations, intelligence gathering and enforcement actions and to significant CT mechanisms, such as the TSA "No-Fly List." In addition to proactive CT investigations, HSI's capabilities are even more relevant in post-attack response operations as HSI SAs are able to seamlessly integrate into multiple law enforcement, intelligence, and analytical mechanisms.

As stated in Chapter 2, SAs should strive to be designated as case managers, co-case managers, or case participants in FBI's case investigative systems (Sentinel and/or Guardian) on investigations in which they are substantially engaged. Often, this applies to situations where ICE authorities can potentially be utilized against an individual or individuals to disrupt or dismantle a terrorist organization or national security threat.

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

### **7.2 HSI JTTF Special Agents' Role**

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 directly support the objectives of PDD 39. HSI plays a pronounced and critical role in U.S. CT efforts to further the war on terrorism and continues to provide unique investigative value that is highly regarded by law enforcement and the IC.

Below are examples demonstrating how SAs provide invaluable support to the JTTF mission. The list is not all-inclusive, but instead serves as a sample of HSI's vast statutory authorities, investigative methods, and international footprint. Of note, HSI SAs do not gain additional authority while assigned to a JTTF. HSI SAs must continue to abide by DHS and ICE policies while supporting a JTTF, such as in the examples below.

SAs are predominantly assigned to JTTF International Terrorism (IT) and Guardian/Assessment squads as those assignments overwhelmingly involve ICE- and HSI-centric equities. SAs also partner on Extraterritorial Terrorism IT squads, Domestic Terrorism (DT), Weapons of Mass Destruction (WMD), Human Intelligence (HUMINT), and counterintelligence squads. Every JTTF is unique, and some JTTF locations only have one squad which manages all CT matters, while others have hybrid squads, e.g., Guardian/DT squad.

SAs typically:

- A. Advise as to the inadmissibility or removability of targets and potential targets, in consultation with the local OPLA field location;
- B. Travel as operationally required (travel expenses for JTTF investigations are funded by the JTTF and/or ITOS);

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

- D. Effect administrative arrests pursuant to the INA in an effort to detect, deter, and disrupt terrorists and acts of terrorism;
- E. Coordinate detention of arrested noncitizens with ERO;
- F. Query multiple data sets for travel records for use in tracking, analysis, and target exploitation;
- G. Ascertain immigration/entry status of targets and affiliates and disseminate same pursuant to policy;
- H. Obtain and analyze A-File information for use in investigations;
- I. Perform border searches;
- J. Retain, analyze, disseminate, and dispose of border search information;
- K. Advise and assist in the procurement, issuance, and use of parole and other immigration benefits;
- L. Determine the viability for potential denaturalization proceedings;

- M. Plan, coordinate, and execute Form I-9 inspections of target businesses or businesses employing targets of investigations;
- N. Leverage HSI International Operations' network of Attaché offices and foreign law enforcement, customs, and immigration partnerships for information collection, analysis, and exploitation;
- O. Conduct parallel criminal investigations of targets suspected of immigration/customs criminal violations;
- P. Leverage NSD and other HSI assets for use in the production and analysis of products located in DHS holdings; and
- Q. Advise on and leverage DHS programs, components, authorities, and entities for use in investigations.

The following are commonly used JTTF terms, acronyms, and abbreviations:

ADIC	Assistant Director in Charge
AFRICOM	U.S. Africa Command
ALAT	Assistant Legal Attaché
ARC	Airlines Reporting Corporation
CART	Computer Analysis Response Team
CENTCOM	U.S. Central Command
CHS	Confidential Human Source
EA	Emergency Action
EC	Electronic Communication
ERT	Evidence Response Team
EUCOM	U.S. European Command
FBINet	FBI Classified Network (Red)
FCI	Foreign Counterintelligence
FD-1023	Source Reporting Document (FBI)
FD-302	Report of Investigation (FBI)
FISUR	Physical Surveillance
(b) (7)(E)	(b) (7)(E)
FTOC	Foreign Transfer of Custody
(b) (7)(E)	(b) (7)(E)
FVEY	Five Eyes (US, UK, NZ, AU & CA)
HIG	High Value Detainee Interrogation Group
IA	Intelligence Analyst
IED	Improvised Explosive Device
IOD	International Operations Division (FBI/HQ)
JOC	Joint Operations Center
JSOC	Joint Special Operations Command



LEGAT	Legal Attaché (Diplomatic or Consular Posting)
LPR	Lawful Permanent Resident
NORTHCOM	U.S. Northern Command
NSLB	National Security Law Branch
(b) (7)(E)	
PACOM	U.S. Pacific Command
POL	Pattern of Life
SABT	Special Agent Bomb Technician
(b) (7)(E)	(b) (7)(E)
SIA	Supervisory Intelligence Analyst
SOG	Special Operations Group (Armed/Agents)
SOS	Staff Operations Specialist
SOUTHCOM	U.S. Southern Command
SSA	Supervisory Special Agent
SSG	Special Surveillance Group (Unarmed)
TEDAC	Terrorist Explosive Device Analytic Center
TREX	Terrorist Review and Examination Unit
TSOU	Terrorist Screening and Operations Unit
(b) (7)(E)	
UNET	Unclassified FBI Network
USPER	U.S. Person
USSOCOM	U.S. Special Operations Command

### 7.3 HSI Supervisors of HSI JTTF Special Agents

HSI supervisors tasked with managing SAs assigned to the JTTFs are responsible for coordination, engagement, and information-sharing activities in addition to typical supervisory duties. SAs are typically assigned to JTTF offices in full-time or part-time capacity, with each type of assignment being equally important to CT investigations and the HSI commitment to JTTF staffing.

HSI supervisors should be fully engaged regarding matters pertaining to the role of HSI at the local JTTFs in not only HSI supervisory roles and duties, but also via active participation and coordination with JTTF partners and FBI JTTF management.

Furthermore, HSI supervisors are typically required to meet with HSI field management (SAC/ Deputy SAC (DSAC)/Assistant SAC (ASAC), etc.) and provide regular case updates, particularly when ICE authorities are applied in furtherance of a JTTF investigation. Supervisors should also advise field management of proposals, policies, and issues that may involve intensive media interest, require analysis of interagency policies, or have longstanding effects on the performance of investigative operations, as these may require visibility and input from HSI HQ.

HSI managers who supervise SAs assigned to the JTTF should:

- A. Maintain an appropriate security clearance for the local JTTF;
- B. When applicable, maintain unclassified/classified systems computers access (Joint Worldwide Intelligence Communications System (JWICS), Homeland Security Data Network (HSDN), FBI Net, FBI Intranet email, FBI Case Management Systems, etc.);
- C. Ensure that SAs assigned to a JTTF retain an ICE-issued laptop and a valid U.S. Government official passport;
- D. Maintain information on locally assigned non-JTTF SAs who retain proper security clearances/previous national security CT experience for use if necessary;
- E. Obtain access to JTTF facilities and develop relationships with their FBI counterparts;
- F. Regularly attend and participate in JTTF management meetings;
- G. Ensure that all cases in Investigative Case Management (ICM) are created, updated, and maintained pursuant to established policies;
- H. Ensure the timely submission and accuracy of all reporting in the SEN system;
- I. Manage information disclosure to field leadership pursuant to law, policy, guidelines, and interagency relationships;
- J. Notify the FBI JTTF Supervisor if the HSI JTTF SA will be absent from the JTTF due to leave, temporary duty (TDY), or other HSI commitments; and
- K. Remain engaged with CTS elements regarding case coordination, information requests, international travel, etc.

## **Chapter 8. HSI HEADQUARTERS OPERATIONAL AND PROGRAMMATIC SUPPORT TO COUNTERTERRORISM EFFORTS**

### **8.1 HSI CTS Mission Statement and Field Support**

The mission of CTS is to investigate, disrupt, and dismantle terrorist organizations that pose a persistent threat to U.S. national security and interests. The vision of CTS is to enhance the defense of the Homeland from persistent international terrorist threats through HSI's unique investigative authorities and placement within the U.S. CT apparatus.

For HSI, CTS is the point of service and coordination for all JTTF international terrorism investigations and threat streams. CTS personnel are HSI Liaison Officers (LNOs) assigned to the FBI CTD's command and control element, ITOS, and are embedded within every U.S. CONUS team. For HSI, CTS staff members serve as subject matter experts on CT operations, provide NSD with a comprehensive picture of pertinent investigations and disruptions, and hone in on HSI's partnership with and role in the same. HSI is the FBI's largest federal partner and longest standing federal contributor to the JTTFs and, due to increased threats from FTOs, has strived to enhance its current footprint both in ITOS and across the JTTFs. In any given year, HSI SAs are engaged in a majority of JTTF investigations and disruptions. Moreover, ICE and HSI's unique authorities and capabilities are often utilized as the disruption option of choice.

CTS is charged with executing one of DHS, ICE, and HSI's priorities to prevent terrorist attacks. As ambassadors of HSI embedded within ITOS, CTS fully supports, both operationally and administratively, HSI SAs and their supervisors who are assigned to the JTTFs nationwide. CTS is the linchpin between disparate elements of HSI HQ, the FBI, and HSI JTTF SAs. CTS provides ICE and HSI strategic and tactical capabilities and disruption options (along with advantages, disadvantages, and considerations) for ultimate decision-making by the FBI JTTF leadership, fused with ITOS leadership, in JTTF investigations. CTS ensures that NSD leadership has full spectrum visibility and advanced warning into appropriate investigations where HSI capabilities and disruption options are employed, and where HSI SAs are otherwise significantly involved as case managers, co-case managers, or case participants in FBI's classified investigative case management platforms.

CTS Program Managers (PMs) in ITOS inject HSI insights and expertise into pressing, time-sensitive CT investigations and threat streams. As investigative plans are being considered and decisions are being weighed, CTS provides the FBI with ICE and HSI capabilities, referred to as 1st thru 4th Order Operations.



## **8.2 Counterterrorism Operations Section Goals**

- A. Prevent terrorist attacks;
- B. Coordinate HSI support to the FBI through embedded support to CTD and JTTFs;
- C. Operationally and administratively support HSI SAs assigned to JTTFs;
- D. Strengthen HSI relationships with key CT partners;
- E. Increase HSI's capability to respond to U.S.-based terrorist attacks;
- F. Centralize post terrorist attack support and communications for HSI and ICE;
- G. Offer unique terrorism disruption capabilities and options;
- H. Recognize HSI personnel contributions to CT Operations;
- I. Ensure that HSI leadership is aware of emerging threat streams and terrorism investigations; and
- J. Train, certify, and accredit HSI JTTF SAs, leaders, and other personnel for full partnership within the JTTF.

## **8.3 Counterterrorism Investigative Priorities**

CTS maintains programmatic oversight of HSI's investigation, detection, interdiction, and participation in the prosecution and/or removal of the following classifications of targets when associated to the JTTF:

- A. KST, as well as promoters, financiers, and supporters of terrorism;
- B. Hostile foreign intelligence agents engaged in espionage;
- C. Those noncitizens in the United States, or those attempting to gain entry or admission to the United States, who, by their actions, associations, or affiliations, are reasonably believed to pose a threat to the national security of the United States; and
- D. Any person or organization whose activities facilitate the unlawful entry, export, employment, movement, or harboring of goods or people posing a threat to the national security of the United States.

A. Background

(b) (7)(E)

(b) (7)(E)

B. (b) (7)(E) (b) (7)(E)

(b) (7)(E)

C. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

D. (b) (7)(E)

(b) (7)(E)

## Chapter 9. CONDUCTING COUNTERTERRORISM INVESTIGATIONS

### 9.1 Field Coordination with HSI CTS Related to Investigations

For coordination and deconfliction purposes, HSI SAs engaged in CT investigations shall notify CTS of all significant investigative activities and maintain constant communication with CTS regarding such investigations. SAs will also email CTS via FBI secure communication systems when they begin to serve as case manager, co-case manager, or case participant on an investigation. Moreover, should HSI SAs need to contact the ITOS FBI Supervisory Special Agent (SSA), they must include CTS in the communication.

National security CT investigative matters encompass activities involving individuals who are suspected of being involved in terrorism or are direct or indirect supporters of a terrorist organization.

### 9.2 Investigative Case Management

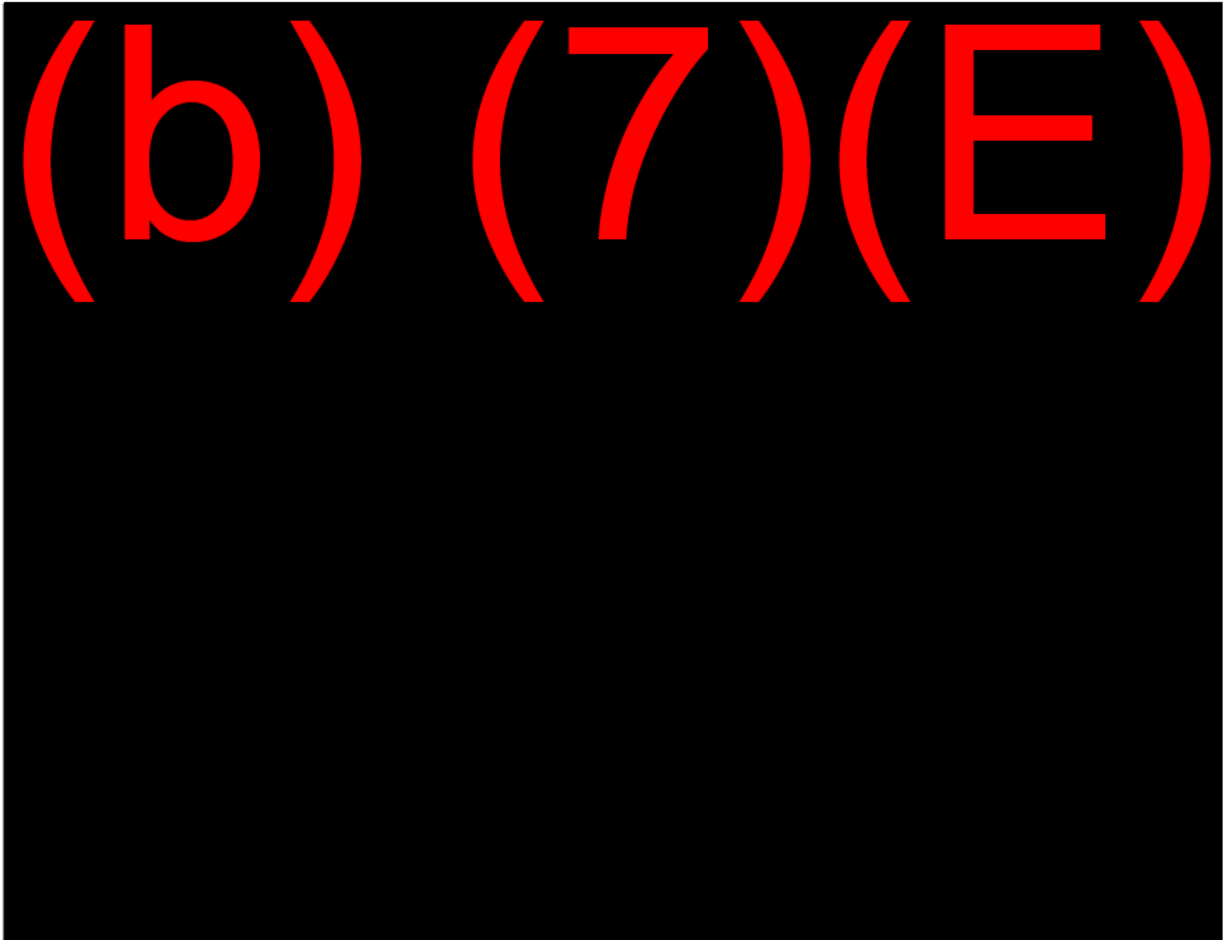
(b) (7)(E)

(b) (7) (E)

(b) (7) (E)

B. Case Categories

(b) (7) (E)



C. Documenting Investigative Reports

Except for classified information, and after consultation with their FBI and HSI supervisor, SAs will document investigative activity in ICM via Reports of Investigation (ROIs) regardless of whether or not HSI is investigating the case through the JTTF.

ICE employees will follow all relevant guidance and procedures for protecting the sources and methods used to collect information and adhere to federal laws, agreements, and regulations that ensure proper maintenance and retention of information and protect against unauthorized access, use, disclosure, or compromise of information.

Statistical information derived from ICM supports the information needs of HSI leadership by providing the data necessary to meet the strategic goals of the agency. In addition, ICM provides investigative data and statistical information used for agency and management oversight, budget allocation, and statistical analysis. HSI



managers use ICM and statistical information for resource allocation purposes in order to make the most effective use of limited resources.

Specifically related to the JTTF, ICM enables an understanding of the utility of ICE's resources in CT activities and allows for broader recognition of the critical role ICE plays in the CT mission. Investigative activity conducted by ICE personnel, captured through ICM, provides leadership with insight into the myriad ways ICE enhances CT investigations. (b) (7)(E)

(b) (7)(E) In addition, capturing investigative information in ICM provides HSI personnel worldwide with a deconfliction mechanism that is critical to the successful execution of HSI's multi-faceted, international investigations.

D. Documenting Arrests

(b) (7)(E)

E. Documenting Seizures

(b) (7)(E)

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

The mandatory JTTF and national security check boxes will be utilized throughout all ICM case categories. (b) (7)(E)

(b) (7)(E)

(b) (7) (E)

(b) (7) (E)

G. Appropriate Use of ICM Subject Record Status Codes

(b) (7) (E)

(b) (7)(E)

#### H. SCR Designation of Counterterrorism Investigations

Traditionally, HSI investigations have led to arrests, to post arrest activity, and, often, to seizures. HSI SAC and HQ leadership understand that traditional methodologies of capturing arrest statistics, post arrest or other investigative activities, and seizures do not apply equally for CT-related investigations. HSI SAC and HQ leadership fully understand that CT investigations focus on intelligence collection while simultaneously being run as criminal investigations. Because of this and in order to highlight HSI's engagement in CT investigations, HSI JTTF investigations involving a (b) (7)(E) are eligible for consideration for SCR status. Applicable JTTF SCR designation is critical to highlight to SAC and HQ leadership the level of engagement of HSI JTTF SAs. At the earliest opportunity, SAs should coordinate with their local FBI office and/or USAO to determine the preferred method of documenting unclassified investigative reports derived through joint investigations, interviews, and enforcement activities. This coordination ensures an accurate and consistent account of the reportable event while creating an unclassified written record that can be used simultaneously by HSI, OPLA, and the FBI.

CTS provides SAs with assistance in the submission of national security CT/HSI JTTF investigations (b) (7)(E) as significant cases via the production of SCRs. CTS can assist in the drafting of SCRs and provide examples to ensure that SAs and field management are aware of the reporting and coding requirements for same. SAs are encouraged to contact CTS upon the initiation of an investigation that qualifies for SCR submission. CTS will also ensure that proper guidance is provided to relevant parties regarding the existence of classified information and processes relative to procuring/disclosing such information.

#### I. Coordination in Support of Counterterrorism Investigations in Foreign Countries

Because of the international nature of investigations, SAs may be required to travel abroad or request information from foreign governments to further their cases. In locations where HSI International Operations does not maintain a presence, CTS will assist SAs and coordinate with other agency partners to obtain the necessary information and ensure that proper support is received at the foreign location. CTS will also notify HSI International Operations to ensure coordination and facilitate support with the respective HSI Attaché.

### 9.3 **Predicating Information and Intelligence**

The strategy and mindset of SAs conducting CT investigations should be to utilize as many resources as appropriate based on HSI's broad statutory authorities.

Investigations commonly begin with an allegation of a violation of federal law related to immigration and/or customs statutes. The case may begin with a broad allegation of terrorism based on IC reporting or other non-law enforcement agency information. SAs should review the predicated intelligence and any investigative information received from another agency to identify any activity that involves criminal or administrative violations enforced by HSI.

#### **9.4 JTTF Investigations Predicated on HSI Information**

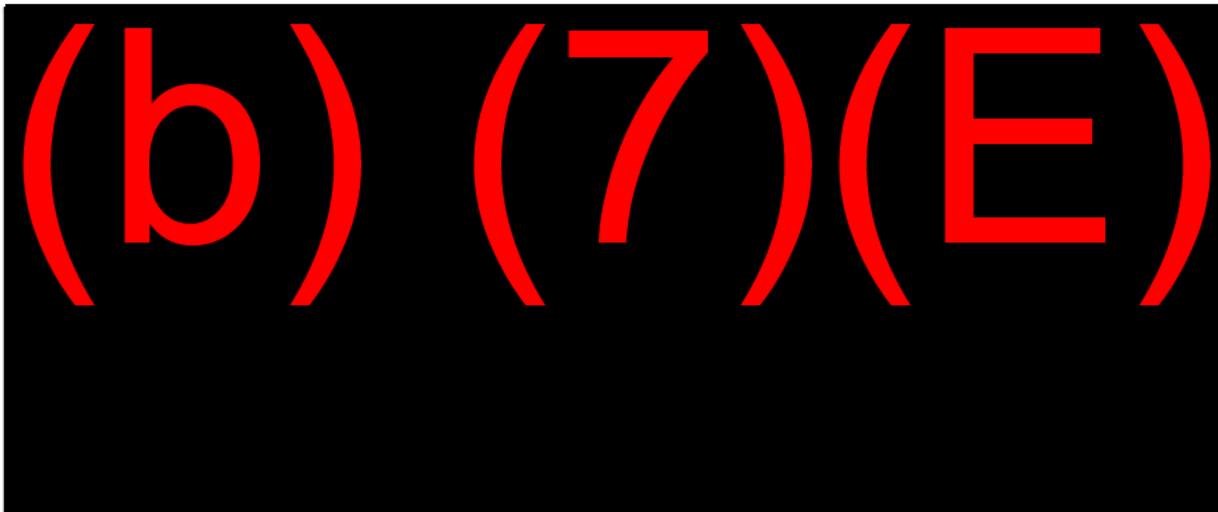


#### **9.5 JTTF Investigations Predicated on FBI Information or Investigations in Which ICE Violations Are Predicate Offenses**

SAs will routinely partner with the FBI or other Task Force Officers (TFOs) as case agents or co-case agents on various types of investigations. HSI should ensure that its investigative capabilities and authorities are represented and communicated and that SAs are fully engaged in any investigation where ICE-specific violations may provide a disruption or dismantlement option. In situations where the aforementioned is applicable but the HSI JTTF SA is serving on a different squad, the HSI JTTF SAs will still communicate with the HSI and FBI first-line supervisors and provide support as needed.

#### **9.6 Initiating a Counterterrorism Investigation**

When initiating a CT investigation, SAs should:



(b) (7) (E)



## **9.7 Information Security Considerations**

During a CT investigation, 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 information derived from or via their investigation. Attempts should be made to recreate, in an unclassified format, any classified information discovered. (*See* Section 9.19.)

Additionally, SAs should be aware of the proprietary interests of other federal law enforcement and government agencies. Pursuant to 28 U.S.C. § 533, 28 C.F.R. § 0.85, and PDDs 39 and 62, the FBI is authorized to coordinate all law enforcement investigative and operational responses to terrorism via the JTTF and, as a result, it behooves all SAs when conducting CT investigations to be mindful of FBI deconfliction and/or retention, safeguarding, maintenance, disclosure, and dissemination of information requirements regarding such investigations.

## **9.8 Collaboration with Federal, State, and Local Law Enforcement and Other Government Agencies**

SAs should consult with appropriate federal, state, and local law enforcement and other government agencies, in addition to the FBI, and review all relevant reporting for any information they maintain on a subject. SAs assigned to a JTTF should reach out to other TFOs to determine if they have investigative insights to support an investigation.

## **9.9 Identifying Potential Immigration Violations**

SAs should carefully examine all available information to ascertain whether a subject is amenable to ICE action on criminal, civil, or administrative grounds. Whenever possible throughout the course of their investigation, SAs should attempt to obtain admissible evidence that may be used to overcome alleged humanitarian factors as well as evidence that would preclude the granting of discretionary relief. In these situations, SAs will communicate the potential HSI disruption options and/or investigative opportunities in writing with their HSI and FBI JTTF supervisors, as well as with CTS.

## **9.10 Managing Foreign Government-Related Information**

When SAs require interaction with an outside law enforcement agency and/or a foreign government as part of an investigation, they should obtain the concurrence of their HSI

supervisor and other applicable U.S. Government entities before such interaction takes place and conduct same pursuant to all applicable policies.

(b) (7) (E)

**9.12 Engaging the U.S. Attorney’s Office and the Local OPLA Field Location in Counterterrorism Investigations**

SAs should consult with the USAO and the designated attorneys at their local OPLA field location early in the investigation and facilitate communications between the local OPLA attorneys and Assistant U.S. Attorneys prior to the submission of charging documents and prosecution memoranda. In investigations of violations of the import and export laws relating to sensitive information or technology, SAs should consult with the local OPLA field location. Additionally, SAs should engage CTS to begin coordination with OPLA HQ attorneys.

**9.13 Considerations When Interviewing and Taking Statements on Information in Counterterrorism Investigations**

To determine the necessity of interviewing individuals who could have information pertinent to an investigation, SAs should consult with all U.S. Government entities that are parties to the investigation prior to conducting any interviews. SAs should consider interviewing individuals who know the subject, co-workers, present and/or previous employers, and residents in the neighborhood where the subject resides or previously resided, as long as the interviews will not compromise the integrity of the investigation.

(b) (7) (E)

**9.14 Considerations on Counterterrorism Investigations Regarding Individuals Who Are Nonimmigrants**

(b) (7)(E)

(b) (7) (E)

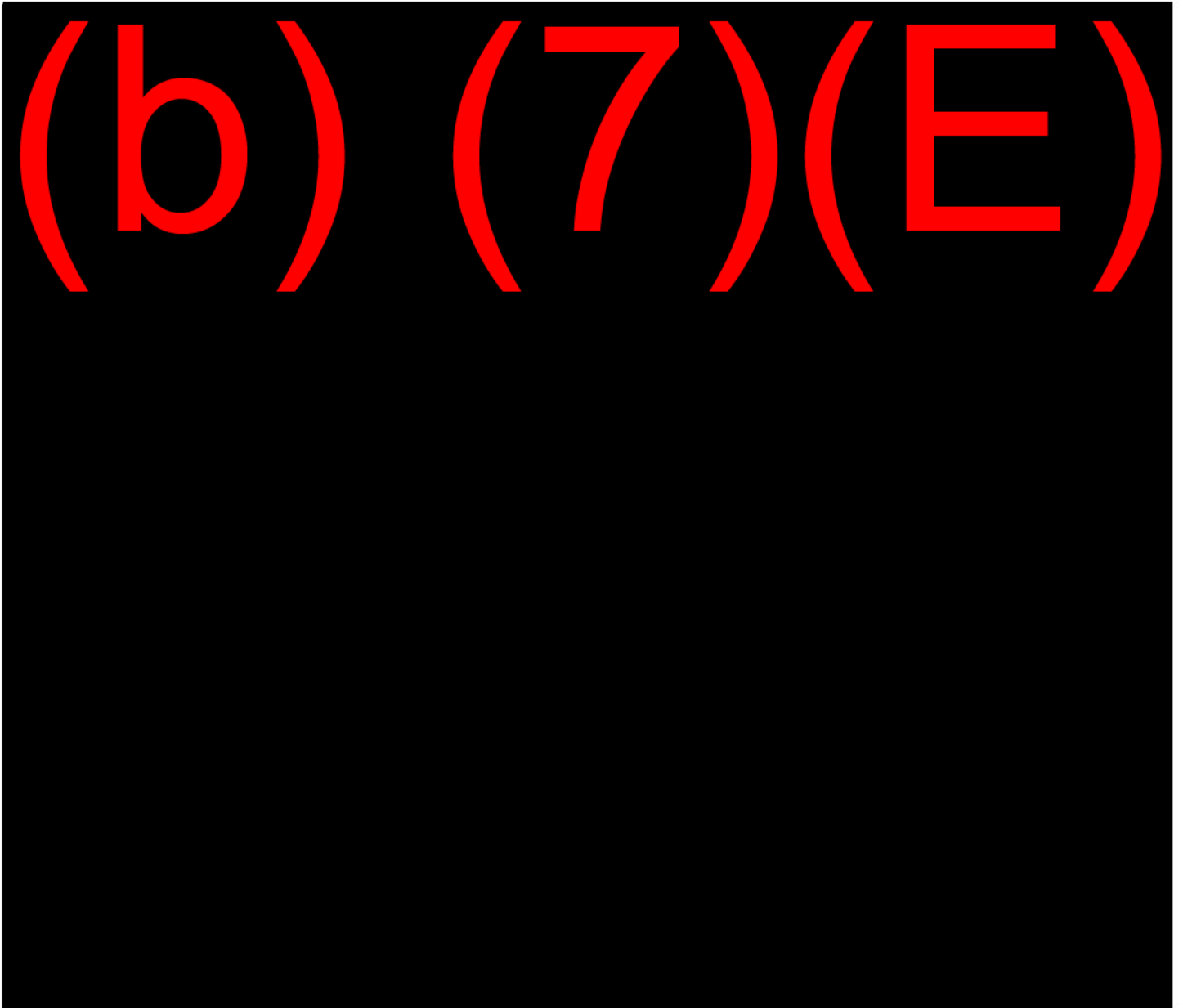
9.15 Other Investigative Activities in Furtherance of a Counterterrorism Investigation

(b) (7) (E)

(b) (7) (E)



## 9.17 Immigration or Document Fraud Schemes and Counterterrorism Investigations

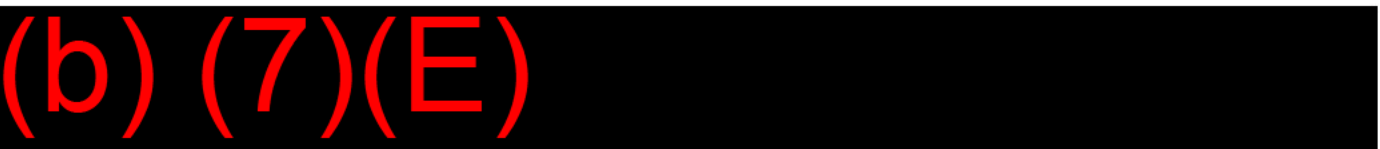
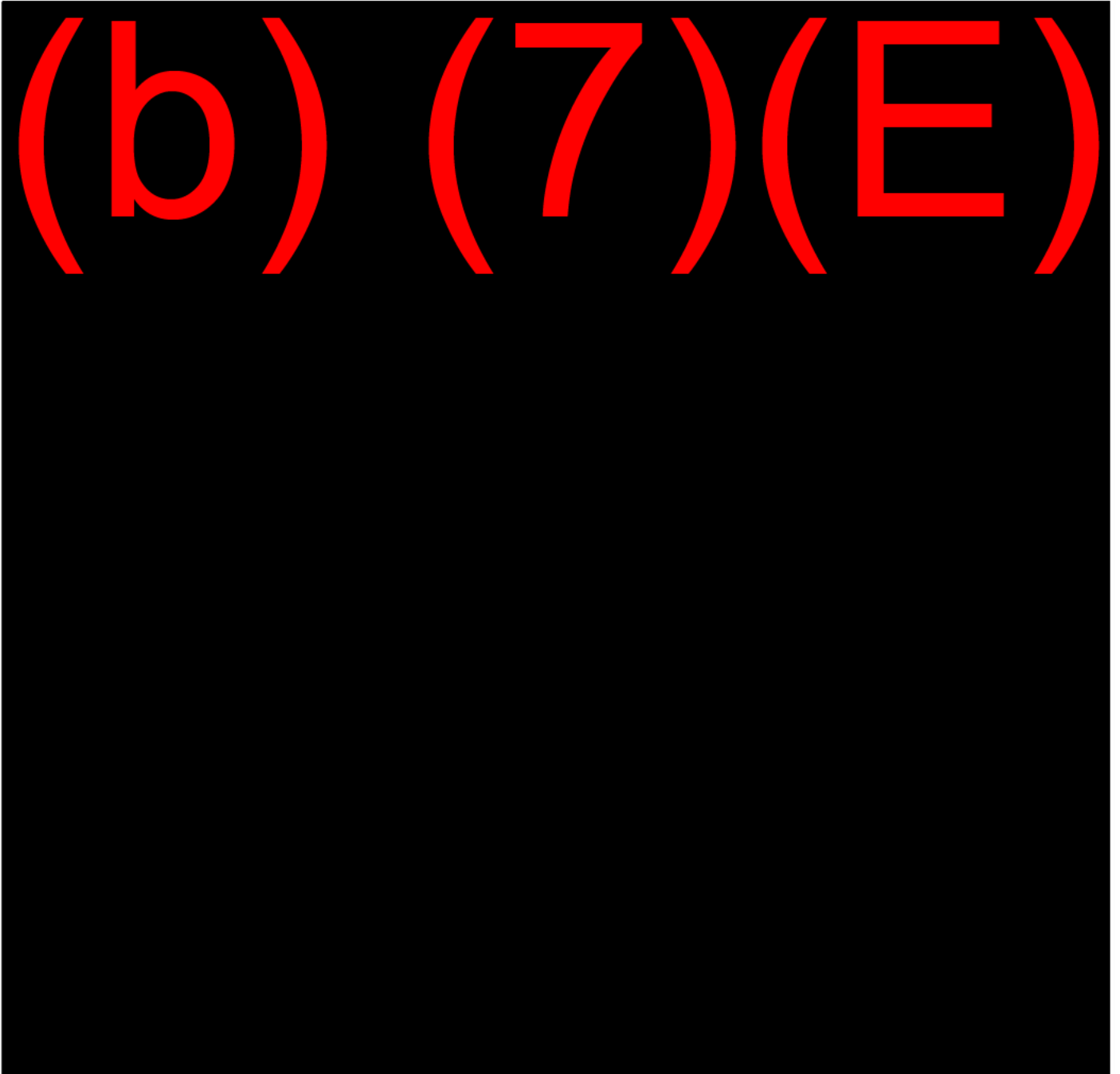


## 9.18 Headquarters-Led Counterterrorism and National Disruptive Efforts

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 definitive link to terrorism. These cases may be in support of national level disruptive efforts or fall under other national CT efforts. Examples may include requests to locate and administratively arrest

noncitizens with third-agency derogatory information or requests to investigate leads or complaints with national security implications received through the HSI Tip Line<sup>3</sup>.

**9.19 Classified Information in Counterterrorism Investigations**



(b) (7)(E)

## 9.20 Tools to Consider in Counterterrorism Investigations

(b) (7)(E)

### 9.20.1 Use of Databases in Counterterrorism Investigations

HSI's broad law enforcement authorities and significant DHS footprint provide for access to multiple information systems and databases that are helpful in conducting CT investigations. Access to such databases is a helpful tool for HSI SAs regardless of assignment or investigative program.

SAs must be mindful that many databases and systems utilized have restrictions on use and further dissemination of the information included in the system. As such, SAs should ensure that they have a complete understanding of each database and system's particular restrictions or limitations for use and dissemination prior to documenting or passing such information. Also, SAs should familiarize themselves with the "Third Agency Rule" and should not disseminate information belonging to another agency to any third agency without permission from the agency

that owns the information. SAs may consult OPLA for questions or concerns regarding the use of and dissemination of government information outside of DHS. The following are helpful database and system query tools:

(b) (7) (E)

(b) (7) (E)

(b) (7) (E)

### 9.21 CTS Investigative Partnership Functions

CTS is tasked with carrying out the agency's CT mission of deterring, disrupting, and preventing terrorist attacks. CTS is ICE's primary coordination element for all JTTF international terrorism threat streams and investigations within the agency. CTS personnel serve as subject matter experts on CT operations and provide NSD leadership with a comprehensive picture of pertinent CT investigations and operations.

CTS is comprised of PMs, Criminal Analysts (CAs), Management and Program Analysts (MPAs), and contractors, all of whom take on specific taskings to support the field and implement HSI's number one mission. All staff assigned to CTS must maintain security clearances and successfully pass a National Security Polygraph Examination.

CTS PMs are assigned to the FBI's CTD and are embedded in ITOS I & II and the Special Threats Section (STS) serving on geographic-based and/or threat-based FBI Units. The PMs'

primary role is to support the CT mission and, by definition, this directly supports HSI JTTF SAs and FBI CTD, ITOS, and STS staff. CTS' objective is to drive operations and anticipate the needs of the field while providing unparalleled support to JTTF personnel.

CTS PMs provide SAs with the following:

- A. A-File scans;
- B. Negotiation of declassification requests resulting in LHMs for utilization in immigration proceedings;
- C. Core and Advanced CT Training for JTTF SAs;
- D. Advanced notification on emerging investigations in the SAs' AOR;
- E. Case coordination meetings between HSI and other government agencies;
- F. Deconfliction for all potential national security CT investigations;
- G. Assistance in drafting SCRs;
- H. Identification and coordination of potential disruption options in consultation with OPLA HQ; and
- I. Dedicated post-attack support.

CTS has CAs both on site and at outside locations. The CTS CAs review intelligence on a daily basis in order to support intelligence-driven operations. Among other duties, CAs compare and apply historical and newly produced intelligence to current investigations.

The MPAs and contractors also provide a multitude of investigative services to CTS and the JTTF SAs operating in the field. A major contribution made by the MPAs and the contractors is the production of HSI subject reports, comprehensive informational documents culled from U.S. Government databases and non-government sources. These reports have proven to be a successful investigative tool to be used during interviews, post attack operations, etc.

The HSI subject reports typically contain:

- A. Biographic data (name, alias, date of birth (DOB), country of birth (COB)/country of citizenship (COC), Alien number (A number);
- B. Government issued numeric identifiers;
- C. Addresses, telephone numbers, email addresses;
- D. Immigration status and history;

- E. Travel history;
- F. Relatives and associates;
- G. Employment, education, finances, criminal history, and social media profiles; and
- H. Information extracted from the subject's A-File (where applicable), which includes USCIS Form N-400 (Application for Naturalization) details, financial details, family members, associates, employment, foreign addresses, interview notes, and refugee/asylum history and certain immigration benefits information. (Note: Information contained in or pertaining to asylum applications, credible fear determinations, reasonable fear determinations, and refugee applications, as well as applications for protection from removal under the Convention Against Torture regulations, withholding of removal under INA § 241(b)(3), and asylee/refugee follow-to-join petitions (USCIS Form I-730, Refugee/Asylee Relative Petition), can only be shared consistent with the disclosure restrictions at 8 C.F.R. § 208.6 and as otherwise provided by DHS Directive 262-02, Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes, dated November 15, 2016, or as updated, and DHS Instruction 262-02-001, Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes, dated November 21, 2016, or as updated.)

Upon receipt of the subject reports, and only as consistent with pertinent disclosure restrictions,<sup>4</sup> SAs in the field will share these reports with appropriate JTTF entities as necessary and upload them into FBI case management systems, as applicable.

(b) (7)(E)  
(b) (7)(E)  
(b) (7)(E) When a potential lead is identified, CTS conducts equities deconfliction to determine if the individual is already under investigation by the FBI, and generates a lead package to be sent to HSI JTTF SAs in the affected AOR. The lead package will generally include basic identifiers (Name, DOB, COB, COC, Alien Registration Number (ARN), last known address, etc.), TSDB watchlist status, FBI investigation status, classified derogatory information, and an unclassified HSI Subject Report.

CTS also provides SAs with assistance in the submission of national security (b) (7)(E)  
(b) (7)(E) CTS can assist in the drafting of SCRs and provide examples to ensure that SAs and field management are aware of the related reporting and coding requirements. SAs are encouraged to contact CTS upon the

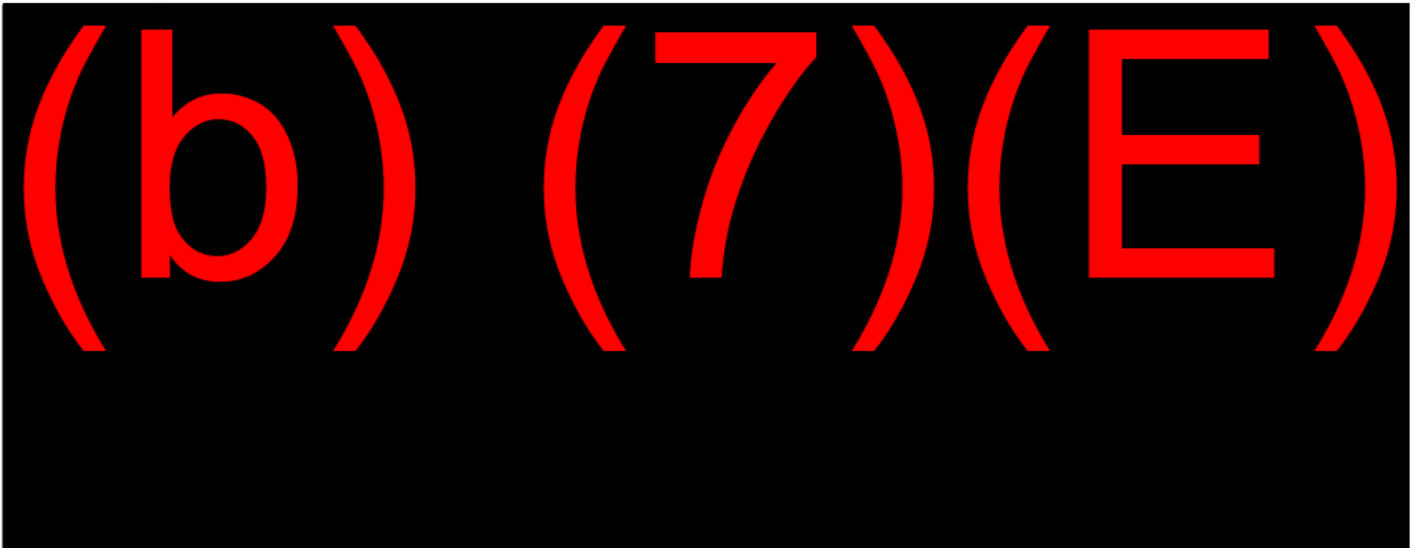
<sup>4</sup> In addition, for information covered by 8 U.S.C. § 1367 (VAWA, T Visa, U Visa) and potential disclosure restrictions, SAs should consult DHS Directive 215-01, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes, dated November 6, 2013, or as updated, and DHS Instruction 215-01-001, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes, dated November 7, 2013, or as updated. SAs should contact OPLA for assistance with disclosure issues, as appropriate.



initiation of an investigation that qualifies for SCR submission. CTS will also ensure that proper guidance is provided to relevant parties regarding the existence of classified information and processes relative to procuring/disclosing any such information. Often, JTTF investigative information is classified at the originator controlled (ORCON) level and/or at a level that precludes sharing classified information outside the JTTF. HSI SAs will not disclose this type of information without prior FBI approval. HSI SAs who are not assigned to the JTTF but have a need to know certain JTTF investigative information may either work through an HSI SA assigned to the JTTF who will coordinate with the HSI SA's FBI supervisor, or through CTS which has access to this information via its placement in the FBI's CTD.

## 9.22 Visa Security Program

The HSI Visa Security Program (VSP) was designed to close the security gap that led to the 9/11 terrorist attacks. Congress, through section 428(e) of the Homeland Security Act of 2002 (6 U.S.C. § 236(e)), authorizes DHS to deploy personnel (delegated to the ICE HSI VSP) to diplomatic posts to perform visa security activities and to provide advice and training to DOS consular affairs. Through VSP, HSI SAs are deployed overseas to identify individuals linked to terrorism and other transnational crime, and to provide law enforcement expertise and recommendations to DOS regarding the issuance of visas for travel to the United States. VSP represents DHS's front line in protecting the United States against terrorists and criminal organizations by preventing foreign nationals who pose a threat to national security from entering the United States.



VSP can assist CT investigations by:

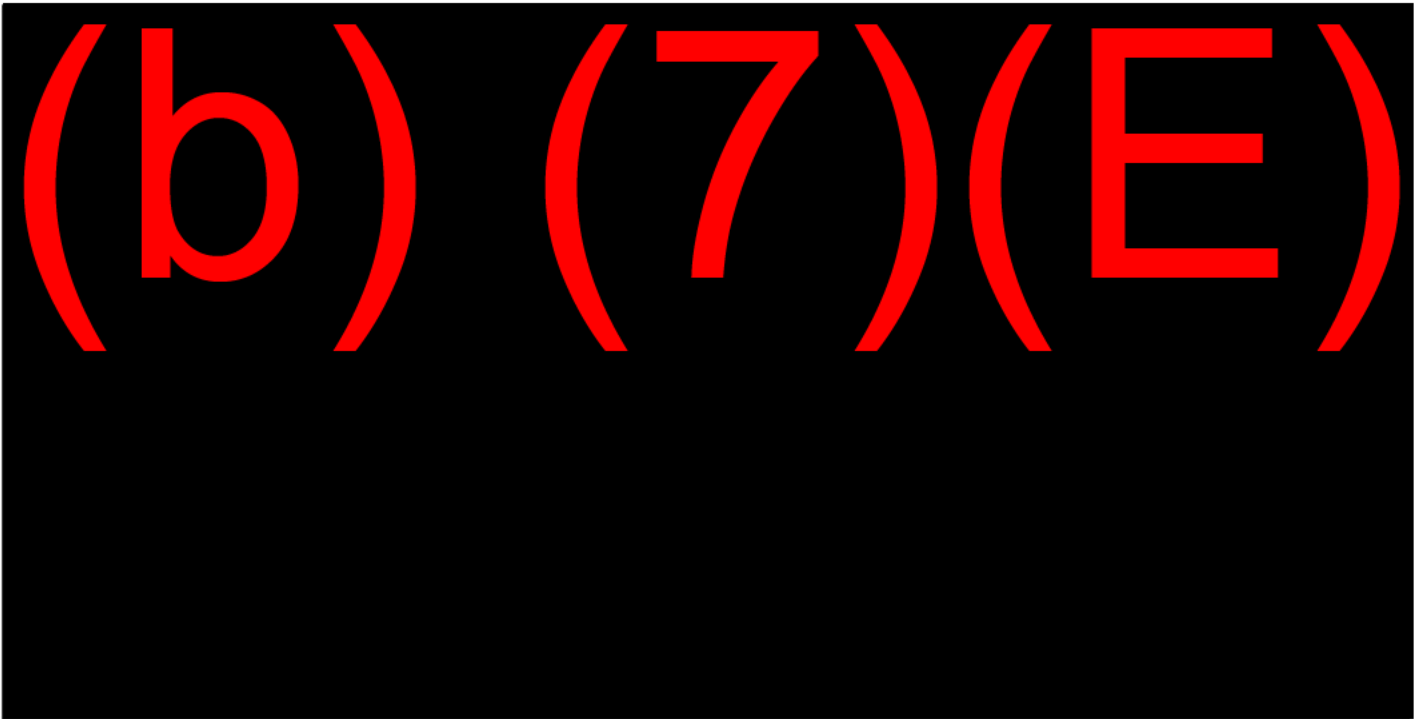


### 9.23 CBP Tactical Terrorism Response Teams

In 2015, the CBP NTC created field-based Tactical Terrorism Response Teams (TTRTs) comprised of CBP officers specializing in CT response, analytics, task force operations, and enforcement operations. TTRT officers serve as the main points of contact (POCs) in the field between the POE and other agencies engaged in national security-related operations, specifically HSI and the local JTTF. CBP officers assigned to TTRT undergo additional training related to the CT mission and hold an appropriate security clearance.

HSI SAs are encouraged to contact their local CBP JTTF representative for coordination with TTRT in furtherance of any national security CT investigations.

TTRT officers can assist JTTF SAs with:



### 9.24 Oversight of ICE Personnel Serving on Federal Investigative Task Forces

Participation on the JTTF falls under ICE Directive 10086.1, Oversight of ICE Personnel Serving on Federal Investigative Task Forces, dated March 25, 2016, or as updated, as specified below:

HSI and ERO cooperate and collaborate in their respective and complementary law enforcement missions. All HSI Special Agents in Charge (SACs) and ERO Field Office Directors (FODs) must regularly communicate to ensure awareness of related enforcement efforts and eliminate redundancies. To ensure efficiency

and proper operational coordination, HSI will have oversight of all ICE personnel assigned to federal task forces, other than U.S. Marshals Service Fugitive Task Forces, as described in this Directive. (See Section 2.)

Homeland Security Investigations, ..., is responsible for overseeing ERO officers serving on federal investigative task forces, other than U.S. Marshals Service Fugitive Task Forces, only to the extent [that] the ERO officers' involvement in the task forces is related to fugitive investigations. (See Section 4.1.)

ERO task force officers, excluding those serving [on] U.S. Marshals Service Fugitive Task Forces, will conduct the following actions under the guidance and supervision of HSI group supervisors: operational activities and preparing and submitting operational reports. This oversight is for purposes of operational and investigative supervision and coordination only; HSI group supervisors will not provide performance ratings or otherwise formally supervise any ERO officers. ERO TFOs will document all investigative activity and statistics into the Investigative Case Management System. (See Section 5.)

## **Chapter 10. DEPARTMENT OF STATE COUNTERTERRORISM OFFICE**

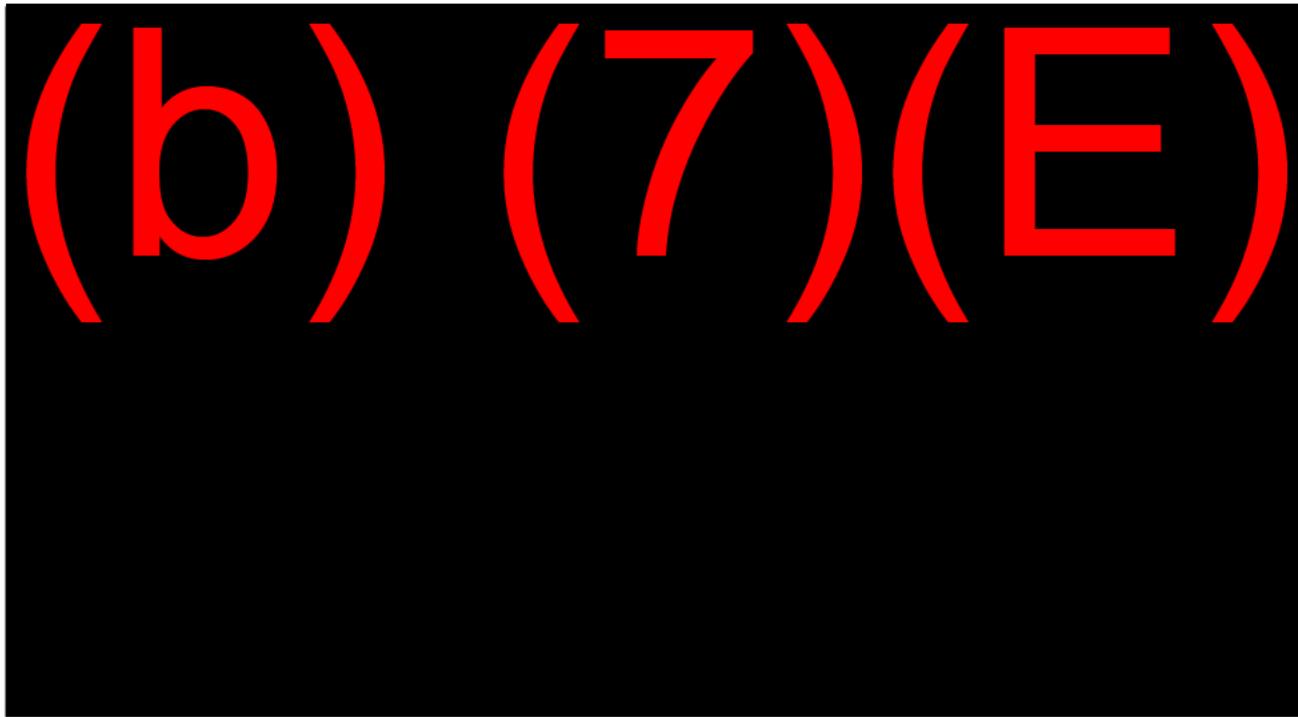
As provided in INA § 219, DOS maintains a list of designated FTOs, including other names by which these FTOs are known. According to the DOS Bureau of Counterterrorism, organizations that have been designated FTOs are listed at <https://www.state.gov/foreign-terrorist-organizations/>.

### **10.1 Identification and Designation of Foreign Terrorist Organizations**

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

### **10.2 Department of State Procedures for Designating a Group as a Foreign Terrorist Organization**

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



### 10.3 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 designations of an FTO:

- A. It must be a *foreign organization*; and
- B. The organization must *engage in terrorist activity*, as defined in INA § 212 (a)(3)(B) [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.

### 10.4 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.”

The INA provides terrorism-related inadmissibility grounds (TRIG) including, but not limited to, noncitizens who have engaged in terrorist activity on behalf of a designated FTO, are current representatives or members of a designated FTO, or have received military-type training from or on behalf of a designated FTO. *See* INA § 212(a)(3)(B)(i); INA § 237(a)(4)(B).<sup>5</sup>

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 OPLA with any questions as to whether the particular conduct of an individual constitutes “material support,” as well as to whether a group constitutes a designated FTO or an undesignated terrorist organization as defined in the INA.

### **10.5 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; and
- D. Signals U.S. concerns about the designated organization to other governments.



<sup>5</sup> It should also be noted that, under the INA, a “terrorist organization” is defined more broadly to include undesignated terrorist organizations in addition to FTOs designated by DOS. *See* INA § 212(a)(3)(B)(vi) (“terrorist organization” defined). OPLA is available for consultation as needed on the complex area of case law pertaining to undesignated terrorist organizations as defined in the INA.

(b) (7) (E)

(b) (7) (E)

## Chapter 11. IMMIGRATION AND NATIONALITY ACT

### 11.1 Evidence to Be Considered for Security-Related Administrative Removal Grounds

For cases with a national security nexus, SAs must look for evidence that will support removal pursuant to INA §§ 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.

SAs should also keep in mind whether the evidence pertains to a matter of inadmissibility or a matter of removability, because inadmissibility and removability carry different burdens of proof. First, noncitizens who have not been admitted to the United States may be subject to grounds of inadmissibility under INA § 212(a)(3) if they cannot show that they are “clearly and

beyond doubt entitled to be admitted and [are] not inadmissible.”<sup>6</sup> Second, noncitizens who have been admitted to the United States may be subject to grounds of removability under INA § 237(a)(4) if DHS shows by “clear and convincing” evidence that the noncitizens are deportable.<sup>7</sup>

The security-related grounds of inadmissibility under INA § 212(a)(3)(A) are forward-looking in that the statutory language is specific to the intent of the noncitizen “seeking to enter” the United States. According to INA § 212(a)(3)(A), any noncitizen who a consular officer or the Attorney General knows, or has reasonable ground to believe, that the noncitizen seeks to enter the United States to engage solely, principally, or incidentally in the following activities is inadmissible:

- A. Any activity (I) to violate any law of the United States relating to espionage or sabotage or (II) to violate or evade any law prohibiting the export from the United States of goods, technology, or sensitive information;
- B. Any other unlawful activity; or
- C. Any activity, a purpose of which is the opposition to, or the control or overthrow of, the Government of the United States by force, violence, or other unlawful means.

While the language providing for removability under INA § 237(a)(4)(A) is similar, it also encompasses a noncitizen’s past conduct (as opposed to the language of INA § 212(a)(3)(A) that focuses on future conduct). Under INA § 237(a)(4)(A), any noncitizen 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 criminal activity which endangers public safety or national security, or
- C. Any activity a purpose of which is the opposition to, or the control or overthrow of, the Government of the United States by force, violence, or other unlawful means.

Further, according to INA § 212(a)(3)(B) or INA § 237(a)(4)(B),<sup>8</sup> a noncitizen is inadmissible and/or removable if the noncitizen:

- A. Has engaged in a terrorist activity;<sup>9</sup>

---

<sup>6</sup> INA § 240(c)(2)(A).

<sup>7</sup> INA § 240(c)(3)(A).

<sup>8</sup> INA § 237(a)(4)(B) refers to aliens described in INA § 212(a)(3)(B) or (F).

<sup>9</sup> See INA § 212(a)(3)(B) for a complete definition. The term “terrorist activity” means any activity which is unlawful under the laws of the place where it is committed (or which, if it had been committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the acts described in INA § 212(a)(3)(B)(iii). The term “engage in terrorist activity” includes, in an individual capacity or as a member of an organization, engaging in any activity described in INA § 212(a)(3)(B)(iv).



- B. A consular officer, the Attorney General, or the Secretary of Homeland Security knows, or has reasonable ground to believe, that the noncitizen is engaged in or is likely to engage after entry in any terrorist activity;
- C. Has, under circumstances indicating an intention to cause death or serious bodily harm, incited terrorist activity;
  - 1) Is a current representative<sup>10</sup> of a terrorist organization;<sup>11</sup> or
  - 2) a political, social, or other group that endorses or espouses terrorist activity;
- D. Is a current member of a terrorist organization, unless the noncitizen can demonstrate by clear and convincing evidence that the noncitizen did not know, and should not reasonably have known, that the organization was a terrorist organization;
- E. Endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization;
- F. Has received military-type training (as defined in 18 U.S.C. § 2339D(c)(1)) from or on behalf of any organization that, at the time the training was received, was a terrorist organization; or
- G. Is the spouse or child of a noncitizen who is inadmissible under this subparagraph, if the activity causing the noncitizen to be found inadmissible occurred within the previous five years.<sup>12</sup>

Examples of evidence in cases include:

- A. A criminal conviction pursuant to a terrorism or other national security-related criminal charge;
- B. The subjects' admission under oath that they have committed acts that place them within the specified grounds for removal;
- C. Witnesses who can attest to the subject's relationship to a terrorist organization;
- D. Witnesses who can identify the subject under oath and who are willing to testify at a formal hearing regarding the subject's involvement with the organization; and

---

<sup>10</sup> 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. INA § 212(a)(3)(B)(v).

<sup>11</sup> See INA § 212(a)(3)(B)(vi) for the definition of a "terrorist organization."

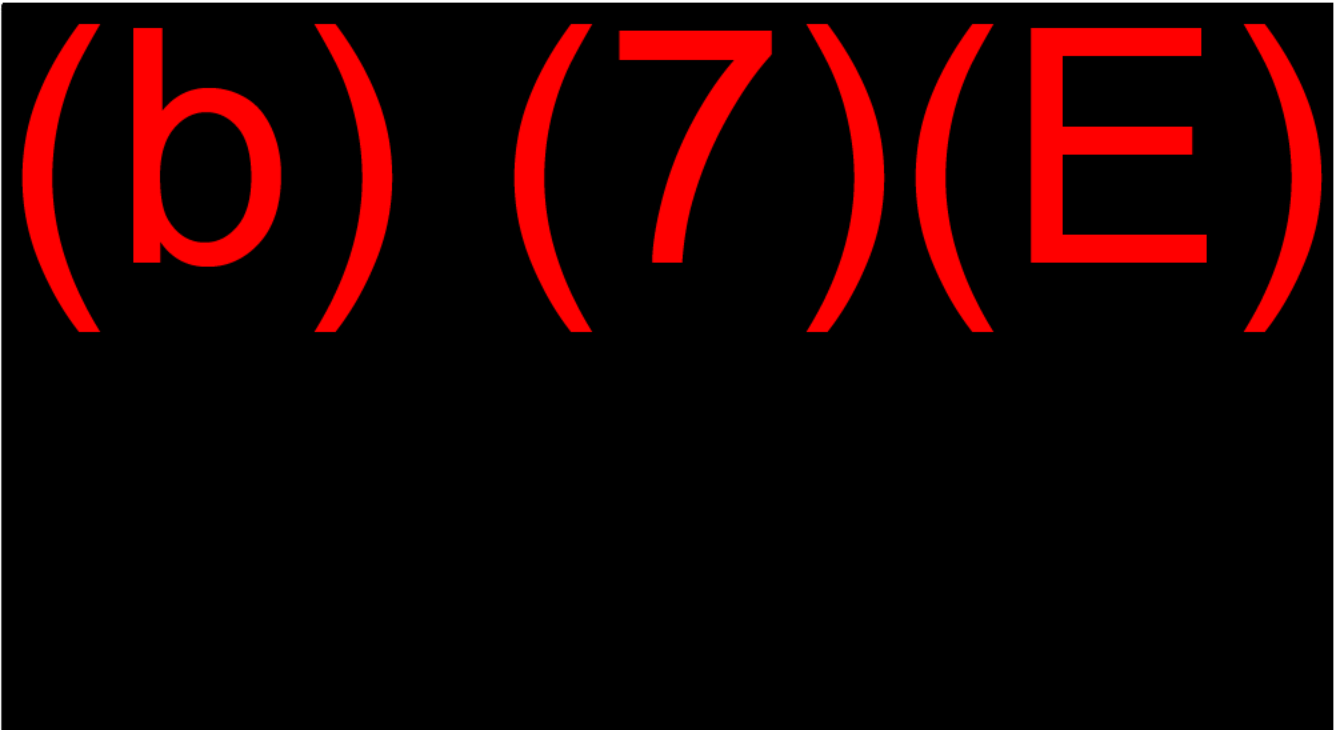
<sup>12</sup> See INA § 212(a)(3)(B)(ii) (explaining additional exceptions to the ground of inadmissibility/removability related to spouses or children of terrorist aliens).

- E. Documentary evidence of a subject’s involvement in terrorism or other conduct that threatens national security.

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.

In addition to lodging security-related grounds of inadmissibility and removability under INA §§ 212(a)(3) and 237(a)(4), respectively, on an NTA, a noncitizen “described in” these grounds may be barred from certain forms of relief regardless of the charges on the NTA. There are mandatory exceptions to certain forms of relief, such as asylum and withholding of removal, for noncitizens “described in” certain grounds of inadmissibility and removability under INA §§ 212(a)(3)(B) and 237(a)(4)(B).<sup>13</sup> The standard of proof for raising a bar to relief, as opposed to lodging a charge of inadmissibility/removability on an NTA, is much lower in that a bar may be raised if the “evidence indicates” that one or more of the mandatory bars to relief may apply.<sup>14</sup>

### 11.2 Classified National Security Information/Evidence in Administrative Immigration Proceedings



<sup>13</sup> See INA § 208(b)(2)(A)(v) (statutory exceptions to asylum for aliens described in terrorism-related grounds of inadmissibility or removability, INA §§ 212(a)(3)(B) and 237(a)(4)(B)); INA § 241(b)(3)(iv) (statutory exceptions for withholding of removal under the INA for aliens described in terrorism-related grounds).

<sup>14</sup> 8 C.F.R. § 1240.8(d).



(b) (7) (E)

### 11.3 Evidence to Be Considered for Administrative Removal Proceedings

ICE may request to use FBI-owned derogatory information as evidence in administrative removal proceedings against a noncitizen who is the subject of a JTTF investigation. Typically, the FBI will provide the declassified derogatory information in the form of an LHM with explicit authority for ICE to use the LHM in administrative removal proceedings.

ICE OPLA attorneys use FBI LHMs to support arguments regarding a noncitizen's custody status and removability before an IJ. Often, when an FBI LHM provides detailed derogatory information regarding noncitizens who are of JTTF interest, OPLA is able to sufficiently argue that the noncitizens should remain detained in ICE custody pending their removal proceedings because they are a danger to the community. In some instances, an FBI LHM may provide sufficient evidence for OPLA to raise a national security bar to relief, or lodge a national security

<sup>17</sup> *Id.* at 4-7 (outlining the review and recommendation process for the use of classified information).

charge of removal, in a noncitizen's removal proceedings. In most cases, FBI LHMs served as extremely valuable evidence in accomplishing ICE's mission to successfully detain and remove noncitizens believed to pose a threat to U.S. national security.

The FBI's ITOS or local JTTF offices may prepare the LHM for ICE in administrative removal proceedings. During the drafting process, HSI CTS and OPLA HQ should be consulted on the contents of the LHM to ensure that the LHM will be sufficient for immigration proceedings. FBI LHMs, whether produced in the field or at HQ, must be elevated to the FBI ITOS and the FBI National Security and Cyber Law Branch (NSCLB) and OPLA HQ for approval.

## **Chapter 12. FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) AND THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC)**

This Chapter provides a brief overview of the FISA for SAs conducting investigations who encounter information that is not generally encountered in traditional HSI criminal or administrative investigations.

Signed into law in 1978, FISA, codified at 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.

### **12.1 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. (*See* 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. (*See* 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/or 4) knowingly enters the United States or otherwise uses a false or fraudulent identity for or on behalf of a foreign power. (See 50 U.S.C. § 1801(b)(2).)

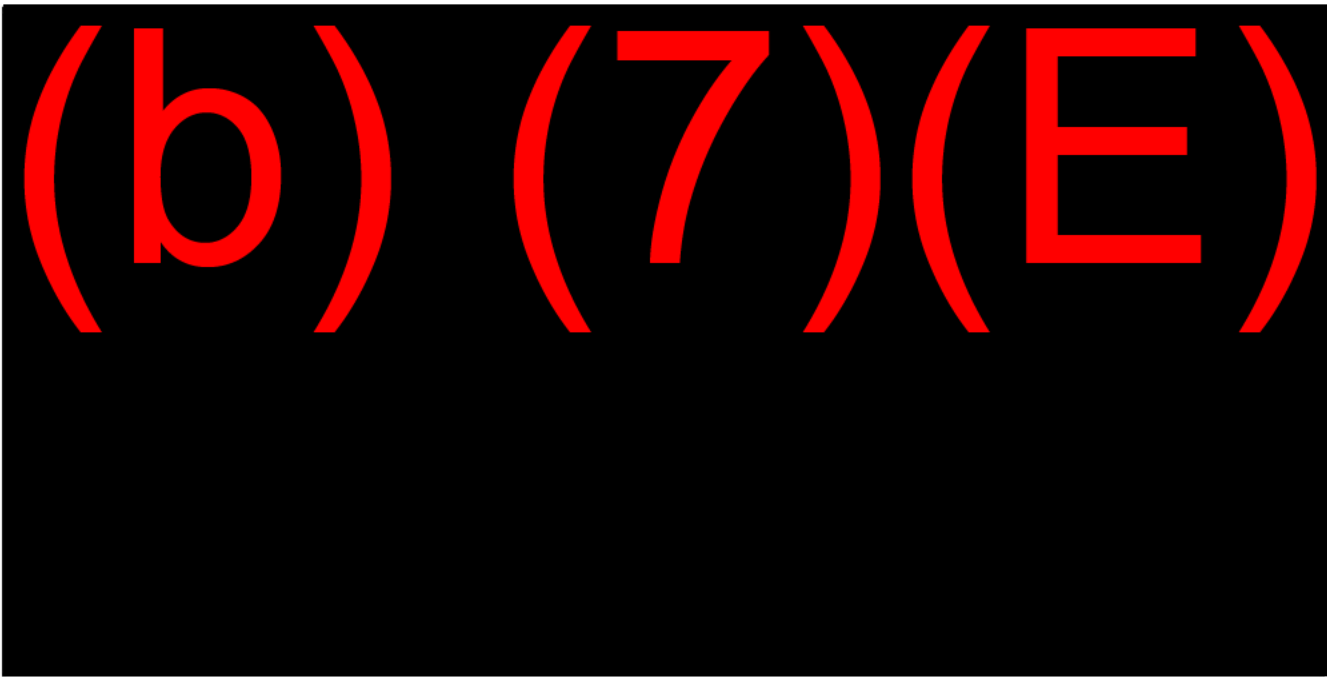
Under the statute, a “U.S. person” refers to a U.S. citizen or a noncitizen lawfully admitted for permanent residence as defined in INA § 101(a)(20) (LPR or conditional resident noncitizen).

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 an agent of a foreign power. FII under FISA also consists of 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.

## 12.2 U.S. Foreign Intelligence Surveillance Court

FISA authorized the creation of the 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. (See 50 U.S.C. §§ 1803, 1822(c).)

## 12.3 (b) (7)(E)



## 12.4 Minimization Procedures



(b) (7) (E)

## 12.5 Uses of Foreign Intelligence Information

Sections 1806(a) and 1825(a) of Title 50 mandate that information collected under a FISA warrant regarding 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. (*See* 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 acquired information and any information derived from such information may be used only in a criminal proceeding with the advance authorization of the AG. (*See* 50 U.S.C. § 1806(b).)

## 12.6 FISA Authority vs. Court-Overseen Criminal Investigatory Surveillance Techniques

(b) (7) (E)

## **12.7 FISA, Counterintelligence, and Law Enforcement**

Before September 11, 2001, DOJ restricted access to intelligence and counterintelligence developed by the FBI. Law enforcement agencies, including those focused on CT 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.

## **12.8 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. (*See* 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. (*See* 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. (*See* 50 U.S.C. §§ 1805(a)(3)(A), 1842(a)(1), 1961(a)(1).)

## **12.9 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.

## **12.10 Emergency FISA Applications**

In the case of an 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.

### **12.11 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. (See 50 U.S.C. § 1801(b)(1)(C).)

## **Chapter 13. BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC DEVICES**

### **13.1 Background**

HSI has 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 generally 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).) As a constitutional matter, border search authority is premised, in part, on a reduced expectation of privacy associated with international travel. (See *United States v. Flores-Montano*, 541 U.S. 149, 154 (2004).)

Following decisions by the Supreme Court and the U.S. Courts of Appeal, HSI distinguishes between *advanced* border searches of electronic devices and other, routine border searches of electronic media. An *advanced* border search of an electronic device is any border search in which external equipment is connected to an electronic device to review, copy, and/or analyze its contents. SAs must have reasonable suspicion before conducting an advanced border search of an electronic device. Other searches, such as searching documents or non-advanced border searches of electronic devices, remain routine border searches that require no level of suspicion.

“Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant.” (See *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).) Additionally, HSI maintains authority to conduct border searches of not only persons and merchandise entering the United States, but also of persons and merchandise exiting the country. (See *United States v. Odutayo*, 406 F.3d 386,



391-92 (5th Cir. 2005); *United States v. Bournelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983.)

### 13.2 Authorities and Policies

Pursuant to Customs border search authorities, contained in Title 19 of the United States Code, HSI may stop and search 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 noncitizens 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 the person’s possession when there is reasonable cause to suspect a basis for denying admission to the United States.

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 31, 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 with certain exceptions.). ICE Directive 10044.1 was modified by a Legal Update – Border Search of Electronic Devices, broadcast by the Assistant Director of Domestic Operations on May 11, 2018, which requires reasonable suspicion for advanced searches of electronic devices. Additional guidance in effect as of the date of issuance of this Handbook includes the 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, as well as the OI memorandum, Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media, dated December 12, 2008, or as updated.

### 13.3 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 HSI as Customs Officers (e.g., TFOs) and persons whose assistance to ICE is demanded under 19 U.S.C. § 507. (b) (7)(E)

[REDACTED]

### 13.4 Chain of Custody

Whenever HSI detains documents or electronic devices, or copies thereof, the detaining SA must initiate a chain of custody form (DHS Form 6051D, Detention Notice and Custody Receipt for Detained Property) or other appropriate documentation. 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 (Note: As stated earlier, ICE Directive 7-6.0 was superseded by ICE Directive 10044.1 (former number: 7-6.1) only as it relates to electronic devices with certain exceptions.); 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 prepare a DHS Form 6051S, Custody Receipt for Seized Property and Evidence, and enter the seizure into ICM via the completion of a (b) (7)(E) Incident Report. (Note: For more guidance on the handling and seizing of evidence, see the HSI Evidence Handbook (HSI HB 15-05), dated November 9, 2015, or as updated, and the HSI Computer Forensics Handbook (HSI HB 20-03), dated June 12, 2020, or as updated.)

### 13.5 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. Pursuant to 19 U.S.C. § 507, SAs may demand assistance from any person when necessary to effect an arrest, search, or seizure, including border searches. Assistance may be 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. The person providing assistance, however, has no independent authority to perform border searches.

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.

SAs are encouraged to contact NSU and/or their respective local OPLA embedded attorney should any questions arise regarding demands for assistance. C3 should be contacted for technical support, such as decryption, before seeking assistance outside of ICE. Additionally, NSU can provide SAs with technical and subject matter expertise upon request. (Note: 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 CTS PM for additional guidance.

### 13.6 Information Sharing

Border searches may not be conducted on behalf of a third agency. Electronic media obtained through ICE border search authority must be searched by an HSI SA or another properly authorized officer who meets the definition of “customs officer” under 19 U.S.C. § 1401(i). SAs should ensure that partner agencies are knowledgeable about ICE’s border search authority and remain up to date on current border search policy. SAs are encouraged to consult CTS and their respective local OPLA embedded attorney for more detailed information regarding when and how information sharing with law enforcement and intelligence authorities is appropriate.

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 31, 2009, or as updated. (Note: As stated earlier, ICE Directive 7-6.0 was superseded by ICE Directive 10044.1 (former number: 7-6.1) only as it relates to electronic devices with certain exceptions.). Also *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, as well as OI memorandum, Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media, dated December 12, 2008, or as updated.<sup>18</sup>

## Chapter 14. HSI RESPONSE PROTOCOL FOLLOWING DESIGNATED NATIONAL SECURITY EVENT

(b) (7) (E)

(b) (7) (E)

(b) (7) (E)

## Chapter 15. GUIDANCE FOR COMMON FIELD ISSUES

### 15.1 JTTF Reduction in Staffing Requests

The FBI National JTTF has defined the criteria for full-time, part-time, and liaison JTTF membership (*see* Appendix B, Joint Terrorism Task Force Membership Designation Criteria). SAC offices are strongly encouraged to assign at least one full-time SA to their respective JTTF and have another cleared SA available if the primary SA is unavailable. Optimally, SAC offices should provide staffing on all JTTF IT squads within their respective JTTF. Additionally, it is

recommended that SAC offices maintain a list of appropriately cleared/trained SAs and managers who can be deployed to support HSI JTTF elements during an active threat stream or post-terrorist attack management environment.

If an HSI SAC office concludes that a reduction in JTTF staffing is appropriate, that office must submit a memorandum to the NSU Unit Chief justifying any proposed staffing reduction to the JTTFs before any such reduction can take effect. NSU will, through the NSD AD, seek approval of any staffing changes to the JTTF from the EAD of HSI prior to any of the requested staffing changes taking effect. A reduction includes removing SAs from serving on the JTTF, changing the status of SAs from full-time to part-time (and/or LNO), and from part-time to LNO.

## **15.2 MOUs and MOAs Pertaining to HSI Participation in the JTTF**

HSI adheres to the guidelines provided in 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, which govern ICE's participation in the JTTF.

The following MOAs are also relevant to HSI 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 the
- 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.

(Note: An updated MOU between ICE and the FBI for participation on the JTTFs is in development and, once approved and signed, will supersede the above-referenced U.S. Customs Service and Immigration and Naturalization Service MOUs with the FBI. Until an updated MOU between ICE and the FBI has been agreed upon, no HSI SA shall sign any local MOUs with the FBI related to ICE's participation on the JTTF. Should a request for the signing of an MOU by an HSI SA assigned to the JTTF be received, supervisors should immediately report it through their local chain of command and to CTS for coordination and concurrent response. Furthermore, HSI Delegation Order 10001.1, Authority to Sign Memoranda of Understanding and Memoranda of Agreement Within Homeland Security Investigations, dated June 3, 2011, or as updated, delegates the authority to sign MOUs and MOAs in field offices only to SACs, and only after review and concurrence by OPLA at HQ and review and approval by the EAD of HSI.

### 15.3 Deputation of HSI Special Agents Assigned to the JTTF

In certain instances, FBI JTTF managers seek to deputize SAs assigned to JTTFs. HSI SAs **do not need to be deputized** to enforce Title 18 of the U.S. Code or any other relevant federal violation of law and **will not be deputized pursuant to, or as a condition of, their participation on the JTTF**. (Extenuating circumstances may arise in the future where HSI SAs might be required to become deputized as a peace officer to enforce state and local laws; however, this is the only situation where consideration should be given to deputation, and only after full consultation with OPLA, NSU, and CTS shall this decision be made). (Note: For guidance on responding to state crimes, *see* HSI Directive 13-01, HSI Special Agents Responding to State Crimes, dated May 30, 2013, or as updated.)

HSI SAs' enforcement authorities are found in 19 U.S.C. § 1589a, Enforcement authority of customs officers, and INA § 287, Powers of immigration officers and employees, and mirror those of the FBI and other federal law enforcement agencies. The FBI does not possess authority to deputize or cross-designate HSI SAs with any authorities that HSI SAs do not already possess; therefore, accepting such deputation may serve to agree that HSI needs some additional authority where that is not the case.

As such, SAs should respectfully decline to accept deputation by the FBI and should not sign any form presented to them related to deputation. Should a request for FBI deputation of an HSI SA assigned to the JTTF be received, supervisors should immediately report it through the local chain of command and to CTS for coordination and concurrent response.

### 15.4 Polygraph Examination of HSI Special Agents Assigned to the JTTF

Pursuant to established OPLA guidance, ICE Directives, and DHS policy, SAs who are assigned to field office JTTFs, are not required to undergo counterintelligence polygraph relative to their participation in the JTTF and will not undergo FBI polygraph examinations as a condition of assignment to a JTTF. (See ICE memorandum, DHS Guidance Regarding Polygraph Examinations of ICE Officers Assigned to the FBI Joint Terrorism Task Forces, dated January 22, 2007, or as updated.) “Unless provided otherwise by law, the investigation of persons ... employed in the competitive service ... is the responsibility of OPM (U.S. Office of Personnel Management).” 5 C.F.R. § 736.201(a). Also, under Executive Order 10450, OPM is primarily responsible for conducting national security investigations of competitive service employees. Under 5 C.F.R. § 736.201(a) and Executive Order 10450, only OPM has the authority to review and approve agency polygraph policies governing competitive service employees. Without OPM approval to administer polygraphs, an agency may not use polygraphs to screen competitive service employees for security positions. (See Use of Polygraph Examinations in the Department of Justice, Department of Justice Office of Inspector General Report, page 8, dated September 2006.)

Unlike ICE, which is subject to competitive civil service rules and regulations, the FBI is in the excepted service. Excepted service agencies set their own qualification requirements and are not subject to the appointment, pay, and classification rules in Title 5, United States Code. As a

result, the FBI establishes its own personnel rules and does not require OPM approval for the polygraphs it requires of its employees. Absent OPM approval, ICE does not have the legal authority to require any of its employees to undergo a polygraph exam<sup>19</sup>.

While DHS employees are not required to undergo a counterintelligence polygraph examination for participation on the JTTF, DHS employees and contractors who request and/or volunteer for a detail or assignment at another agency's HQ facility that requires a polygraph to obtain facilities or computer access must successfully complete a voluntary counterintelligence polygraph examination and comply with this requirement to be eligible for the detail or assignment. Those who decline to take the examination may not access the facility requiring the examination as a condition of access. (*See* DHS memorandum, Counterintelligence Polygraph Requirement for Liberty Crossing Detailees, dated September 8, 2008, or as updated.)

Should a request for the counterintelligence polygraph of an HSI SA assigned to the JTTF be received, supervisors should immediately report it through their local chain of command and to CTS for coordination and concurrent response.

### **15.5 National Security Letters**

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

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

### **15.6 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 SA assigned to the local JTTF. This process enables HSI to ensure the integrity of the file control process and appropriately interpret the contents of a requested A-File and utilizes HSI's expertise to develop potential administrative and/or criminal violations. Immigration status checks that do not require a physical file review will continue to be vetted locally. SAC offices will enforce third-agency disclosure requirements when the FBI

---

<sup>19</sup> ICE has been authorized by OPM to conduct polygraph screening examinations in the pre-employment context for entry-level law enforcement applicants. *See* ICE Directive 17014.1, Polygraph Screening Examinations for Entry-Level Law Enforcement Applicants, dated June 29, 2018, or as updated.



requests a physical review of A-Files. SACs will designate a POC for their entire AOR, or multiple POCs, as needed, for DSAC, ASAC, and RAC offices.

### **15.7 Disclosure of Asylum or Refugee Related Information**

For further information related to the disclosure of asylum or refugee-related information, SAs should *see* DHS Directive 262-02, Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes, dated November 15, 2016, or as updated, and DHS Instruction 262-02-001, Disclosure of Asylum or Refugee Information for Counterterrorism and Intelligence Purposes, dated November 21, 2016, or as updated. For the purpose of this Section, asylum or refugee-related information includes information contained in or pertaining to asylum applications, credible fear determinations, reasonable fear determinations, and overseas refugee applications. It includes applications for protection from removal under the Convention Against Torture regulations, statutory withholding of removal, and asylee/refugee follow-to-join petitions (USCIS Form I-730, Refugee/Asylee Relative Petition). NSU always recommends that SAs coordinate with their local OPLA office or their CTS PM who can assist in identifying whether or not asylum or refugee-related information can be shared. Moreover, SAs are reminded that even when asylum or refugee-related information is properly disclosed, the fact of such disclosure still may be used by a noncitizen to attempt to raise a new, or bolster an existing, claim for asylum or refugee-related protection.

### **15.8 Disclosure of 8 U.S.C. § 1367 Information**

For further information related to the disclosure of information covered by 8 U.S.C. § 1367 (VAWA, T Visa, U Visa, Continued Presence), SAs should consult DHS Directive 215-01, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes, dated November 6, 2013, or as updated, and DHS Instruction 215-01-001, Disclosure of Section 1367 Information to National Security Officials for National Security Purposes, dated November 7, 2013, or as updated. NSU recommends that SAs coordinate with their local OPLA office and/or the ICE Office of Information Governance and Privacy who can assist in identifying whether or not 8 U.S.C. § 1367 information can be shared.

(b) (7) (E)

(b) (7) (E)

## JOINT TERRORISM TASK FORCE MEMBERSHIP DESIGNATION CRITERIA

- A. **Full-Time:** U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs) must meet all the following criteria to be considered full-time Joint Terrorism Task Force (JTTF) members/participants:
1. Maintain a Top Secret/Sensitive Compartmented Information (TS/SCI) security clearance;
  2. Have full Federal Bureau of Investigation (FBI) systems access (must have access to FBINET, FBI Intranet email, FBI case management systems, etc.);
  3. Maintain a case load or leads with the JTTF;
  4. Be assigned and report to a work area in a JTTF facility;
  5. Work at least 85% (greater than 34 hours per week) of their time conducting JTTF investigations, managing JTTF leads, and performing other JTTF assignments, or have an appropriate full-time schedule approved by the JTTF Supervisory Special Agent (SSA). There should be minimal exceptions where the SA is required to work an assignment within other disciplines at the Special Agent in Charge (SAC)/Deputy SAC/ASAC/RAC Office other than to complete administrative matters; and
  6. Participate in file review sessions with the JTTF SSA.
- B. **Part-Time:** SAs must meet all the following criteria to be considered part-time JTTF members/participants:
1. Maintain a TS/SCI clearance (or assigned to the JTTF and pending clearance);
  2. Have full FBI systems access (must have access to FBINET, FBI Intranet email, FBI case management systems, etc.);
  3. Maintain a case load or leads with the JTTF;
  4. Spend the majority of their time (greater than 16 hours per week) conducting investigations and providing support to HSI; however, the SA must also maintain a case load with the JTTF conducting JTTF investigations, managing JTTF leads, and performing other JTTF assignments;
  5. Are not solely on an on-call basis with the JTTF;

6. Work on JTTF matters a minimum of 16 hours per week in JTTF space (to be coordinated with the JTTF SSA), to complete work, attend meetings, and coordinate activities;
  7. Maintain workspace in the JTTF space, whether at their own desk or at a shared desk; and
  8. Participate in file review sessions with the JTTF SSA.
- C. **Liaison:** SAs cannot be considered full-time or part-time members/participants of the JTTF, and will be considered Liaisons if they:
1. Do not retain the appropriate security clearances and there is no intent on acquiring them;
  2. Are on an on-call basis or can be reached as needed via telephone;
  3. Are not active in the majority of JTTF functions (meetings, case coordination, etc.);
  4. Are not assigned to directly affect JTTF investigations, issues, or assignments but do follow up on ICE-related authorities, as appropriate;
  5. Work less than 16 hours per week on JTTF matters;
  6. Do not report to JTTF space for work; or
  7. Do not maintain a dedicated workspace in JTTF space.

(Note: Liaison contacts are considered Task Force Participants.)

- D. **Recommendation:** The Counterterrorism Sections (CTS) of the National Security Unit recommends that each field office with a JTTF in its area of responsibility maintain the permanent, **full-time assignment of an SA to its respective JTTF**. CTS also recommends the following:
1. Prospective JTTF SAs have TS/SCI access or that such access be forthcoming; and
  2. Each new JTTF SA has a 2-month transition period with the previous JTTF SA.
- E. **HSI Policy:** HSI memorandum with subject line, “Minimum Commitment and Requirements for Special Agent Assignments to the Joint Terrorism Task Forces,” dated June 27, 2019, or as updated, established a three-year minimum commitment for SAs assigned to the JTTF as well as the requirement that HSI SAs selected to be assigned to the JTTF must be General Schedule (GS)-1811-13 SAs at the time of their selection to the assignment.

## SUPERSEDED DOCUMENTS

The following policy documents are superseded by the Homeland Security Investigations (HSI) Counterterrorism Investigations Handbook:

### HSI Handbook

National Security Investigations Handbook, dated April 26, 2013.

### Memoranda issued by HSI or by the former Office of Investigations

- 1) HSI Domestic Field Office Reporting to NSD on a Designated National Security Event/ U.S. Based Terrorist Attack, dated December 8, 2017.

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

- 3) Policy and Procedures for Requesting Retroactive Revocation of Non-Immigrant Visas in Certain National Security Cases, dated May 15, 2014.
- 4) Superseding Field Guidance on the Proper Designation of National Security Investigations in TECS, dated January 5, 2011.
- 5) Creation of TECS Program **(b) (7)(E)** to Capture HSI Enforcement Actions Against Subjects in the Terrorist Screening Database, dated December 13, 2010.
- 6) Revision of Sub-Categories for **(b) (7)(E)** – Counterterrorism Investigations, dated April 24, 2007.
- 7) Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry, dated March 5, 2007.

## ACRONYMS

A-File	Alien File
AD	Assistant Director
ADIS	Arrival/Departure Information System
AES	Automated Export System
AFI	Analytical Framework for Intelligence
AG	Attorney General
AOR	Area of Responsibility
ARN	Alien Registration Number
ASAC	Assistant Special Agent in Charge
ATRC	Alien Terrorist Removal Court

(b) (7)(E)

(b) (7)(E)

C3	Cyber Crimes Center
CA	Criminal Analyst
CAT	Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment of Punishment
CBP	U.S. Customs and Border Protection
CCD	Consular Consolidated Database
CFA	Computer Forensics Agent
C.F.R.	Code of Federal Regulations
CIA	Central Intelligence Agency
CIKR	Critical Infrastructure and Key Resources
CITF	Counterintelligence Task Force
(b) (7)(E)	(b) (7)(E)
CLEAR	Consolidated Lead Evaluation and Reporting
CMIR	Currency and Monetary Instruments Report
COB	Country of Birth
COC	Country of Citizenship
CONUS	Continental United States
CPMS	Customer Profile Management System
CT	Counterterrorism
CTD	Counterterrorism Division
CTLD	Counter Threat Lead Development Unit
CTR	Currency Transaction Report
CTS	Counterterrorism Operations Section
DHS	Department of Homeland Security
DOB	Date of Birth
DOJ	Department of Justice
DOMEX	Document and Electronic Media Exploitation
DOS	Department of State

DSAC	Deputy Special Agent in Charge
DT	Domestic Terrorism
EAD	Executive Associate Director
(b) (7)(E)	(b) (7)(E)
EARM	ENFORCE Alien Removal Module
EDMS	Enterprise Document Management System
EID	Enforcement Integrated Database
ENFORCE	Enforcement Case Tracking System
ERO	Enforcement and Removal Operations
ESTA	Electronic System for Travel Authorization
FBI	Federal Bureau of Investigation
FI	Full Investigation
FII	Foreign Intelligence Information
FinCEN	Financial Crimes Enforcement Network
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FOD	Field Office Director
FOUO	For Official Use Only
FTO	Foreign Terrorist Organization
(b) (7)(E)	(b) (7)(E)
GS	Group Supervisor
HB	Handbook
HQ	Headquarters
HRVWCU	Human Rights Violators and War Crimes Unit
HSDN	Homeland Security Data Network
HSI	Homeland Security Investigations
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IC	Intelligence Community
ICE	U.S. Immigration and Customs Enforcement
ICM	Investigative Case Management
INA	Immigration and Nationality Act
IJ	Immigration Judge
IRTPA	Intelligence Reform and Terrorism Prevention Act
IT	International Terrorism
ITOS	International Terrorism Operations Section
JOC	Joint Operations Center
JTTF	Joint Terrorism Task Force
JVU	Joint Vetting Unit
JWICS	Joint Worldwide Intelligence Communications System
KST	Known or Suspected Terrorist
LHM	Letterhead Memorandum
LNO	Liaison Officer
LPR	Lawful Permanent Resident
M3	Multimedia Message Manager



MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPA	Management and Program Analyst
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NIV	Nonimmigrant Visa
NSA	National Security Agency
NSCLB	National Security and Cyber Law Branch
NSD	National Security Division
NSE	National Security Event
NSL	National Security Letter
NSP	National Security Program
NSU	National Security Unit
NTA	Notice to Appear
NTC	National Targeting Center
NUIN	National Unique Identification Number
OFAC	Office of Foreign Asset Controls
OI	Office of Investigations
OIG	Office of Inspector General
OPLA	Office of the Principal Legal Advisor
OPM	Office of Personnel Management
ORCON	Originator Controlled
PACER	Public Access to Court Electronic Records
PATRIOT	Pre-Adjudication Threat Recognition Intelligence Operations Team
PCQS	Person Centric Query System
PDD	Presidential Decision Directive
PI	Preliminary Investigation
PM	Program Manager
POC	Point of Contact
POE	Port of Entry
PWP	Performance Work Plan
RAC	Resident Agent in Charge
RFI	Request for Information
ROI	Report of Investigation
SA	Special Agent
SAC	Special Agent in Charge
SAR	Suspicious Activity Report
SCR	Significant Case Report
S/CT	Department of State Office of the Coordinator for Counterterrorism
(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)
SEN	Significant Event Notification
SEVIS	Student and Exchange Visitor Information System
SEVP	Student and Exchange Visitor Program
(b) (7)(E)	(b) (7)(E)
SIR	Significant Incident Report

SPEAR	Significant Prospective Enforcement Activity Report
SSA	Supervisory Special Agent
STS	Special Threats Section
TDY	Temporary Duty
(b) (7)(E)	(b) (7)(E)
TFO	Task Force Officer
TFOS	Terrorism Financing Operations Section
(b) (7)(E)	(b) (7)(E)
TOL	(b) (7)(E) Online
TPN	(b) (7)(E) Person Number
TPS	Temporary Protected Status
TRIG	Terrorism-Related Inadmissibility Grounds
TSA	Transportation Security Administration
(b) (7)(E)	(b) (7)(E)
(b) (7)(E) (b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)
TURK	Time Utilization Record Keeping
U.N.	United Nations
UPAX	Unified Passenger
U.S.	United States
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USAO	U.S. Attorney's Office
U.S.C.	U.S. Code
USCIS	U.S. Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VAWA	Violence Against Women Act
VSP	Visa Security Program
(b) (7)(E)	(b) (7)(E)
WMD	Weapons of Mass Destruction