



Homeland Security Investigations

Counterterrorism and Criminal Exploitation Investigations Handbook

HSI HB 14-07 / November 12, 2014



U.S. Immigration
and Customs
Enforcement

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

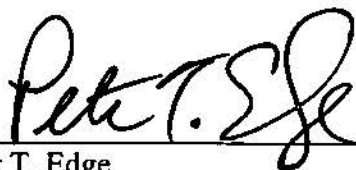
Foreword

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

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

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

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



Peter T. Edge
Executive Associate Director
Homeland Security Investigations

11/12/14
Date

COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS HANDBOOK

Table of Contents

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

- 3.32 Student and Exchange Visitor Program8
- 3.33 TECS.....8
- 3.34 Web-Based Commercial Databases8

Chapter 4. AUTHORITIES/REFERENCES8

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

Chapter 5. RESPONSIBILITIES15

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

Chapter 6. CTCEU PROGRAMS AND RELATED RESOURCES16

- 6.1 Student and Exchange Visitor Information System.....16
- 6.2 Overstay Data Sources and Biometric Services.....20
- 6.3 Automated Biometric Identification System22
- 6.4 International Criminal Police Organization22
- 6.5 Visa Revocation Program24
- 6.6 International Military Student Absent Without Leave Program25
- 6.7 Lost and Stolen Passport Program25
- 6.8 Alien Flight Student Program25
- 6.9 Visa Waiver Enforcement Program26
- 6.10 Targeted Enforcement Program.....27
- 6.11 DHS National Security Overstay Initiative.....27
- 6.12 SEVIS Recurrent Student Vetting Program.....27
- 6.13 Project Campus Sentinel27
- 6.14 National Security Entry-Exit Registration System28
- 6.15 Compliance Enforcement Advisory Panel.....29
- 6.16 (b)(7)(E)30
- 6.17 FBI Counterterrorism Division30
- 6.18 Foreign Terrorist Tracking Task Force.....30
- 6.19 National Counterterrorism Center.....30
- 6.20 (b)(7)(E)30
- 6.21 NCTC Pursuit Group31
- 6.22 Open Source Team.....31

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

- 7.1 Violator Identification.....31
- 7.2 Database Analysis32
- 7.3 School and Program Leads33
- 7.4 LeadTrac Database.....34
- 7.5 Investigative Lead Referral.....34
- 7.6 TECS Case Categories.....34
- 7.6.1 TECS Primary Program Codes35
- 7.6.2 TECS Secondary Program Codes35
- 7.7 Collateral Request Assignment.....36
- 7.8 Timely Assignment and Reporting Requirement36
- 7.9 Database Review.....36
- 7.10 Field Investigation and Interview37
- 7.11 Criminal and Administrative Charges39
- 7.12 Database Reporting/Management Notification.....40

Appendix

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

COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

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

Chapter 2. INTRODUCTION

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

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

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

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

Chapter 3. DEFINITIONS

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

3.1 Alien Change of Address Request Database

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

3.2 Alien Flight Student Program

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

3.3 Alternate Responsible Officer

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

3.4 Analytical Framework for Intelligence

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

3.5 Arrival Departure Information System

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

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

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

3.6 Automated Biometric Identification System

IDENT is the DHS biometric database. It collects biometric, biographic, and encounter-related data. Biometric data includes, but is not limited to, fingerprints and photographs. Biographical data includes, but is not limited to, name, date of birth, nationality, and other personal descriptive data.

3.7 Automated Targeting System-Passenger

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

3.8 Central Index System

The Central Index System (CIS) is a master records management system that displays biographical information on certain classes of aliens and certain U.S. citizens. CIS contains information on the status of an alien, as well as the physical location of the individual’s Alien File (A-file).

3.9 Computer Linked Automated Information Management System

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

3.10 Consular Consolidated Database

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

3.11 Deportable Alien Control System (Historical)

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

3.12 Designated School Official

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

3.13 DHS Pattern Information and Collaboration Sharing System

The DHS Pattern Information and Collaboration Sharing System (DPICS²) is a DHS search tool that allows DHS law enforcement users to conduct federated queries in data sets derived from multiple DHS law enforcement databases (TECS, SEVIS, the National Security Entry/Exit Registration System (NSEERS), ENFORCE, ADIS, the ICE Law Enforcement Support Center, and I-94 (Arrival-Departure Record)). It also allows users to conduct queries in law enforcement databases provided by other federal, state, and local law enforcement information sharing collaborations, including the Federal Bureau of Investigation (FBI) National Data Exchange system (FBI N-DEx), which may provide police record information ranging from traffic citations and booking information to departmental reports. Users receive hit information in the form of subject biographic information and photos or mug shots, if available. They also receive identifying record information from the source systems. DPICS² offers a visual linking tool and global relationship function that allow users to view information pertaining to subjects who are associated in the DHS source systems to the primary search subject.

3.14 Enforcement Case Tracking System (Historical)

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

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

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

3.15 Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement

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

3.16 ENFORCE Alien Removal Module

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

3.17 Enforcement Integrated Database

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

3.18 Fingerprint Identification Number

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

3.19 I-94 Subject Query in TECS

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

3.20 Intelligence Fusion System (Historical)

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

3.21 LeadTrac Database

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

3.22 National Security Entry-Exit Registration System

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

3.23 Office of Biometric Identity Management

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

3.24 Person Centric Query Service

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

3.25 Principal Designated School Official

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

3.26 Refugee, Asylum and Parole System

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

3.27 Responsible Officer

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

3.28 Secondary Inspection Tool

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

3.29 Significant Event Notification

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

3.30 Significant Incident Reports

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

3.31 Student and Exchange Visitor Information System

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

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

3.32 Student and Exchange Visitor Program

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

3.33 TECS

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

3.34 Web-Based Commercial Databases

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

Chapter 4. AUTHORITIES/REFERENCES

4.1 Authorities

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

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

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

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

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

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

C. Homeland Security Act of 2002

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

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

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

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

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

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

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

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

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

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

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

I. National Security Act of 1947, as amended

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

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

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

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

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

L. Executive Order (EO) 12333

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

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

M. EO 13231

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

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

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

N. EO 13354

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

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

O. EO 13388

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

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

P. 8 U.S.C. §§ 1103-1104

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

Q. 8 U.S.C. § 1202

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

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

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

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

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

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

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

U. 8 U.S.C. §§ 1365a-1365a note

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

V. 8 U.S.C. § 1365b

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

W. 8 U.S.C. § 1372

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

X. 8 U.S.C. § 1372(c)(2)

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

Y. 8 U.S.C. § 1379

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

Z. 19 U.S.C. § 1401(i)

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

AA. 19 U.S.C § 1589a

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

BB. 19 U.S.C. § 1595

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

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

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

DD. 8 C.F.R. § 208.6

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

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

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

FF. 8 C.F.R. § 214.2(f), (m), and (j)

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

GG. 8 C.F.R. § 214.3

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

HH. 8 C.F.R. § 214.3(g)

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

II. 8 C.F.R. § 214.4

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

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

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

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

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

4.2 References

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

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

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

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

5.2 Deputy Assistant Director, National Security Program Division

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

5.3 Unit Chief, Counterterrorism and Criminal Exploitation Unit

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

5.4 Special Agents in Charge and Attachés

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

5.5 Special Agents, Investigative Research Specialists, and Investigative Assistants

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

Chapter 6. CTCEU PROGRAMS AND RELATED RESOURCES

6.1 Student and Exchange Visitor Information System

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

(b)(7)(E)

(b)(7)(E)

A. Student and Exchange Visitor Program

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

B. Certification/Recertification of Schools

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

C. Decertification of Schools

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

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

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

D. Procedure for Obtaining Information from SEVP-Certified Schools

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

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

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

E. Contact with SEVP-Certified Institutions

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

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

F. Failure to Provide Information

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

G. Rejection of PDSO/DSO

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

H. Requests for Data and Other Information

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

(b)(7)(E)

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

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

I. Exchange Visitor Programs

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

6.2. Overstay Data Sources and Biometric Services

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

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

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

(b)(7)(E)

(b)(7)(E)

A. OBIM Biometric Watch List

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

(b)(7)(E)

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

(b)(7)(E)

(b)(7)(E)

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

B. OBIM Biometric Support Center

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

(b)(7)(E)

(b)(7)(E)

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

C. Biometric Exit

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

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

6.3 Automated Biometric Identification System

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

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

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

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

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

6.4 International Criminal Police Organization

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

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

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

(b)(7)(E)

(b)(7)(E)

Explanations of the most common notices encountered by HSI SAs, as provided by INTERPOL, are as follows:

A. Red Notices

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

B. Blue Notices

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

C. Green Notices

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

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

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

(b)(7)(E)

(b)(7)(E)

6.5 Visa Revocation Program

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

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

(b)(7)(E)

(b)(7)(E)

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

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

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

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

6.6 International Military Student Absent Without Leave Program

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

(b)(7)(E)

(b)(7)(E)

6.7 Lost and Stolen Passport Program

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

(b)(7)(E)

6.8 Alien Flight Student Program

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

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

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

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

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

6.9 Visa Waiver Enforcement Program

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

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

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

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

6.10 Targeted Enforcement Program

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

(b)(7)(E)

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

6.11 DHS National Security Overstay Initiative

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

6.12 SEVIS Recurrent Student Vetting Program

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

(b)(7)(E)

6.13 Project Campus Sentinel

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

(b)(7)(E)

(b)(7)(E)

6.14 National Security Entry-Exit Registration System

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

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

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

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

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

6.15 Compliance Enforcement Advisory Panel

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

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

(b)(7)(E)

6.17 FBI Counterterrorism Division

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

6.18 Foreign Terrorist Tracking Task Force

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

(b)(7)(E)

6.19 National Counterterrorism Center

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

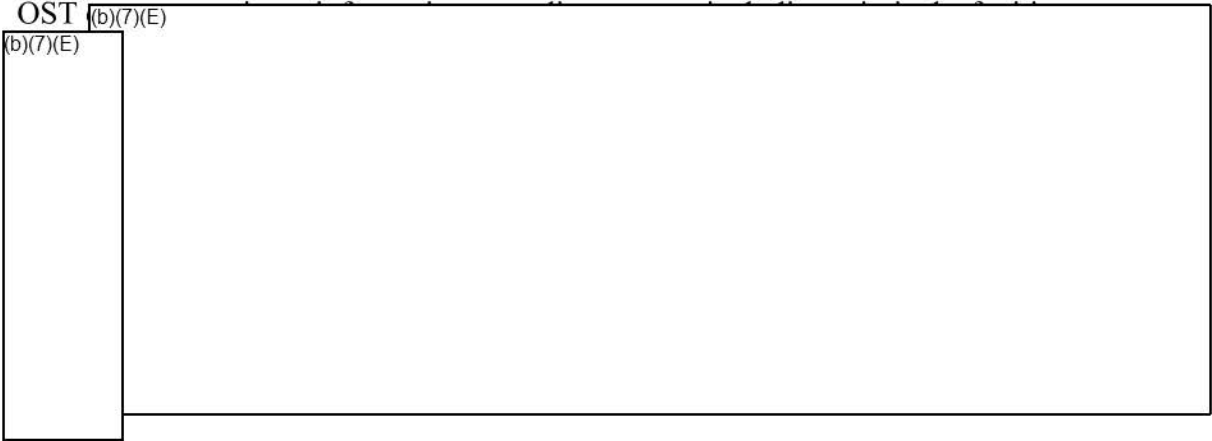
(b)(7)(E)

6.21 NCTC Pursuit Group

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

6.22 Open Source Team

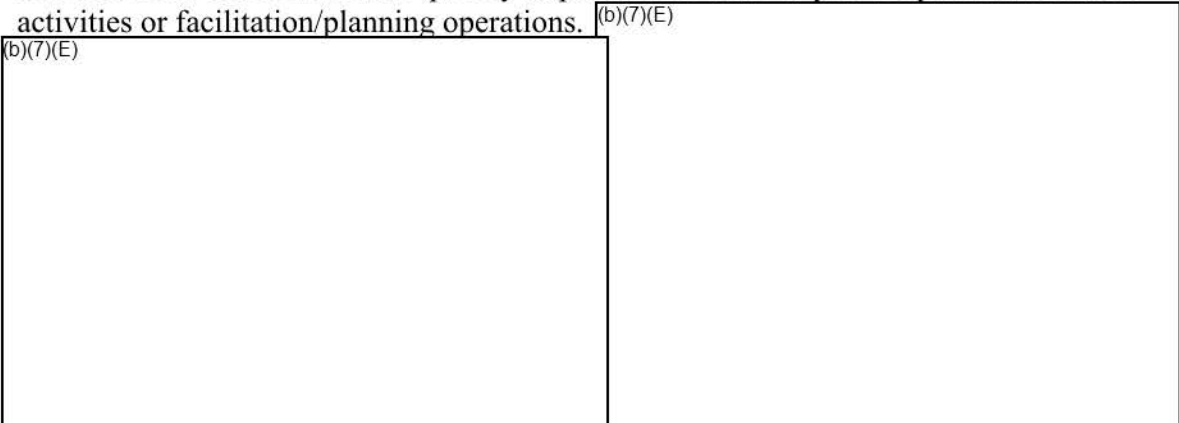
With the proliferation of openly available information through ever-changing internet technologies, CTCEU has created an Open Source Team (OST) to capture and analyze an expanding share of unclassified information available through various open sources. The OST



Chapter 7. COUNTERTERRORISM AND CRIMINAL EXPLOITATION INVESTIGATIONS

7.1 Violator Identification

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



A. System Leads

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

B. Specialized Leads

(b)(7)(E)

(b)(7)(E)

7.2 Database Analysis

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

(b)(7)(E)

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

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

7.3 School and Program Leads

CTCEU utilizes information from SEVIS, along with other analytical tools, to identify school and exchange visitor program anomalies. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

7.4 LeadTrac Database

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

7.5 Investigative Lead Referral

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

(b)(7)(E)

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

(b)(7)(E)

7.6 TECS Case Categories

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

(b)(7)(E)

(b)(7)(E)

7.6.1 TECS Primary Program Codes

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

(b)(7)(E)

7.6.2 TECS Secondary Program Codes

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

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

7.7 Collateral Request Assignment

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

(b)(7)(E)

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

(b)(7)(E)

7.8 Timely Assignment and Reporting Requirement

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

(b)(7)(E)

7.9 Database Review

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

(b)(7)(E)

7.10 Field Investigation and Interview

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

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

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

7.11 Criminal and Administrative Charges

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

A. Criminal Prosecution

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

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

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

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

B. Administrative Proceedings

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

7.12 Database Reporting/Management Notification

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

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

(b)(7)(E)

ACRONYMS

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

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

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