Note: Table of Contents page numbers are subject to change based on ongoing review and edits.

CASE MANAGEMENT HANDBOOK

Table of Contents

Note: Table of Contents page numbers are subject to change based on ongoing review and edits.

Note: Table of Contents page numbers are subject to change based on ongoing review and edits.

Note: Table of Contents page numbers are subject to change based on ongoing review and edits.

Note: Table of Contents page numbers are subject to change based on ongoing review and edits.

APPENDICES

Appendix B

ACRONYMS

AD	Assistant Director
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
AUO	Administratively Uncontrollable Overtime
CBP	U.S. Customs and Border Protection
DAD	Deputy Assistant Director
DAH	Designated Availability Hours
DFO	Director, Field Operations
DHS	Department of Homeland Security
DOD	Department of Defense
DSAC	Deputy Special Agent in Charge
EABM	Enforcement Apprehension and Booking Module
EAD	Executive Associate Director
EAGLE	Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement
EID	Enforcement Integrated Database
EIRS	Executive Information Reporting Section
ELSUR	Electronic Surveillance
ENFORCE	Enforcement Case Tracking System
FBI	Federal Bureau of Investigation
FD	Federal Document
FEP	Federal Employee Pay
FP&F	Fines, Penalties and Forfeitures
FYI	For Your Information
HB	Handbook
HRO	Headquarters Responsible Official
HSI	Homeland Security Investigations
IAFIS	Integrated Automated Fingerprint Identification System
ICE	U.S. Immigration and Customs Enforcement
ICM	Investigative Case Management
IDENT	Automated Biometric Identification System
JTTF	Joint Terrorism Task Force
LEAP	Law Enforcement Availability Pay
MOIR	Memorandum of Information Received
NCIC	National Crime Information Center
OCDETF	Enforcement Apprehension and Booking Module
OFO	Office of Field Operations
OI	Office of Investigations
ORI	Originating Agency
POE	Purchase of Evidence

POI	Purchase of Information
RAC	Resident Agent in Charge
ROI	Report of Investigation
SA	Special Agent
SAC	Special Agent in Charge
S/A/S	Search/Arrest/Seizure
SCO	System Control Officer
SEACATS	Seized Asset and Case Tracking System
SEN	Significant Event Notification
UOT	Uncontrollable Overtime
USAO	U.S. Attorney's Office
U.S.C.	United States Code

Prepared By: (b)(6);(b)(7)(C)
Email: (b)(6);(b)(7)(C)
Account Name: ICE

Created Date: 7/18/2012
Expiration Date: 8/31/2012
Contact Name: (b)(6);(b)(7

(b)(4)

(b)(4)

Maintenance

Palantir's Enterprise Operations and Maintenance (O&M) program includes: remote support, onsite support, training, rapid turnaround, simple data integration and configuration, analyst support, and program management. All of these are detailed in the section "Technical Support."

Under Enterprise O&M, onsite and remote engineering support is offered to integrate with third party products, enable interoperability, simple data integration tasks and simple helper development.

At the discretion of Palantir, additional support may be provided, as a part of the maintenance fees, which will not cause a deduction from any applicable yearly onsite support hours specifically included in applicable maintenance costs. This level of support shall be determined by Palantir.

Technical Support

Helpdesk Support

Technical issues can be submitted via email to (b)(7)(E) email address will be distributed widely by Palantir personnel during all group and deskside training interactions as the primary resource for resolving any and all issues in using Palantir to support users' work. Palantir personnel will staff a shared inbox between 9AM and 5PM EST. All requests to the helpdesk will be pursued until resolved or until the users chose to stop corresponding with the helpdesk. The helpdesk will also be used as a communication tool for disseminating relevant information to users on an ad hoc basis.

Onsite Support:

Under Enterprise O&M, the explicit level of guaranteed support is 30 hours per annum of onsite support per core. Our past deployment experience indicates that this is an adequate level of support given the relative complexity of larger deployments. Palantir requires onsite access to accomplish the included onsite support. To secure onsite support, the customer must coordinate with the Palantir deployment lead. Palantir will request the COR's approval for the personnel supporting this contract.

Training:

Palantir will provide training to ICE agents, special agents, group supervisors and any other employee involved in directly supporting active investigations. Training will be pursued on a strategic basis targeting only users with a clear, operational use for the Palantir system. Training schedules will give preference to locations where entire groups – agents, analysts and group supervisors – can be trained together, creating entire units capable of working together in Palantir to complete investigations. For this 6 month extension, there is no explicit training goal by user count.

Remote Support:

Palantir documentation, Palantir DevZone, and Palantir Labs are available without additional charge as long as Standard O&M is current.

(b)(6);(b)(7)(C)

Overview

DARTTS (Data Analysis and Research for Trade Transparency System) is a web-based system that tracks the import and export data between the United States and a variety of countries. Palantir was requested to provide an overall assessment of the requirements necessary to integrate the DARTTS database into Falcon.

Planned Capabilities

(b)(7)(E);(b)(4)

The Falcon Workspace enables detailed analysis of suspected targets

Hardware Requirements

- Up to 10 (ten) 16-core servers
- Palantir Phoenix on the backend to enable dynamic, multi property searches across billions of records

Tentative Schedule

(b)(5)

Palantir Torch is an example of our web visualization tools that allow an analyst to quickly identify trends and isolate discrepancies

Palantir

- Platform will be available for testing in a Production environment by Monday, September 30th, 2013

(b)(7)(E)

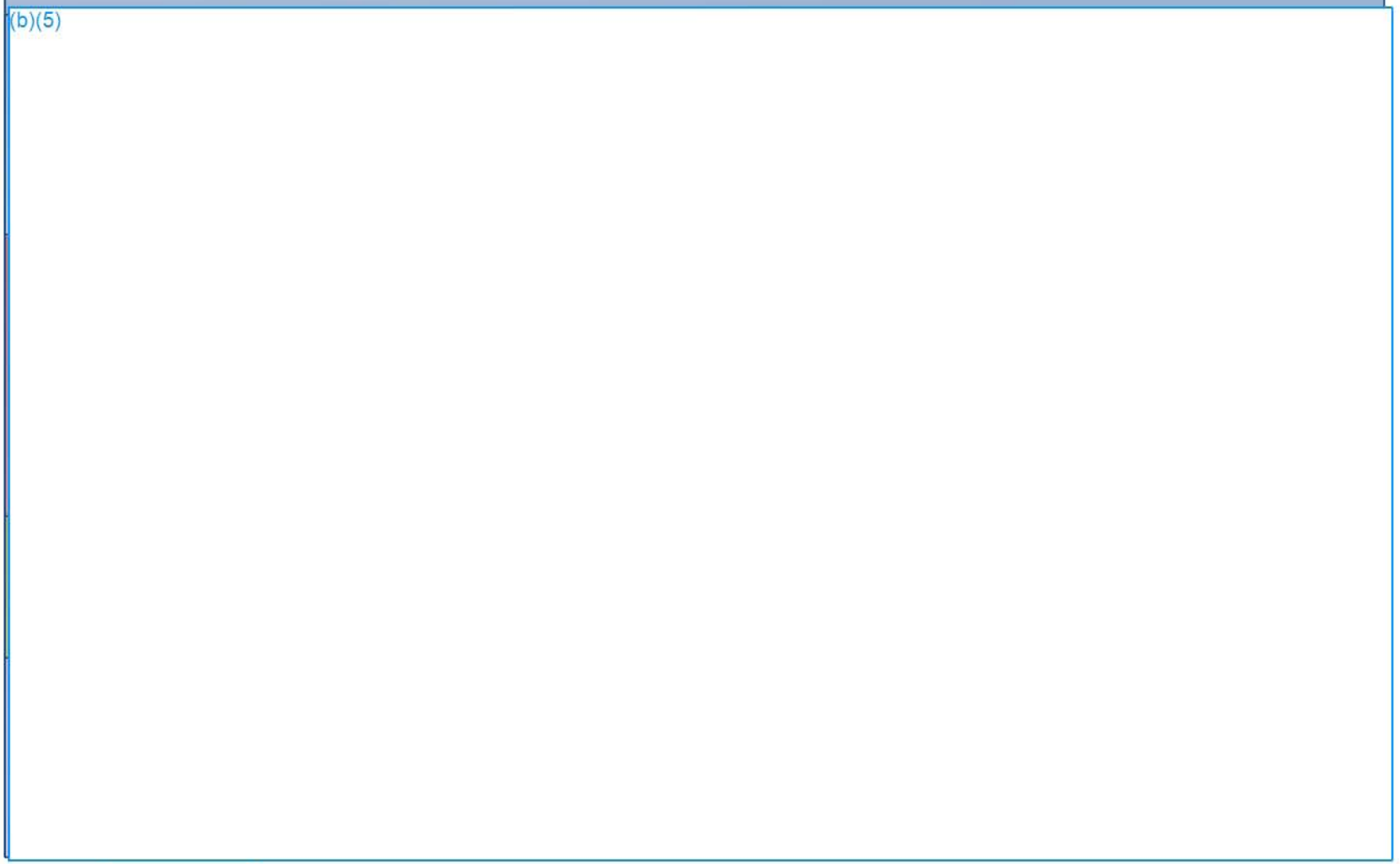
The Executive Dashboard can highlight recent incidents and top events in a region, or across the country

(b)(7)(E)

- System goes live to end users before December 31st, 2013

FALCON Tipline App

Draft HSI Tipline Workflow



Created by (b)(6);(b)(7)(C)
05/23/12

CASE MANAGEMENT HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The *Case Management Handbook* establishes the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) policies and responsibilities for the use of Case Management by HSI Special Agents (SAs), Task Force Officers (TFOs), and other HSI personnel.

HSI is the principal investigative arm of the U.S. Department of Homeland Security (DHS). The mission of HSI is to investigate, disrupt, and dismantle terrorist, transnational, and other criminal organizations that threaten or seek to exploit U.S. customs and immigration laws. Case Management is critical to the accurate and timely tracking of the investigations HSI conducts in support of its mission.

This Handbook outlines the policies by which HSI conducts Case Management activities and refers readers to the online *Investigative Case Management (ICM) User Portal* and *ICM User Manual*, both found on HSINet, and other documents as appropriate.

1.1 HSI Law Enforcement Systems

HSI uses various law enforcement systems in the execution of Case Management activities.

ICM (also referred to as "Case Management") is the Case Management system used to document HSI investigations. ICM organizes electronic case files and associated records and documents in a single accessible location. Authorized HSI personnel may enter, modify, and query Case Management information in ICM.

The ICM user menu is specifically tailored to a user's assigned role(s). The system authenticates users based on their unique network account credentials and does not require a separate password. Users must be connected to the ICE network to access the system.

Depending on their role, Case Management users have the ability to query and/or create subject records that reference persons, conveyances, businesses, addresses, or organizations. Every transaction a user performs is logged for audit purposes. Additionally, source documents, enforcement reports, and other data electronically stored in ICM are considered "Law Enforcement Sensitive" and must be treated as such.

The Seized Asset and Case Tracking System (SEACATS) is a system owned by U.S. Customs and Border Protection (CBP) that is used by HSI personnel to document all seizures of tangible property. SEACATS is not to be used to document arrests in which no property has been seized.

The Enforcement Integrated Database (EID) Arrest Graphical User Interface (GUI) for Law Enforcement, referred to as EAGLE, is an application used to document all arrests. (See HSI Directive 14-01 entitled, "Mandatory Booking of Arrestees Using EAGLE," dated April 23, 2014, or as updated). EAGLE works in conjunction with the Integrated Automated Fingerprint Identification System (IAFIS), which automates 10-print processing by enabling the electronic capture of 10-print fingerprints.

Falcon (not an acronym) is an application that provides search, analytical, geospatial, and situational awareness capabilities to enhance investigative and intelligence processes. FALCON enables HSI agents and analysts to import and model data; iteratively define and test hypotheses; and search and analyze volumes of information from multiple data sources to identify and visualize individuals and other subjects or records that are interrelated. Case data and data from other law enforcement systems are available in FALCON.

1.2 ICM User Portal and User Manual

The *Case Management Handbook* is not intended to be a User's Guide. The *ICM User Portal* and *ICM User Manual* describe in detail how to use the ICM application. In addition, ICM contains context sensitive "tooltips" which appear when performing operations in the system. HSI personnel should refer to the *ICM User Portal* and *ICM User Manual* when specific questions arise regarding Case Management. Additional sources of information regarding Case Management include HSI supervisors and local System Control Officers (SCOs). Case Management questions and issues can also be referred to the National SCO (NSCO) by submitting a ticket via the ICE Service Desk.

1.3 EAGLE User Guide

The EAGLE User Guide is located on HSINet. It describes in detail how to use EAGLE.

1.4 Executive and Management Information and Resource Allocation

Statistical information derived from Case Management supports the information needs of HSI senior executives by providing the data necessary to meet the strategic goals of the agency. In addition, Case Management provides investigative data and statistical information to other DHS components and outside entities, as well as internal and external stakeholders, as appropriate, for use as management tools, for agency and management oversight, for budget allocation, and for statistical analysis.

HSI managers use Case Management and statistical information for resource allocation purposes in order to make the most effective use of limited resources (e.g., personnel and equipment). HSI personnel in all job series and at all levels must be aware of the importance of Case Management statistics and how they are used.

1.5 Requests for Information

Frequently, HSI is required to respond to requests for information from a variety of organizations and individuals (e.g., Congressional committees, Executive Branch offices, the Government Accountability Office, the Office of Management and Budget, and offices within ICE). Case Management provides the information necessary to respond to many of these requests, therefore the detail and accuracy of the information is critical. All HSI law enforcement systems information must be treated as "Law Enforcement Sensitive."

Chapter 2. DEFINITIONS

The following definitions are provided for the purposes of this Handbook and are not intended to be all-inclusive. Some are provided for information only and may not be subsequently referenced in this Handbook.

2.1 Area of Responsibility

An area of responsibility (AOR) is a particular geographic region defined as the responsibility of a specific HSI office. An AOR encompasses the geographical area of responsibility overseen by the Special Agent in Charge (SAC) or Attaché.

2.2 Arrest

A person is arrested when probable cause exists to believe that he or she has committed a crime and is taken into custody. Arrests should not be confused with detentions for questioning or detentions for the continuation of border search authority. For Case Management purposes, arrests can be initial enforcement statistics.

2.2.1 Administrative Arrest

An administrative arrest is the arrest of an alien for administrative immigration charges. Administrative charges are normally adjudicated before an Immigration Administrative Law Judge. An administrative arrest may also be affected pursuant to the issuance of an administrative warrant or based on probable cause.

2.2.2 Criminal Arrest

A criminal arrest is the arrest of an individual for criminal charges which are further adjudicated before a U.S. District Court Judge; a U.S. Magistrate Judge; or a state or local court judge before whom the individual is arraigned and will face criminal charges. A criminal arrest may also be effected pursuant to the issuance of a criminal warrant or based on probable cause.

2.3 Asset Sharing (also known as Equitable Sharing)

Asset Sharing is the application for the sharing of forfeited proceeds and/or assets.

For additional information concerning asset sharing, refer to the Department of the Treasury, "Guide to Equitable Sharing for Foreign Countries and Federal, State, and Local Law Enforcement Agencies," dated April 2004, or as updated.

2.4 Border Search

In accordance with border search authority pursuant to Title 19, U.S. Code (U.S.C.) § 1582, ICE law enforcement personnel may conduct routine stops and searches of merchandise and persons at the U.S. border. The use of border search authority must be documented in Case Management.

2.5 Case Category

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 Case Management. A case category must be based on the predicate (primary) offense under investigation.

2.6 Case File

The case file refers to the electronic collection of all information that pertains to a case. This includes subject records, Reports of Investigation (ROIs), case reviews, as well as other documents, hours, statistics, and select media that are associated with the case. There is no requirement to print the information contained within the case file.

2.7 Case Status

The case status refers to the level of activity in an investigation. Investigations are "draft," "open," "pending," or "closed."

2.7.1 Case Status – Draft

A case that is in draft status has not yet been approved by a supervisor is considered unopened.

2.7.2 Case Status – Open

A case may be opened when information is developed which indicates that a violation of one or more laws enforced by HSI has occurred or will likely be committed by specific individuals, organizations, or businesses. In addition, cases are opened to assist other federal, state, local, or tribal agencies, or foreign governments in enforcing their laws and regulations. Cases can be opened for criminal and/or administrative purposes.

2.7.3 Case Status – Pending

A case is placed in a pending status when all appropriate investigative activities have been completed but there is still a judicial or administrative action pending completion. A case is also placed in pending status if the subject is a fugitive.

2.7.4 Case Status – Closed

A case is closed when all investigative leads have been exhausted, or the predicate offense has changed and a new case has opened under a new case category. A case will not be "closed" until all judicial and administrative proceedings, including property dispositions, have been resolved and properly reported in Case Management.

The case status is automatically changed to "closed" when the supervisor approves the closing ROI, the case statistics are finalized, and the supervisor has completed a case review. (Note: A case cannot be closed unless a minimum of 1 hour has been posted against the case and has been approved).

2.8 Co-Case Agent

A second case agent, or co-case agent, is often assigned in large, complex criminal investigations. For Case Management purposes, a co-case agent is documented in cases and receives proper statistical credit for his/her involvement in an investigation.

2.9 Collateral Investigation

Collateral investigations are investigations opened in one or more HSI offices based on investigative information provided by another HSI office where the investigation originated.

2.10 Consensual Intercepts

A consensual intercept is the electronic monitoring of private communications with the consent of at least one party to the conversation. Consensual intercepts do not require a court order. For Case Management purposes, consensual intercepts are case statistics and are documented via the Electronic Surveillance (ELSUR) report.

2.11 Conviction

A conviction is the final legal disposition of a defendant who has been found guilty. For Case Management purposes, convictions are final enforcement statistics.

2.12 Country Codes

Country codes refer to three-character country codes in Case Management. Country codes are added to Case Management records in an effort to identify the countries that may be involved in an ongoing investigation and to inform the appropriate HSI Attachés.

2.13 Court-Imposed Fines

Court-imposed fines are monetary penalties imposed by a criminal or civil court subsequent to a conviction on criminal or civil charges.

2.14 Dismissal

A dismissal is a final legal disposition of a defendant where prosecution has been terminated prior to a finding of guilt or innocence. For Case Management purposes, dismissals are final enforcement statistics.

2.15 EAGLE

The Enforcement Integrated Database (EID) Arrest Graphical User Interface (GUI) for Law Enforcement, referred to as EAGLE, is an application used to document all arrests. EAGLE works in conjunction with the Integrated Automated Fingerprint Identification System (IAFIS), which automates 10-print processing by enabling the electronic capture of 10-print fingerprints.

2.16 Electronic Device

An electronic device is any device capable of storing or processing data.

2.17 Electronic Evidence

Electronic evidence is probative information stored or transmitted in digital form that can be admissible as evidence in a court case.

2.18 Electronic Surveillance Authorization

An Electronic Surveillance (ELSUR) authorization is used to request authorizations, grant authorizations, and submit reports of use/non-use for consensual electronic surveillances.

2.19 FALCON

FALCON is an application that provides search, analytical, geospatial, and situational awareness capabilities to enhance investigative and intelligence processes. FALCON enables HSI case agents and analysts to import and model data; iteratively define and test hypotheses; and search and analyze volumes of information from multiple data sources to identify and visualize individuals and other subjects or records that are interrelated.

2.20 Forfeiture

Forfeiture results whenever the title of seized property is transferred to the U.S. Government either through a judicial or an administrative process. Forfeiture can be based on criminal, civil, or administrative statutory authorities. For Case Management purposes, forfeitures are final enforcement statistics.

2.21 Fugitive

A fugitive is a defendant who has been charged by an indictment, information, criminal complaint, and/or administrative warrant of deportation or removal, and is not yet in custody. A fugitive may also be a defendant who was in custody and who has absconded.

2.22 General Investigative Activity

General investigative activity is any activity that is not otherwise creditable against any specific investigation.

2.23 HSI-Sponsored Organized Crime Drug Enforcement Task Force Investigation

HSI-sponsored Organized Crime Drug Enforcement Task Force (OCDETF) investigations are those that have been presented to and approved by an OCDETF Core City Coordination Group based on a proposal that was either formally sponsored or co-sponsored by an HSI SA. For Case Management purposes, HSI-sponsored or co-sponsored OCDETF investigations are case statistics.

2.24 Indictment/Information

Indictments and informations are legal documents that charge suspects with violations of law. Indictments are issued by grand juries, whereas informations are issued by a U.S. Attorney and filed in U.S. District Court. Informations are used when a defendant has waived his or her right to a grand jury indictment. Both businesses and persons may be the subjects of indictments or informations. For Case Management purposes, an indictment /information is an initial or interim enforcement statistic.

2.25 *In Rem* Arrests

In rem arrests occur when tangible property is taken into custody by the U.S. Government during the seizure and forfeiture process. *In rem* arrests are normally accomplished using a court order or arrest warrant that has been issued by a judge. For Case Management purposes, *in rem* arrests are initial enforcement statistics.

2.26 Integrated Automated Fingerprint Identification System

The Integrated Automated Fingerprint Identification System (IAFIS) is a Federal Bureau of Investigation (FBI) system that holds specific fingerprint, biographic, and criminal history information of those persons who have been apprehended/arrested by various law enforcement agencies. All criminal bookings in EAGLE are automatically submitted to IAFIS.

2.27 Investigation

An investigation is initiated when it has been determined that one or more violations of law enforced by HSI have occurred or are likely to occur. Investigations can be criminal, civil, or administrative in nature.

2.28 Investigative Case Management

Investigative Case Management (ICM) is the HSI system of record for Case Management. All HSI Special Agents and TFOs utilize Case Management to document investigative cases.

2.29 Investigative Referral

Investigative referrals are used when one HSI office has received or developed information and sends it to the appropriate HSI office. Investigative referrals may be general in nature (unlike specific collateral lead requests) and may be categorized primarily as "tips" or general non-specific case-related leads. Referrals may involve general for your information (FYI) types of information which do not warrant a collateral investigation.

2.30 Juvenile

A juvenile is a person who has not reached the age (usually 18) at which one is generally treated as an adult by the legal system.

2.31 Mid-Level Field Manager

Mid-level field managers include Resident Agents in Charge (RACs), Assistant Special Agents in Charge (ASACs), and Deputy Special Agents in Charge (DSACs), who manage supervisors overseeing day-to-day operations.

2.32 Nolle Prosequi (Nolle Pros)

A *nolle pros* is a final legal disposition for a defendant where the prosecutor has decided to discontinue the prosecution. For Case Management purposes, a *nolle pros* is considered a final enforcement statistic.

2.33 Non-Consensual Monitoring

A non-consensual intercept is the electronic monitoring of private communications without the consent of any of the parties to the conversation. Typically, this requires the issuance of a court order.. Applications for non-consensual intercept court orders must be processed through HSI Headquarters. For Case Management purposes, non-consensual intercepts are case statistics and are captured via an ROI and ELSUR. (Note: For additional information on non-consensual monitoring, SAs should consult the Technical Operations Handbook (HSI HB 14-04), dated July 14, 2014, or as updated).

2.34 Offers in Compromise

An offer in compromise occurs when a subject or business voluntarily agrees to pay duties and/or penalties, either prior to or after the issuance of a penalty notice by CBP Office of Field Operations (OFO) Director of Field Operations (DFO). Voluntary tenders are reported in Case Management as offers in compromise. For Case Management purposes, offers in compromise are final enforcement statistics.

2.35 Participation Code

Participation refers to the role of an office in relation to an enforcement action such as an arrest or seizure. The level of participation in the enforcement action must be measurable in order to claim credit for the enforcement action and any subsequent enforcement results. Supervisory

personnel must be able to specifically articulate how their office personnel directly participated in the enforcement action.

2.36 Penalty Issued

A penalty issued refers to instances when a CBP OFO DFO issues a penalty notice for a civil violation of law. Penalties may also be issued based on CBP referrals or may be issued by other agencies or departments including, but not limited to, DHS, the Department of Commerce, the Department of Justice, and the Department of the Treasury. Penalties may be issued to individuals, businesses, or both. CBP penalties are only issued by the DFOs in their respective ports. Worksite fines are issued by HSI field offices. Penalties are entered in Case Management only by the office that conducted the investigation and referred the case for penalty action. Offices that conduct collateral investigations will not report the penalty unless their local field office issues the penalty as a result of their collateral investigation. For Case Management purposes, penalties issued are initial enforcement statistics.

2.37 Penalty Recovered

A penalty recovered is a payment to CBP or ICE for the penalties or fines that have been issued based on a civil violation of law. Penalties may also be recovered by other agencies or departments based on CBP or ICE referrals. There must be a penalty issued for a penalty to be recovered. For Case Management purposes, penalties recovered are final enforcement statistics.

2.38 Polygraph Examination

A Polygraph Examination is a process that involves the monitoring and recording of respiration, electrodermal activity, cardiovascular activity, and possibly other parameters during which questions are presented to the examinee. The physiological recordings are analyzed to determine if specific and consistent responses are noted that research has identified to be associated with deception. For the purposes of Case Management, a Polygraph Examination conducted during the course of an HSI investigation is a case statistic.

2.39 Pre-Trial Diversion

A pre-trial diversion is a final disposition of a defendant who has pleaded guilty to one or more charges and has been typically placed on a form of probation for a specified period of time. If all the conditions of the probation are met, the guilty plea is set aside. For Case Management purposes, a pre-trial diversion is a final enforcement statistic.

2.40 Principal Headquarters Officers

The Principal Headquarters Officers (PHOs) are the HSI Executive Associate Director, Deputy Executive Associate Director, Assistant Directors, and Deputy Assistant Directors.

2.41 Program/Project Codes

Program/Project codes are used to associate Case Management data (e.g., hours, statistics, reports, etc.). with specific program/project areas and specific undercover or special operations. Several program codes can be entered into one case, providing greater flexibility when querying Case Management. Program codes will allow a case to be included in statistical reports that focus on a particular program area. Program Codes should also be used across law enforcement systems (e.g., ICM, EAGLE, SEACATS, etc.).

(Note: The terms "Program" and "Project Codes" are used interchangeably in this document, as they are in HSI law enforcement systems).

2.42 Purchase of Information/Purchase of Evidence

Purchase of Information (POI)/Purchase of Evidence (POE) costs identify the amount of POI/POE expenses for each investigation. (Note: For additional information on POI/POE, SAs should consult the Informants Handbook [HSI HB 12-03], dated August 2, 2012, or as updated).

2.43 Referral for Prosecution

A referral for prosecution refers to the date when a case is presented for prosecution. (Note: For additional information, SAs should consult the "ICM User Manual.")

2.44 Search Warrant

For the purposes of Case Management, a search warrant is a case statistic when an SA was the affiant or co-affiant on the search warrant application, or when the SA was instrumental in providing or developing the probable cause that was required to obtain the warrant.

2.45 Seized Asset and Case Tracking System

The Seized Asset and Case Tracking System (SEACATS) is the CBP-owned system used to document all seizures of tangible property.

2.46 Seizures

Seizures are the physical or constructive possession of property, real or personal, which may be held for forfeiture, for violation of law, or as evidence. Seizures will normally be claimed by the HSI office in whose AOR the seizure was made. For Case Management purposes, seizures are initial enforcement statistics.

2.46.1 Seizure (with no value)

A seizure with no value is a seizure in which the item does not have any monetary value. Examples of this type of seizure include drugs, photographs, and documents. Although these items will normally require additional processing, there will not be an automatic updating of the seizure disposition from the Fines, Penalties, and Forfeitures (FP&F) system. Final dispositions are required in Case Management for seizures of evidence.

2.46.2 Seizure (with value)

A seizure with value is a seizure in which the item has monetary value. Examples = include currency, monetary instruments, vehicles, real estate, and jewelry. Final dispositions are required in Case Management for all seizures with value.

2.47 Statistics

2.47.1 Case Statistics

Case statistics are activities and incidents that are attributable to a specific case. These statistics are used by management to evaluate the productivity of enforcement personnel, offices, and specific investigations. Case statistics do not require association with final enforcement statistics, but do require closing statistics.

2.47.2 Collateral Statistics

Collateral statistics are used to account for case work that is conducted based on information provided by another HSI office via a collateral case request. Collateral statistics allow an office to capture enforcement statistics where the action occurred, in conjunction with the office that initiated the case.

2.47.3 Enforcement Statistics

Enforcement statistics can be initial, interim, and/or final. Statistics are used to track activities and incidents that are attributable to specific cases. Enforcement statistics are used by management to evaluate the productivity of enforcement personnel, offices, and specific investigations. Final enforcement statistics document the ultimate disposition of initial enforcement statistics. Cases cannot be closed in Case Management unless all initial enforcement statistics are associated with final enforcement statistics.

2.48 Sub-Category

A sub-category is used to further define the broad investigative case categories. Each case category has several sub-categories that facilitate the querying of information in Case Management.

2.49 Superseding Indictment

A superseding indictment is an indictment that is returned by a grand jury subsequent to the return of a previous indictment. Superseding indictments are recorded as indictments in Case Management. No distinction is made in Case Management between superseding indictments and original indictments. Only additional (new) charges (statutes) and counts will be added in Case Management when a superseding indictment is obtained. For the purposes of Case Management, an indictment is an initial enforcement statistic.

(b)(5)

2.50 Task Force Officer

A Task Force Officer (TFO) is a law enforcement officer from another federal agency who supports HSI investigations, works under the direct supervision of an HSI supervisor, and needs access to Case Management.

2.51 TECS Portal

TECS Portal is the information system used by CBP to perform their border security mission. TECS Portal interfaces with Case Management so that appropriate information can be shared between ICE and CBP.

2.52 Telecommunications Linking System

The Telecommunications Linking System (TLS) is an application accessed from within Case Management that stores case-related telecommunications information derived from investigative events. TLS links data with investigations, facilitates collaboration, and shares information with other federal law enforcement agencies. TLS data is also accessible from within FALCON.

2.53 Threat and Assault Investigations

HSI has the responsibility to investigate certain assault and threat activity as it relates to ICE and CBP employees. (Note: For further information, see U.S. Customs Service (USCS) Directive 1440-021A entitled, "Investigation of Threats and Assaults and Protection and/or Relocation of Threatened Employees and Family Members," dated September 13, 2000, or as updated.)

Chapter 3. ROLES AND RESPONSIBILITIES

The utility of Case Management relies on the conscientious efforts of personnel at all levels in HSI. Each level of user has specific responsibilities with respect to Case Management. The following sections outline roles and responsibilities as they pertain to Case Management and general office functions.

3.1 Roles

The following are key roles within Case Management. The list is not comprehensive.

3.1.1 Agent

The case agent creates cases, documents, and subject records, and performs searches in conjunction with investigative duties.

3.1.2 Supervisor

The "Supervisor" reviews and approves case actions, documents (including ROIs), subject records, media, and hours reports submitted by his/her direct subordinates. The supervisor can reassign cases between case agents reporting to him/her.

3.1.3 Referral Manager

The Referral Manager receives all collateral case requests and investigative referrals and routes them to the appropriate supervisor within his or her office.

3.1.4 SAC Approver

The "SAC Approver" approves items requiring second-level approval, including specific documents, foreign language hours, electronic surveillance (ELSUR) authorizations, and significant case reports (SCRs). The head of the office is responsible for designating a "SAC Approver" for these items.

3.1.5 Headquarters Approver

The "Headquarters Approver" approves items that require HSI Headquarters-level approval, including ELSUR authorizations and SCRs.

3.1.6 System Control Officer (SCO)

The "SCO" creates, assigns, and maintains user roles and office profiles in Case Management. The SCO has the ability to activate new users; set user roles in the system; make profile changes to users and offices; and transfer agents and cases between offices and supervisors. The SCO has the authority to make changes for users within or below his or her assigned office level.

3.1.7 National System Control Officer (NSCO)

The "NSCO" holds all SCO capabilities for every office across HSI.

3.2 Responsibilities

The following are responsibilities of HSI investigative personnel as they pertain to Case Management and general office functions.

3.2.1 Case Agent

This section will discuss case agent responsibilities in the following areas:

- Accuracy of information
- Timely completion of reports
- Timely entry of hours and statistics
- Completeness of case files
- Proper storage and security of files
- Completeness and maintenance of subject records

3.2.2 Accuracy of Information

The case agent is the primary individual responsible for the accuracy of Case Management information. This includes case hours, case and enforcement statistics, and reports entered into relevant law enforcement systems. The accuracy of information relating to investigations is of critical importance during all phases of a case.

3.2.3 Timely Completion of Reports

The case agent is responsible for the timely and accurate completion of case reports. Chapter 4 of this Handbook, entitled "Investigative Case Files and Reports," identifies specific time limits for the completion of reports. Case agents must submit these reports to their supervisor no later than the specified times. If a reporting time limit cannot be met, it is the responsibility of the case agent to discuss the delay with the first-line supervisor. If appropriate, the first-line supervisor may extend the reporting time limits.

3.2.4 Timely Entry of Hours and Statistics

The case agent is responsible for the timely entry of hours and statistics in Case Management. Posting hours and statistics in an untimely manner will result in those hours and statistics not being included in certain management information reports. Investigative hours are required to be entered no later than the tenth working day of the next month. If this time limit cannot be met due to unforeseen circumstances, it is the responsibility of the agent to enter the hours as soon as possible.

Case and enforcement statistics are required to be entered as soon as possible but no later than 5 days after the occurrence of the enforcement activity or immediately upon receiving notification of occurrence. If this time limit cannot be met due to other investigative commitments, it is the responsibility of the case agent to discuss the matter with the first-line supervisor.

Initial enforcement statistics include, but are not limited to, arrests (criminal and administrative), indictments/informations, seizures, and penalties (issued).

Final enforcement statistics include, but are not limited to, convictions; voluntary returns; turn-overs to other agencies; court-imposed fines; nolle-pros; acquittals; dismissals; seizures that have been forfeited, destroyed, or returned; and penalties or duties that have been collected.

Case Management will not allow cases to be closed unless all enforcement statistics have final disposition(s) reported and approved.

3.2.5 Completeness of Case Files

The case agent is responsible for ensuring that each case file is complete. This includes attaching relevant documents to the media tab of the case in Case Management, such as:

- Court documents (e.g., warrants, subpoenas, indictments, court orders, pleadings, etc.)
- Agency documents (e.g., immigration documents, customs documents, memoranda, letters, custody receipts, inventory sheets, monetary count sheets, etc.)
- Investigative paperwork (e.g., miscellaneous documents, photographs, fingerprint cards, investigative notes, photocopies, etc.)

3.2.6 Proper Storage and Security of Files

Case agents are responsible for the proper storage and security of all physical and electronic files that are in their custody, including case files, A-files, and other working files. All physical files must be maintained in a secure location and placed into locked storage when not in active use. All electronic files must be stored on approved encrypted media or must be encrypted when being transmitted via email or other means.

Loss of sensitive case information can result in danger to SAs, material witnesses, and confidential informants. Proper electronic security and media control procedures must be employed for files that are kept in an electronic format. (Note: See ICE Directive 4003.2, entitled, "Safeguarding Law Enforcement Sensitive Information," dated May 20, 2014, or as updated. For additional information, see DHS 4300A, entitled "Sensitive Systems Handbook," dated November 15, 2015, or as updated).

3.2.7 Transmission of Contents of Case Files

Case agents may transmit case file information via email provided that any law enforcement sensitive information is encrypted.

3.2.8 Completeness and Maintenance of Subject Records

The case agent who owns a subject record is responsible for ensuring that the subject record is complete (see Section 4.1.9). This includes adding all identifiers (i.e., driver's license numbers, FBI numbers, Social Security numbers, etc.), as well as all related phone numbers, addresses, etc. Subject records must be updated with current and accurate information as it becomes available. Whenever practical, the case agent should add a photo of the subject.

3.3 First-Line Supervisor

The first-line supervisor's duties are discussed in the following sections:

- Verifying adherence to policies and procedures
- Promptly reviewing and approving/disapproving reports, statistics, media, and hours
- Evaluate necessity of collateral requests
- Providing advice and direction
- Conducting periodic case reviews
- Assigning an acting supervisor
- Ensure case hours logged are as accurate as possible

3.3.1 Verifying Adherence to Policies and Procedures

First-line supervisors are responsible for ensuring that enforcement personnel under their supervision are conducting investigations in compliance with applicable policies and procedures. First-line supervisors must ensure continuity of investigations, which includes reassigning open and pending cases to another SA in the event of an originating SA's transfer, retirement, or resignation. This includes any subject records which have law enforcement or investigative value. Any standalone subject records not meeting the above criteria must be archived by the owner prior to their departure.

3.3.2 Promptly Reviewing and Approving/Disapproving Reports, Statistics, and Hours

First-line supervisors are responsible for entering their own case hours as well as for reviewing/approving/disapproving reports, statistics, media, and hours in Case Management for case agents under their supervision. Supervisors must ensure that reports are well written and in compliance with the applicable standards regarding format and content. Supervisors are required to perform a "quality control" role for the reports and data they review and approve/disapprove. Quality control includes verifying the accuracy and clarity of the data, ensuring that all codes and fields are entered correctly, excluding reports containing sensitive information that should not be entered in Case Management, and vetting associated documents. The review of reports, statistics, and hours must be approved by the first-line supervisor as soon as possible, but not to exceed 5 business days after they are submitted.

3.3.3 Evaluate Necessity of Collateral Requests

First-line supervisors are in the best position to evaluate the necessity of collateral requests that seek assistance from other HSI offices. Supervisors should request collaterals from other offices only when the requested action(s) cannot be done in their own office. Because some offices can be inundated with collateral requests for assistance, supervisors must exercise good judgment when approving collateral requests. Prior to forwarding a collateral request that will result in work by another office, the first-line supervisor should contact and discuss the request with his or her counterpart in the receiving office.

3.3.4 Providing Advice and Direction

First-line supervisors are responsible for providing advice and direction to the personnel they supervise regarding Case Management issues. Depending on their level of experience, case agents will require guidance regarding how to establish and achieve investigative goals. Advice and direction should be provided through routine oral and written communications and through periodic case reviews. Supervisors must also work in concert with more senior SAs to ensure that SAs with less experience receive appropriate guidance.

3.3.5 Conducting Periodic Case Reviews

First-line supervisors are required to review the case file, including but not limited to case openings, modifications, and closings. In addition, first-line supervisors are required to ensure that cases are properly updated during case reviews.

The case review functionality in Case Management assists first-line supervisors during periodic case reviews, which are conducted at a minimum every 120 days or more frequently, as needed, or as mandated by the SAC. When conducting a case review, the first-line supervisor is required to provide narrative comments, recommendations, and/or investigative objectives which will provide the case agent with clear guidance and direction on how best to proceed with the investigation. Case reviews, to include supervisor comments, are captured in the case index.

3.3.6 Assigning an Acting Supervisor

First-line supervisors are required to designate an acting supervisor in Case Management when they are not able to fulfill Case Management duties due to scheduled leave or other circumstances. The acting supervisor must assume the roles, rights, and responsibilities of the individual for whom they are acting for a specified period of time.

In instances in which the supervisor is on extended leave (e.g., TDY, medical leave, vacancy, etc.), the identified long-term acting supervisor should be assigned the supervisor role. This includes receiving all direct reports, supervised cases, and supervised records from the previous supervisor.

3.4 Mid-level Field Managers

The duties of mid-level field managers (e.g., DSACs, ASACs, RACs, and designees) are discussed in the following sections:

- Verifying adherence to policies and procedures
- Establishing local office policies
- Coordinating office and SAC communications
- Coordinating investigative activities with other offices

3.4.1 Verifying Adherence to Policies and Procedures

Mid-level field managers are responsible for ensuring office adherence to applicable policies and procedures. They should not assume that first-line supervisors are consistently requiring their personnel to adhere to policies and procedures. Small but important details can easily be overlooked. Periodic spot checks and a vigorous internal controls program can aid mid-level field managers in determining adherence to policies and procedures.

3.4.2 Establishing Local Office Policies

Mid-level field managers are responsible for establishing local office policies and procedures that implement the AOR and national policies and procedures. These local policies can be more restrictive but not less restrictive than the SAC's AOR policies. Local policies must be clearly documented and accessible to case agents in the office.

3.4.3 Coordinating Office and SAC Communications

Mid-level field managers have primary responsibility for coordinating communications between the SAC office and sub-offices. Mid-level field managers are responsible for providing routine and periodic briefings and updates to their SAC.

3.4.4 Coordinating Investigative Activities with Other Offices

As Referral Managers or their designee in Case Management, mid-level field managers (or their designees) are responsible for receiving collateral cases and investigative referrals from other HSI offices, and routing them to the appropriate supervisors within their offices.

3.5 Special Agents in Charge (SACs)

The SACs' duties are discussed in the following sections:

- Maintaining oversight of policies and procedures
- Establishing AOR policies
- Coordinating headquarters and field communications

3.5.1 Maintaining Oversight of Policies and Procedures

SACs are responsible for ensuring oversight and implementation of the policies and procedures relating to Case Management. For example, as a SAC Approver in Case Management, the SAC or his/her designee must ensure that SCRs are routed to the appropriate Headquarters Approver(s).

3.5.2 Establishing AOR Policies

SACs are responsible for establishing AOR office policies and procedures that implement national policies and procedures. These AOR policies can be more restrictive but not less restrictive than national policies (e.g., SACs are permitted to establish more restrictive time frames than those set in this Handbook). Local policies must be clearly documented and accessible to case agents in the AOR.

3.5.3 Coordinating Headquarters and Field Communications

SACs have primary responsibility for coordinating communications between their office and Headquarters. Routine and periodic briefings and updates to Headquarters are the responsibility of the SACs or designees.

3.6 Assistant Director over Case Management (AD)

The ADs' duties are discussed in the following sections:

- Supporting field offices
- Verifying adherence to policies and procedures
- Monitoring case activity
- Responding to requests for information

3.6.1 Supporting Field Offices

ADs are responsible for ensuring that SACs receive necessary and appropriate Headquarters-level support, based on the availability of resources. The most important role of Headquarters is to support the SACs. Headquarters personnel also provide final approval of key enforcement documentation, such as SCRs, ELSURs, and Assault Threat Reports (ATRs).

3.6.2 Verifying Adherence to Policies and Procedures

ADs will maintain a level of oversight to verify that SACs are properly complying with national policies and procedures. This oversight function by Headquarters is essential to validate that SACs are being held accountable for adherence to national policies and procedures.

3.6.3 Monitoring Case Activity

ADs will maintain a level of oversight to monitor SAC case activity in their AOR. PHOs must be aware of significant developments in the major investigations that are being conducted by SACs.

3.6.4 Responding to Requests for Information

ADs are responsible for properly responding to various requests for information that are received by HSI Headquarters. When appropriate, Case Management is relied upon to respond to these requests for information. Efforts must be made to coordinate these requests with the field offices. Requests for information may be coordinated with the SACs.

3.7 Case Initiation

The Case Initiation section will discuss the following areas:

- Case number assignment
- Investigative case categories
- Types of investigations
- Vehicle accident investigations
- Distribution

3.7.1 Case Number Assignment

HSI case numbers are normally drafted by case agents and forwarded to first-line supervisors for approval. Once the first-line supervisor approves the case number in Case Management, the case is assigned the next sequential case number available. The case number consists of 14 characters as follows:

(b)(7)(E)

(b)(7)(E)

3.7.2 Types of Investigations

Case Management primarily focuses on four types of investigations:

- Formal Investigations
- Collateral Investigations
- Investigative Referrals
- Umbrella Investigative Activities

3.7.2(1) Formal Investigations

Formal investigations are opened when it has been determined that violations have occurred or are likely to occur.

3.7.2(2) Collateral Investigations

Collateral investigations are investigations which are opened in more than one HSI office and which focus on the same or related investigative targets. The HSI office that first opens the investigation will assign the originating office case number. It is imperative to the integrity of Case Management that non-originating offices use the collateral case number generated by the originating office's collateral request. Failure to comply with this procedure severely limits the ability to properly analyze the information contained in Case Management.

Examples of Collateral Case Numbers:

MI07OR16NY00090-Collateral Case
NY07OR16NY00090-Originating Case

Collateral investigations are used to request specific investigative case activities from another HSI office. All collateral investigative requests for assistance must be completed by the receiving office in a reasonable and timely manner. **Offices receiving requests for assistance must be responsive within 30 days from the date the originating collateral request was approved**. If there is a perceived need to have a collateral request for assistance expedited, the first-line supervisor who approved the collateral request may contact the first-line supervisor in the receiving office in an effort to coordinate the expeditious handling of the collateral request.

Collateral cases are electronically sent from the originating HSI office to the receiving HSI office via Case Management. Care must be taken when selecting the destination office for collateral requests in Case Management. Collateral requests cannot be re-routed once they have been routed to the receiving office.

It is critical to report collateral case statistics properly in order to avoid duplicate statistics. The same statistic should not be attributed to more than one investigative case as duplication can skew reporting to HSI Headquarters, agency leadership, Congress, and other key stakeholders.

3.7.2(3) Investigative Referrals

Investigative referrals are used to forward information received by an HSI office to another appropriate HSI office. Referrals may be general in nature (unlike specific collateral requests) and may be categorized primarily as tips or general non-specific case-related leads. Referrals may involve a general type of information that do not result in collateral investigations. Unlike collateral requests, the receiving office has the discretion of deciding whether or not an investigative lead is actionable.

3.7.2(4) Umbrella Investigative Activities

Umbrella investigative activities (e.g., FY17 assistance to the state police) are investigative activities not associated with a specific investigation. Typically, umbrella investigative activities are not specific enough to warrant the opening of a formal investigation. Often, an investigation begins as a general investigative activity and develops into a formal investigation, which may or may not generate one or more collateral investigations.

Case Management contains several investigate categories. These categories are to be utilized in the preparation of monthly hours reports that contain umbrella investigative activities.

Umbrella investigations must be closed in the fiscal year in which they are opened. The inclusion of arrests or seizures in umbrella cases should be discouraged.

3.7.3 Vehicle Accident Investigations

Government vehicle accident investigations conducted by HSI are reported using Case Management. Case Management non-suspect subject records will be created only on the non-DHS individuals involved in the accident, regardless of who is believed to be at fault in the accident. **Under no circumstances will a subject record be created for an agent/officer because of involvement in a government vehicle accident.** The subject records on the other individual(s) involved will be linked to the ROI that documents the investigation. The primary purpose for capturing this information is to assist Office of the Principal Legal Advisor attorneys who may be required to represent the government in legal proceedings. For more specific information, consult the applicable vehicle management and local policies.

Chapter 4. INVESTIGATIVE CASE FILES AND REPORTS

In conducting investigations, HSI case agents are required to record all activity and document all information using case files. Investigative case file organization will be discussed in the following sections:

- Case file composition
- Case file security

4.1 Case File Composition

The case file refers to the electronic collection of all information that pertains to a case, including but not limited to subject record(s), documents (e.g., ROIs), hours, statistics, and select media that is associated with a case. The case file includes documentation from the inception of a case to its conclusion. HSI uses case files to manage all investigative activities, as well as for personnel and administrative matters.

Case Management provides the ability for HSI case agents to create case documents and submit them through an electronic workflow process. Supervisors, reviewers, and others involved in the approval process can approve the insertion of documents into the appropriate electronic case files. Upon approval, Case Management serializes and records the documents as part of the official case file.

While all documents should exist in the electronic case file, certain types of documents must also be maintained in their original form in the event that a case is adjudicated. Original documents should be kept in a work file and archived when the case is closed (See Section 4.2).

The following sub-sections provide details about the composition of electronic case files.

4.1.1 Case Records (Case Management)

Electronic case files in Case Management are referred to as case records. Case Management case records are used to organize and link all records and documents associated with HSI investigations. Every data field must be completed in a case record if the information is known. Case agents and supervisors are required to update their case records as necessary.

First-line supervisors are required to review case openings, modifications, and closings. In addition, first-line supervisors are required to ensure that cases are properly updated during case reviews. The included case title must be as specific as possible (e.g., a person, business, or organization). Cases should not be named after certified undercover operations. General statements such as “theft of merchandise,” vehicle registration numbers, or vessel names should not be used as case titles. Incomplete case titles must be updated as more specific information is developed on the subject(s).

4.1.1(1) Cases Opened in Error

(b)(5)

Cases created and approved in error, even when no documents have been created, require a "Closing" ROI and at least one hour posted to the case.

4.1.1(2) Time Limits for Opening Case Records

Cases must be opened in Case Management as soon as possible, but no later than the end of the fifth business day after the investigation has been initiated. The first-line supervisor must approve any exceptions to this policy.

4.1.1(3) Automatic Creation of Collateral Cases

Case Management automatically sends a draft collateral case to a receiving HSI office. The receiving office referral manager is required to assign the collateral request to a first-line supervisor. Once the first-line supervisor receives the collateral request, the first-line supervisor must open and approve the case within 5 business days. Once the case is approved, it can be assigned to a specific case agent. **Offices receiving requests for assistance must be responsive within 30 days from the date the originating collateral request was approved.** (See Section 3.7.2(2)).All policies pertaining to regular cases in Case Management apply to collateral cases.

4.1.1(4) Updating OCDETF Cases

Once a case is approved by an Organized Crime Drug Enforcement Task Force (OCDETF), the specific date of acceptance and the OCDETF assigned case number must be entered in the appropriate places in the cases. It is important to update the cases with the OCDETF number within 30 days of approval in order to ensure timely reimbursement of investigative expenses and statistical recognition for the OCDETF program. (Note: Enforcement statistics and expenses for category 13 cases are applied to the OCDETF program if they occurred after, or 30 days prior to, the date of approval by the core-city OCDETF. Enforcement statistics and expenses for category 02 and all other case categories are applied to the OCDETF program if they occurred after or up to 90 days prior to the date of acceptance by the OCDETF).

4.1.1(5) Updating Other Special Interest Fields (Joint Terrorism Task Forces (JTTFs), Title 21, etc.)

In instances where the investigation involves a special interest field, case agents will ensure that these cases are properly designated. It is also case agents' responsibility to ensure that cases are updated if there are any changes in case status.

4.1.1(6) Significant Impact Questions
Insert language

4.1.1(7) Case Management Case Review

The case review assists the first-line supervisor and will be conducted every 120 days at a minimum. During or subsequent to the case review, the first-line supervisor is required to provide narrative comments, recommendations, and/or investigative objectives in Case

Management. These comments provide the case agent with clear guidance and direction on how best to proceed with the investigation.

4.1.1(8) Case Index

The case index in Case Management serves as an automated chronology of the actions served on the case. Case agents and supervisors can manually enter entries in the Case Management case index, but are not required to do so.

4.1.1(9) Access Levels

Subject records linked to Case Management case records may be restricted by access level. Access levels on Case Management subject records determine which groups of Case Management or external users may view the subject records. In general, the access level of HSI subject records must allow as many users as practical to view the records. The access level is determined by the sensitivity of the information contained in the subject record and by the security needs of the investigation. HSI should not arbitrarily restrict access to subject records. HSI has the option of allowing greater access to subject records, while at the same time restricting access to their related source documents, such as ROIs. All records that have been restricted to specific users will be updated to a lower-level of case restriction upon case closure.

4.1.1(10) Distribution

Case Management case records allow for the inclusion of country codes in an effort to identify other HSI offices that may be interested in an ongoing investigation. Country codes are defined at the office level (e.g., MEX for Attaché Mexico). If a three-character country code is included in the appropriate place in aca Case Management case record or document, the case record or document will be visible in the distribution tab for the identified office. It should be noted that only the record/document in which the country code is applied will be distributed. This procedure allows one HSI office to automatically keep other interested HSI offices up to date on ongoing investigative activities. This procedure does not replace the need to properly coordinate investigative activities between offices via other means of communication.

4.1.1(11) Significant Event Notification System

Even though they are not a part of Case Management, Significant Event Notification (SEN) records must be included in the case file. (See the applicable ICE policy on SEN for more information). Approved SEN reports must be saved as a PDF and uploaded as part of the electronic case file in ICM.

4.1.2 Reports of Investigations (ROIs)

Case agents and first-line supervisors must be cognizant of the importance of ensuring that ROIs are properly written and provide the most accurate information possible.

4.1.2(1) Purpose of the ROI

The ROI is used to document investigative activities, to document results of an investigation, and to report on collateral requests to and from other offices. ROIs can be entered against an open or pending case. The ROI provides a narrative description of information received or significant action (i.e., investigative findings, surveillance, search warrants etc.).

4.1.2(2) General Guidelines

ROIs describe the who, what, where, when, how, and why of an investigation. ROIs must be written in the third person. The author of the ROI must not use indeterminate or passive language. Once approved in ICM, the ROI generates an electronic signature, which documents the date, the case agent, and the approving supervisor. If an acting supervisor approved the ROI in ICM, the name of the acting supervisor will appear on the ROI as the approving supervisor. As electronic submission by the author and approval by their supervisor denotes approval of the ROI, it is not necessary to have either party physically sign a hard copy of the ROI. A physical signature may be required by some United States Attorney Offices

When writing the ROI, the information should be presented in chronological order according to when the activity occurred. Whenever possible, paragraphs should begin with statements such as: "On January 21, 2016, at approximately 10:35 p.m…." The case agent must normally refrain from including subjective comments, conclusions, and opinions in ROIs. The most common exception to this policy involves Customs Broker License investigations where the investigator is required to provide recommendations to CBP based on his/her investigative findings, if any. (Note: For further information, see U.S. Immigration and Customs Enforcement "Style Guide" dated October 2009, or as updated).

4.1.2(3) Case Statistics-Generating ROIs

Certain types of ROIs generate statistics towards a case. As with all statistics, it is imperative that case statistics-generating ROIs be recorded accurately to support the strategic information needs of the agency. ROIs that generate statistics include (codes included):

- W – Search warrants
- 6 – Electronic media
- N –Computer forensics
- 9 – Title III
- Q – Grand jury information
- E – Polygraph examinations

4.1.2(4) Confidential Informants

The first page or synopsis of all ROIs containing information provided by confidential sources of information must be included in the source file. Initial source documentation ROIs must contain specific information that has been provided by the source. Every report that refers to a documented informant should be referred to by the assigned informant number and a copy

should be placed in the source file. (For additional information on confidential informants, see the Informants Handbook (HSI HB 12-03), dated August 2, 2012, or as updated.)

4.1.2(5) Timeliness of Reporting

The opening ROI will be written within 20 business days after the case is opened in Case Management. Subsequent ROIs which report significant activities must be written as soon as practical after the conclusion of the investigative activity described in the report.

Investigative activities should be promptly documented in ROIs while the events are clear in the memory of the writer. In addition, the same concept should apply to first-line supervisors when reviewing and approving submitted reports. Supervisors are required to approve any ROIs submitted for review and approval as soon as possible.

Any exceptions to these requirements must be approved by the first-line supervisor.

4.1.2(6) Synopsis

The purpose of the synopsis is to provide an overview of the investigation and the purpose of the report.

The first paragraph should make a brief statement concerning the nature of the investigation, including the violations, violators, sources of information, time frames, and other agency participation. The second paragraph should contain a brief explanation as to the content of the particular report.

The synopsis is limited to a maximum of 16 lines. The synopsis may evolve as the case develops. If an ROI only includes a synopsis, the synopsis should include case status, whether it be ongoing, pending, or closed.

4.1.2(7) Details of the Investigation

There is no requirement to enter "Details of Investigation" in the body of the ROI text. This is added automatically from ICM. Lengthy ROIs which attempt to report investigative activities over several months of the investigation should be avoided.

First-line supervisors should be cognizant of the importance of ensuring that ROIs are properly written and provide the most accurate information possible.

4.1.2(8) Removal of ROIs from Case Management

The removal of ROIs from ICM is conducted only in extreme circumstances, such as those that may compromise the integrity of an undercover operation or threaten the life of an agent/officer or an informant. With appropriate justification, authorized Headquarters personnel may remove a previously-approved ROI from ICM.

In order to request the removal of an ROI, the SAC must send a written request to the appropriate AD and/or his/her designee. The request must state the specific reason(s) for requesting the removal of the ROI.

If the request is approved, the SAC or his/her designee is responsible for ensuring that the original (approved) copy is maintained by the office. The original approved ROI will not be destroyed after the ROI is removed and must be maintained for presentation during the discovery process, if required. The removed ROI number will not be reissued to a subsequent ROI. ROIs will not be removed due to factual, spelling, or grammatical errors. If approved ROIs contain these types of errors, the case agent shall make the necessary corrections and then re-upload the ROI as a new ROI. The new ROI should contain a sentence at the end of the synopsis identifying the new ROI as a replacement of a specifically identified prior ROI that contained errors.

The removal of an ROI will be decided on a case-by-case basis by the AD or his/her designee.

4.1.3 Classified Information and Certain Sensitive Documents

Classified information will not be included in any ROI or document within ICM. Case agents need to be cognizant of the fact that certain sensitive documents are not to be included in the case file or referenced in ROIs (i.e., sensitive HSI, FBI, DEA, and/or DOD, financial documents, etc.).

4.1.4 Grand Jury Material

Grand Jury Material cannot be stored in the electronic case file. Therefore this information will not be included in an ROI. To record status, a case agent should document the return of Grand Jury Material and an analysis of material within it. Grand Jury Material must be handled in accordance with the procedures outlined in Rule 6(e) of the Federal Rules of Criminal Procedure.

4.1.5 SEACATS S/A/S

SEACATS is used to document all seizures of tangible property. Enforcement activities that are reported as SEACATS S/A/S must also be reported in ROIs. SEACATS S/A/S do not replace the need to write ROIs. (Note: For detailed information, consult the "Seized Asset Management Enforcement Procedures Handbook," dated July 2011, or as updated.)

4.1.6 Mandatory Adoption of CBP-Generated SEACATS S/A/S

CBP-generated incidents should be adopted within 10 business days. It is inappropriate to adopt only a portion of the SEACATS S/A/S. For example, case agents must adopt both the Seizure and Arrest. Any exceptions to these requirements must be approved by the first-line supervisor.

4.1.7 Case Management Incident Reports

The Case Management incident report is used to document arrests, seizures, and enforcement statistics. They can be entered directly in Case Management or created by importing EAGLE

events or adopting SEACATS incidents. Case Management incident reports must be entered to accurately capture enforcement statistics.

4.1.8 DHS-191 Privacy Act Disclosure

The DHS-191 Privacy Act Disclosure is used to document the disclosure of information from ICM. The disclosure report is associated with the applicable Case Management document. A separate ICM disclosure report must be completed for each subject of a Privacy Act disclosure. If a disclosure which is reportable under the Privacy Act is made, then a Privacy Act Disclosure Report must be completed and attached to the media tab of the case in Case Management. The DHS-191 Form is available on HSINet.

4.1.9 Subject Records

Subject records are created in ICM to document HSI interest regarding individuals, entities, or items. They may be linked in Case Management to cases or documents such as ROIs, ELSURs, and Case Management incident reports. Subject records are automatically published to CBP's TECS Portal and should be linked to all HSI-initiated SEACATS S/A/S.

Case agents are responsible for ensuring the subject records they own are as complete as possible for Case Management purposes. This includes adding all identifiers (i.e., Driver's License Numbers, FBI Numbers, Social Security Numbers, etc.), as well as all related phone numbers, addresses, etc. Whenever practical, the case agent should also add a photo of the subject.

Multiple subject records on the same individual, entity, or item may be created for a specific purpose, but should be avoided whenever possible.

4.1.9(1) Updating and Maintaining Subject Records

It is the responsibility of the subject record owner to ensure that the most current information available is included in subject records. Subject records must be updated with current and accurate information as it becomes known.

Appropriate maintenance of subject records includes linking records to a case whenever possible. Agents should create standalone records for investigated subjects who are not associated with a case at the time of creation.

4.1.9(2) Transferring and Archiving Subject Records

It is the responsibility of the subject record owner to transfer or archive records prior to leaving an office. During office transitions, subject records that are actionable or that still have investigative value should be transferred to a local owner. Standalone records that are no longer actionable or that do not have investigative value can be archived.

First-line supervisors must ensure that investigations and subject records are reassigned to another SA in the event of an originating SA's relocation, retirement, or resignation.

While subject record owners are responsible for transferring or archiving their own records, SCOs and supervisors should facilitate the process when necessary.

4.1.9(3) Access Levels

Access levels on Case Management subject records determine which groups of ICM or external users may view the subject records. In general, the access level of HSI subject records should allow as many users as practical to view the records. The access level should be determined by the sensitivity of the information contained in the subject record and by the security needs of the investigation. HSI should not arbitrarily restrict access to subject records. HSI has the option of allowing greater access to subject records, while at the same time restricting access to their related source documents, such as ROIs. All records that have been restricted to specific users will be updated to a lower-level of case restriction upon case closure.

4.1.11 Case Management ELSUR

The Case Management-generated Electronic Surveillance (ELSUR) is used to request authorizations, grant authorizations, and submit reports of use/non-use for consensual electronic surveillances.

The ELSUR is typically initiated by the case agent and subsequently submitted for approval to the first-line supervisor and the appropriate SAC and/or Headquarters Approver. The ELSUR, like other Case Management documents, is linked to the case and subject records.

The ELSUR is used for all forms of electronic surveillance. Prior to conducting non-telephonic and telephonic consensual electronic surveillances, approval must be granted by the SAC or their designee, and concurrence must be received from a U.S. Attorney. An ELSUR request for authorization must be submitted for both exigent and non-exigent consensual non-telephonic electronic surveillances. In the cases of exigent circumstances, please refer to the HSI Technical Operations Handbook 14-04 (verify) dated July 21, 2014, or as updated.

Reports of use/non-use for both telephonic and non-telephonic authorizations are initiated by the case agent after the authorization time period has expired. The reports of use are submitted for approval via Case Management to the first-line supervisor, the SAC or their designee, and ultimately the Headquarters Approver. Reports of use/non-use are required to be entered into ICM no later than 5 business days after the expiration of the reporting period.

Recordings or other intercept data generated from ELSUR authorizations are government created electronic evidence and have specific storage and safeguard requirements. (See the Technical Operations Handbook (HSI HB 14-04), dated July 21, 2014, or as updated.)

4.1.12 Confidential Source Payment and Benefit Transaction Receipt

Payments and benefits to confidential sources shall not be documented in an ROI. (Note: For additional information on confidential informants, see the Informants Handbook [HSI HB 12-03], dated August 2, 2012, or as updated.)

4.1.13 Investigative Notes

All investigative notes will be retained by the case agent in an envelope labeled "Investigative Notes" that includes the case number and date of closure. Notes taken by a case agent while interviewing a potential witness, an informant, a suspect, or a subject of an investigation are subject to discovery. Failure to produce these notes, even due to good faith loss or destruction, could result in the dismissal of a criminal case. Case agents must preserve such notes, even if their contents have been subsequently documented in an ROI.

Court decisions require that investigative notes be retained in the same manner as interview notes. Therefore, all notes made during investigative operations which could contain information that may ultimately be included in formal reports or which record events about which enforcement personnel may later testify must be retained. Court documents, including investigative notes, should be uploaded as media in the Case Management case record within 20 business days.

The notes taken by informants to assist in their reporting of information to a case agent must be preserved.

4.1.14 Court Documents

Court documents routinely saved in the case file include affidavits, court orders, criminal complaints, indictments, search warrants, arrest warrants, subpoenas, and judgment and committal orders. Court documents must be uploaded as media to the case file within 10 business days. Any exceptions to these requirements must be approved by the first-line supervisor.

4.1.15 Original Documents

All original documents that are associated with an investigative case will be uploaded to the Media tab, including Waiver Rights Forms, Suspect Total Lineups, Search Warrant Inventories, Change of Custody Forms, and any other source documents (See Section 3.2.5). The documents must be uploaded to the case file within 10 business days. Any exceptions to these requirements must be approved by the first-line supervisor.

4.1.16 Capturing Biometrics

All subjects arrested by enforcement personnel must be recorded electronically in EAGLE. Biometrics may be captured directly or imported electronically. In no circumstance should an arrest not captured in EAGLE be recorded in Case Management. Biometrics must be recorded in Case Management within 10 business days of an arrest. Any exceptions to these requirements must be approved by the first-line supervisor.

4.1.17 Photographs and Video

Photographs of arrestees, suspects, surveillance photographs, and other photographs of evidentiary value will be placed in the electronic case file. Photographs should also be attached to appropriate subject records and other case documents. Whenever possible, at least two frontal and one profile photographs will be taken of each person arrested.

When video of evidentiary value is available, video should also be attached to cases, documents, and/or subject records.

Photographs and videos must be uploaded as media to the case file within 10 business days. Any exceptions to these requirements must be approved by the first-line supervisor.

When applicable, photographs and/or videos within the electronic case file can be utilized for a discovery package. Under no circumstances will child pornography or other contraband be uploaded to the media section.

4.1.18 Other Media

Case-specific media is not limited to photographs and/or video. Media should also include documents or any other media format that can be digitally attached to a case, document, and/or record. Media must be uploaded to the case file within 10 business days. Any exceptions to these requirements must be approved by the first-line supervisor.

(Note: The Media tab is not a repository for digital evidence. Case agents are prohibited from uploading classified information and child pornography. Digital evidence will be maintained in accordance with existing policies in the following handbooks:

1) Computer Forensics Handbook (HSI HB 11-01), dated April 27, 2011, or as updated;
2) Child Sexual Exploitation Investigations Handbook (HSI HB 12-05), dated November 19, 2012, or as updated;
3) Asset Forfeiture Handbook (HSI HB 10-04), dated June 30, 2010 or as updated);
4) Cyber Crimes Investigation Handbook (HSI HB 11-03), dated August 9, 2011, or as updated.)

4.1.19 DHS-59 Fugitive Report

The DHS-59 Fugitive Report is typically completed on all HSI fugitives by the case agent and subsequently approved by the SAC or designee. This report must be completed as soon as possible but no later than the end of the first business day after the need for the report has been established. Fugitive reports are completed when efforts to arrest a defendant who has been formally charged in an HSI investigation have failed. (See Section 2.21 for a definition of "Fugitive.")

Fugitive reports are completed for any of the following reasons: initial entry, entry modification, and entry cancellation. Case agents must ensure that HSI fugitives are entered into the National Crime Information Center (NCIC) database. The case agent ensures that copies of the fugitive

reports are sent to the SAC Fugitive Coordinator, who distributes copies to the HSI National Fugitive Program Manager in Headquarters, and to the Law Enforcement Support Center (LESC). The original fugitive report will be maintained in the original case file.

Fugitive reports must contain as much identifying information as possible in an effort to facilitate the arrest of the subject and to assist law enforcement personnel in properly verifying whether or not a subject in their presence is truly the fugitive being sought. Whenever possible, a photograph and a set of fingerprints should be attached to the copy of the fugitive report that is sent to the HSI National Fugitive Program Manager.

The HSI case agent is responsible for ensuring that Case Management and NCIC fugitive records are cancelled whenever appropriate. If the person is no longer a fugitive, for whatever reason, a cancellation must be completed. (Note: For more information, consult the Fugitives Handbook [HSI HB 15-06], dated November 23, 2015, or as updated).

4.2 Case File Security

4.2.1 Work File Storage

Working files will be stored in an approved storage container in a location designated according to local office policy. (Note: Refer to DHS Management Directive 11030.1, "Physical Protection of the Facilities and Real Property, "dated April 21, 2003, or as updated.) Original case files will not be stored at home, vehicles, or other unapproved storage locations, (e.g., another agency's storage location).

4.2.2 Creation of Work File

A work file is created to allow the SA the opportunity to reference materials related to the investigation while working in the field. The work file should contain only information necessary to conduct appropriate field investigative activity. The intention is to prevent the amount of information released in the event that the file is compromised. The work file may contain copies of documents already uploaded to the case media tab. The work file will not contain original documents and can be destroyed at any time based on need. Appropriate security safeguards should be applied to ensure the integrity of the work file.

4.2.3 Disclosure of Case File

Any release of investigative case file material containing identifying data on a U.S. citizen or a legal resident alien to persons or agencies outside DHS (e.g., to other federal agencies), whether verbal or written, is required to be documented utilizing the DHS-191 Privacy Act Disclosure Report, in accordance with procedures implemented by ICE under the Privacy Act of 1974. There are exceptions for disclosure for law enforcement use and investigative/prosecution purpose under Title 5, U.S. Code (U.S.C.) § 552a(b)(7) and a(b)(3).

Additionally, Title 31, U.S.C., imposes stringent disclosure requirements on data collected on financial information forms and in associated computer databases. Disclosure of Currency and

Monetary Instrument Reports, Currency Transaction Reports, Foreign Bank Account Records, or Casino Report data, whether written or verbal, must comply with the applicable reporting requirements or other policy documents written on this topic.

4.2.4 Case File Retention

Original document retention procedures should be followed in accordance with local office policy. In no circumstances will the case file be destroyed prior to completion of judicial/administrative processes and appeals.

4.3 Juveniles

Subjects encountered under the age of 18 should be processed with due diligence and sensitivity. Case agents should be cognizant of the need to use discretion when dealing with juvenile subjects encountered during the course of a case. Case agents should review all applicable juvenile policies.

4.3.1 Fingerprints and Photographs

No subjects under the age of 14 will be fingerprinted or photographed without the approval of the SAC or designee. Juveniles above the age of 14 may be fingerprinted and photographed upon arrest utilizing EAGLE.

4.3.2 Subject/Booking Records

4.3.2(1) Subject Records

ICM subject records will be created for all individuals over the age of 14 who have been criminally charged or are the subject of an HSI investigation. At the direction of the SAC, subject records may be created for individuals under the age of 14 for the same circumstances.

4.3.2(2) Booking Record

An event will be created in EAGLE for all subjects arrested for an immigration violation regardless of age.

Chapter 5. EAGLE

5.1 Purpose

The Enforcement Integrated Database (EID) Arrest Graphical User Interface (GUI) for Law Enforcement, referred to as EAGLE, is the mandatory booking system for all subjects arrested by HSI. When HSI SAs book a subject in EAGLE, fingerprints will be electronically submitted to the Criminal Justice Information Services (CJIS) and the Integrated Automated Fingerprint Identification System (IAFIS).

Every arrest conducted by HSI must be entered into EAGLE. The subject's information and fingerprints must be entered into EAGLE as soon as possible. HSI does not fingerprint juveniles under the age of 14 without SAC approval, but in limited cases juveniles should be booked if they have a criminal history or are being arrested for criminal charges. Every entry into EAGLE must contain a subject's biographical data and biometrics.

SAs must still enter Incident Reports into Case Management, including administrative and criminal arrests.

5.1.1 User Fee Investigations

Case agents should ensure that User Fee Investigations are documented appropriately in EAGLE. (See 8 U.S.C. § 1356, "Disposition of monies collected under the provisions of this subchapter.")

5.2 Subject Entries

All arrests of individuals (excluding juveniles under the age of 14 unless approved by the SAC) will be processed using EAGLE. Subjects can be processed either by using a fingerprint scanner and digital camera, or by using a flatbed scanner and hard copies of the fingerprint cards and photographs. In the event of criminal proceedings, documentation generated in EAGLE will be maintained in the case file.(Refer to EAGLE 1.6, User Guide, dated April 12, 2013, or as updated.)

5.3 Interoperability

All EAGLE event numbers must be included in the ICM Incident Report and may be included in SEACATS S/A/S (if the incident involved seized property). SAs are responsible for ensuring that all related case and event numbers are annotated in the appropriate locations. **(Refer to EAGLE 1.6, User Guide, dated April 12, 2013, or as updated).**

Chapter 6. MANAGING HOURS AND STATISTICS

Law enforcement statistics (e.g., arrests and seizures) and administrative data (e.g., agent work hours on cases) are used for management and reporting purposes. Accurate reporting of hours and statistics is essential as this information is used for a variety of purposes, including evaluating enforcement programs, offices, and individuals; informing policy and funding decisions; and responding to requests for information from external offices.

6.1 Case Hour Entry into ICM

Case hours for a previous month will be entered into ICM by the end of the tenth business day of the new month. If, due to other casework, some personnel are unable to enter case hours by the tenth business day, they must obtain verbal approval from their first-line supervisor to enter their hours as soon as practical.

6.1.1 Responsibility for Entering Hours

A. HSI SAs, Intelligence Research Specialists, Intelligence Officers, Seized Property Specialists, Forensic Auditors, Investigative Assistants, Technical Enforcement Officers, and other enforcement personnel as instructed by management must post all their hours in ICM whether case-related or administrative in nature.

B. HSI personnel occupying support positions, such as Administrative Officers, Mission Support Specialists, Mission Support Technicians, Student Aids, Management and Program Analysts, Management Information Specialists, Management Program Technicians, Enforcement Support Specialists, Administrative Assistants, TFOs etc., are not required to post their hours in ICM. However, HSI personnel may enter hours at the discretion of local management.

Those HSI personnel who are required to enter their hours in ICM must do so on a monthly basis. Personnel must always be accurate when reporting their hours. If applicable, hours will be attributed to specific HSI case numbers. If there is no case to credit the hours to, hours will be attributed to specific investigative or interdiction program areas. Case Management hours are to be reviewed and approved by the first-line supervisor or acting supervisor by the end of the second business day after the hours have been entered into Case Management.

6.1.2 Programmatic-Specific Hours (i.e., OCDETF, JTTF, etc.)

Hours worked in support of specific investigations will be attributed to the specific investigation case number whenever possible. Non-case specific hours should be attributed to the programmatic-specific general case numbers. SACs are required to monitor programmatic-specific hours on a monthly basis to ensure that all time spent is reflected accurately in ICM.

6.1.3 Undercover Hours

Enforcement personnel who perform in an undercover capacity are required to enter these hours in Case Management in the appropriate columns that are identified for undercover use only. Hours that are reported in the undercover columns are not to be reported in the non-undercover hours columns. Hours are either undercover or not undercover; never both. Enforcement personnel will report hours as being attributable to undercover work only when they were actually in an undercover role. Translating audiotapes of undercover meetings, writing reports on undercover activities, and participating in security surveillances of undercover meetings will not be reported in Case Management as undercover hours. Supervisors who review the hours of undercover personnel must ensure that the number of these hours is reasonable and that they were actually spent in an undercover role.

6.1.4 Foreign Language Hours

Enforcement personnel who work foreign language hours related to a case should report the hours as such.

6.1.5 Computer Forensic Hours

Computer forensic agents and analysts should accurately reflect computer forensic hours to the appropriate case.

6.1.6 Intelligence Hours

Enforcement personnel who are performing intelligence work must attribute these hours based on the following criteria:

- Intelligence hours conducted in support of ongoing criminal investigations must be placed to the appropriate criminal case number in ICM.
- Intelligence activities not supporting a criminal case documented in ICM should be placed to the appropriate administrative category case number in ICM for field or Headquarters personnel.

6.1.7 Review and Approval of Hours

First-line supervisors are responsible for entering their own case hours as well as for reviewing/approving/disapproving hours reports in Case Management for case agents under their supervision.

6.1.8 Supervisory Hours

Whenever practical, supervisors will attribute their hours to specific HSI case numbers. When this is not possible, supervisors will report their hours to specific program areas whenever possible. Each case category has a case number designated for general supervisory investigative activities.

6.1.9 Administrative Hours

In addition to case-related hours, administrative hours worked by HSI SAs, Intelligence Research Specialists, Intelligence Officers, Seized Property Specialists, Forensic Auditors, Investigative Assistants, Technical Enforcement Officers, and other enforcement personnel should be posted in ICM.

6.1.10 Uncontrollable Overtime: Law Enforcement Availability Pay and Administratively Uncontrollable Overtime

SAs who work Law Enforcement Availability (LEAP) hours or enforcement personnel who work Administratively Uncontrollable Overtime (AUO) must enter their hours in the Uncontrollable Overtime (UOT) column in ICM. (Note: For additional information on LEAP and AUO, see ICE Policy #: 1040.1, Premium Pay Guide [Version 2.0] dated May 7, 2015, or as updated).

6.1.11 Designated Availability Hours

Designated Availability Hours (DAH) hours are off-duty hours during which an SA is given a specific start and end time by a supervisor when they are expected to be on stand-by. If the SA is not called in, those stand-by hours are recorded in the DAH column.

(Note: If employees are required to post hours under AUO, their hours cannot be posted under DAH. For additional information, consult the applicable policies on LEAP and AUO [see Section 6.1.10]).

6.2 Case Statistics

The case statistics section will discuss the following topics:

- Who captures statistics
- Collateral statistics
- When statistics are entered
- CBP-initiated statistics

6.2.1 Who Captures Statistics

Statistical information derived from Case Management supports the information needs of HSI senior executives by providing the data necessary to meet the strategic goals of the agency. HSI personnel in all job series and all levels must be aware of the importance of Case Management statistics and how they are used.

Case agents are responsible for ensuring that statistics are entered in an accurate and timely manner. First-line supervisors are responsible for approving statistics entered by their subordinates.

6.2.2 Collateral Statistics

The purpose of collateral statistics is to ensure that statistics are not recorded twice. The field office(s) where the enforcement activity ultimately takes place will be credited and responsible for capturing the statistics. Any arrests conducted by a field office based on the indictment or information of an HSI subject of investigation or fugitive will be credited to the arresting office. The office originating the investigation can claim the information/indictment and convictions statistic, but not the arrest statistic. Agents should be mindful not to duplicate incident records/statistics.

6.2.3 When Statistics Are Entered

Case and enforcement statistics are required to be entered as soon as practical after the occurrence, but no later than 5 days after the occurrence of the enforcement activity or upon being notified by the USAO. The first-line supervisor should approve statistics as soon as possible, but not to exceed 5 business days after they are submitted.

Certain initial statistics require a corresponding final statistic. Enforcement personnel are required to provide final dispositions for all initial enforcement activities (e.g., arrests, seizures, penalties issued, etc.). Each initial enforcement statistic must have a final disposition associated with it before the case status can be set to "closed" in Case Management.

6.2.4 CBP-Initiated Statistics

Enforcement statistics adopted by HSI must include both the seizure and arrest statistic if present. ICM will automatically attribute CBP-initiated enforcement statistics to Case Management when the appropriate HSI case number and an HSI participation code are entered into the CBP-initiated SEACATS S/A/S.

6.3 COGNOS

COGNOS is the Case Management reporting application currently used by HSI. COGNOS encompasses all migrated legacy case data, seizure data from SEACATS, and all data created in the ICM.

The information contained in COGNOS reports is derived from the hours, statistics, and reports entered ICM. PHOs/SACs and other personnel use management information reports compiled from ICM data in COGNOS for a variety of reasons, including evaluating the performance of enforcement programs and offices, and responding to requests for information from external agencies. SACs also use these reports to evaluate the performance of their offices, groups, and specific individuals. Information from COGNOS is also used to provide statistical reports to other stakeholders, including Congress.

6.4 Executive Information Reporting

The Executive Information Reporting Section (EIRS) of the HSI Data Management and Reporting Unit is the primary point of contact for the generation of all executive level statistical reports. All requests for ICE data and/or statistics from agencies or entities external to ICE

should be routed to the EIRS in order to ensure consistency, uniformity, and accuracy of statistical data.

6.5 Disclosure of Report Data and Statistics

Executive information reports contain sensitive statistics, and should be generated and disseminated in accordance with applicable Privacy Act disclosure requirements. If reports are requested by any agencies or entities external to ICE, proper disclosure procedures must be followed.

All HSI statistics (e.g., arrests, seizures, etc.) must be approved through the appropriate HSI PHO prior to being released outside of HSI.

Foreword

The Case Management Handbook provides a single source of policy and responsibilities for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents and other HSI personnel when using Case Management to process investigative cases. The Case Management Handbook contains policy that will help ensure uniformity and consistency at all HSI field offices. Investigative Case Management (ICM) is the HSI system of record for Case Management. Guidance on system procedures can be found in the online Case Management User Portal and Case Management User Manual. Oversight over Case Management resides with the Unit Chief, Operational Systems Development and Management (OSDM).

This Handbook supersedes ICE Office of Investigations (OI) Handbook 08-02, "Case Management Handbook," dated February 1, 2008, and any other policy documents on case management issued by the former OI or by HSI prior to the date of issuance of this Handbook. (See Appendix A for a list of superseded documents.)

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

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

_____ _____

Peter T. Edge
Executive Associate Director
Homeland Security Investigations

Date

FALCON User Footprint

1350 Trained HSI Users	1273 Current Accounts

- *HSI Tipline:* All HSI Tipline (41*) personnel have been formally trained on the FALCON system and Tipline workflow application. The Tipline user accounts will be activated on the date of their official workflow application launch.

- *Deactivated Accounts:* A small percentage (36*) of user accounts were immediately deactivated due to separation from the agency.

*shows variance between trained users and current accounts

User Numbers by Office

July 2012 – September 2012

Office	User Numbers
Washington, DC (HQ included)	180
San Diego	179
Boston	68
New York	61
El Paso	53
Houston	52
Chicago	47
Miami	46
Los Angeles	46
Atlanta	42
Tucson	41
San Antonio	38
Newark	37
Tampa	36
Phoenix	33
Dallas	31
St. Paul	29
San Juan	22
San Francisco	19
Detroit	16
Seattle	15
New Orleans	14
Honolulu	14
Baltimore	13
Philadelphia	12
Buffalo	10
Denver	8

FALCON User Footprint

FALCON Weekly Logins

Date	Unique Users	Total Logins
16 July – 22 July	263	730
23 July – 29 July	241	794
30 July – 5 August	273	890
6 August – 12 August	327	1107
13 August – 19 August	267	858
20 August – 26 August	257	889
27 August – 2 September	243	590
3 September – 9 September	269	752
10 September – 16 September	280	787
17 September – 23 September	263	748
24 September – 30 September	252	724
1 October – 7 October	274	788

Monthly Unique Logins

Month	Logins
July	561
August	607
September	538

Breakdown of FALCON User Methods

Method Type	Number of Users
Search and Link Chart	145
Link Chart Only	154
Research Only	118
Advanced Investigators*	110

*use FALCON for daily/weekly cases to conduct complex analysis

Data Sharing & Collaborative FALCON Metrics

Category	Totals
Number of Records Published	1480
Collaboration Teams (Number of unique users)	106 (341)
Number of Special Projects	60
Records collaboratively worked by multiple users	1500

The current FALCON Operations and Maintenance contract with Palantir, HSCETC-13-F-00030, has a period of performance from 6/14/2013 to 9/13/2018 (including the optional 6 month extension). OAQ's

(b)(5)

U.S. Immigration and Customs Enforcement

U.S. Department of Homeland Security
801 I Street, NW
Washington, DC
20536

Subject: Appointment as a Contracting Officer Representative (COR)

From: (b)(6);(b)(7)(C)

To: (b)(6);(b)(7)(C)

You are hereby appointed as the Contracting Officer Representative (COR) under Task Order HSCETC-13-F-00030 with Palantir Technologies Inc for FALCON Operations and Maintenance (O&M) Support Services. As the COR, your primary duty is to monitor Palantir Technologies performance to ensure that all of the requirements under the task order are met by the delivery date or within the period of performance, and at the price or within the estimated price stipulated in the contract. The duties or authorities in this letter are not delegable; therefore, you must advise the Contracting Officer, (b)(6);(b)(7)(C) or the Contract Specialist, (b)(6);(b)(7)(C) immediately when you are unable to perform these duties.

The duties and responsibilities of the COR for this task order are as follows:

1. Performing surveillance/inspection and acceptance

a. Perform on-site surveillance, as required, in accordance with the surveillance plan.
b. Document surveillance activities and provide a copy of documentation to the contracting officer.
c. Review technical proficiency and compliance against the technical provisions of the task order, and verify the performance of work by the contractor.
d. Perform surveillance of the performance under the business agreement and conduct inspections necessary to assure performance and compliance with the terms and conditions of the agreement.
e. Assure prompt review of draft reports and approval of final reports to contractor to assist with meeting the specified completion date of the task order, and assuring prompt inspection and acceptance, or rejection of deliverables.
f. Notify the contractor of deficiencies observed during surveillance.
g. Record and report to the contracting officer all incidents of faulty or nonconforming work, delays, or problems which may disrupt or hinder future performance.

2. Monitoring activities, cost, and providing input to contractor performance evaluations and notifications to the Contracting Officer

a. Component HCAs are responsible for contractor performance evaluation procedures and policies (see HSAM 3042.1500) for ensuring that contractor performance evaluations (interim and final) are included in the PPIRS through the Contractor Performance Assessment Reporting System (CPARS). The contracting officer has identified and requested that the COR submit input of the contractor's performance into CPARS.

b. Any requests for changes from a contractor.

c. Potential labor disputes or workforce problems.

d. Lack of performance which may jeopardize the cost or required schedule.

e. Monitoring financial management controls with respect to the allocation of appropriated dollars under the designated task order.

f. Possible changes in contractor management and/or key personnel.

g. Disagreements with the contractor regarding performance of performance work statement (PWS) requirements or other potential disputes with the contractor about technical or other business matters.

h. Any possible contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.

i. Procurement fraud, waste, abuse, bribery, conflict of interest, or other improper conduct to the CO and agency office, such as the OIG.

j. All problems, potential disagreements or controversy, both oral and in writing, regarding the status of the contract and performance of its requirements.

3. Making recommendations for invoices and payments

a. Report any discrepancies in payment vouchers to the contracting officer. Provide documentation to support the representation.

b. Evaluate progress payment requests based on costs incurred and actual work accomplished.

c. Certify invoices to the contracting officer for payment, using the Federal Financial Management System (FFMS) electronic invoicing system.

d. Reviewing contractor invoices for accuracy of work completed in accordance with contract requirements and certifying acceptance or rejection.

e. Review the contractor's invoices/vouchers for reasonableness and applicability to the contract and recommend to the contracting officer your approval, conditional approval, or disapproval for payment. The review must be completed within five days after receipt of the invoice or voucher. If you cannot meet the required review time, advise the contracting officer so that action can be taken to ensure Government compliance with the Prompt Payment Act, thereby avoiding the payment of interest penalties to the Contractor.

f. Review the contactors invoices/vouchers to ensure that they accurately reflect the work completed in accordance with the requirements of the contract, and certify acceptance of the delivered items. Submit certified invoices/vouchers to the Dallas Finance Center and copies to the contracting officer in a timely manner.

4. Managing Government Furnished Assets (when required)

a. You are not authorized to provide any Government-owned (or leased) equipment or supplies or use of Government space to the Contractor, other than those specifically identified in the business agreement and authorized by the contracting officer.

b. If applicable, ensure Government-furnished property is made available in a timely manner.

c. Request the contracting officer authorize Government-furnished property and, when requested by the contracting officer, provide disposition advice on Government-furnished property or contractor-acquired property.

5. Managing Contractor Employee Access (when required)

a. Serve as a Federal sponsor for the contractor, by assisting with the agency Security process, to include handling, as appropriate, the Contractor Suitability worksheet for contractor requiring a DHS PIV card, notification of results of the contractor access submissions, ensuring the return of the DHSPIV card, and communication of contractor and employee's changes in status.

b. Perform oversight of inherently Governmental and critical functions. See HSAM 3007.5 and DHS Guide on Inherently Governmental and Critical Functions regarding specific requirements.

c. Perform on-going reviews of the functions performed by contractors, especially ways in which work is performed, and the manner in which Government personnel are managing services acquisitions. Reviews should focus on functions that are closely associated with inherently governmental functions and critical functions. In addition, monitor your contract to ensure that the relationships between Government personnel and contractors have not evolved into unauthorized personal services or inherently governmental functions. Also, provide information to the contracting officer in order for them to document the contract file to reflect the results of the on-going review.

6. Non-Delegable Functions and Exclusions

a. As COR you shall not:

i. Make or give the appearance of being able to make commitments, modifications, or other actions which would commit the Government to a change in price, performance, quality, quantity or the delivery schedule;
ii. Provide guidance to the contractor, either orally or in writing, which might be interpreted as a change in the scope or terms of the contract;
iii. Change or modify any of the terms and conditions, or statement of work of a contract, business agreements, or transaction;
iv. Approve items of cost not specifically authorized or increase dollar limits for the contract or business agreement;
v. Take any action with respect to termination, except to notify the contracting officer that action may be necessary and to assist with the process as requested;
vi. Engage in conduct prejudicial to the Government;

vii. Sign contracts or contract modifications;
viii. Solicit proposals;
ix. Direct a contractor (oral or written) to begin work prior to contract award date or notice to proceed, or to stop work;
x. Participate in negotiations with a contractor outside the presence of a contracting officer;
xi. Render a decision on any dispute or question of fact under the Disputes clause of the contract;
xii. Interfere with the contractor's management by supervising contractor employees or otherwise directing their work efforts;
xiii. Specify limitations and include the admonition that the COR may be personally liable for unauthorized commitments; or
xiv. Make any agreement with the Contractor relating to the expenditure of Government funds.

7. FAR and DHS Authorities/Directives, Government Ethics and Training. October 2009 HSAM - Appendix W W-3 HSAM Notice 2013-01

a. FAR and DHS require strict compliance with established standards of conduct and conflict of interest rules.

b. Adherence to applicable requirements for ethics (annual training), procurement integrity, no conflict of interest, and proper standards of conduct, including the identification of regulations (e.g., FAR Part 3, Improper Business Practices and Personal Conflicts of Interests), statutes, or agency directives governing these topics (e.g., 5 CFR Part 2635 Standards of Conduct and Management Directive 0480.1, Ethics/ Standards of Conduct (or any successor directive).

c. Submit disclosure reports, such as the OGE 450, Confidential Financial Disclosure Report, via the appropriate confidential report system.

d. Use of authority for appointment letter is "Pursuant to the Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulation (HSAR).

8. Federal Acquisition Certification Requirements

a. Based on the technical and administrative characteristics of this task order, I have determined that the COR must possess a Federal Acquisition Certification (FAC) for CORs Level II. Your appointment as COR is based on the training, experience, certification, and other qualifications cited in your nomination letter. It is your responsibility to maintain your certification and/or qualifications for COR on this task order, including completing continuous learning points. If you fail to maintain your FAC COR certification at this level, DHS is prohibited by law from paying you for performing COR functions.

b. Adherence to DHS Annual Skills Currency to maintain COR certification and any special instructions for obtaining training, to include ethics or other relevant training.

c. The responsibilities and exclusions set forth in this document are not intended to be all encompassing. As a COR, you are required to consult with the contracting officer when there are questions on your authority. You are not authorized to re-delegate your authority. Violation or misuse of your authority could result in abuse of DHS policy and resources at a minimum or

monetary loss to the COR or firm involved, disciplinary actions, and other measures, depending on the extent of the offense.

9. Contract File Content and Maintenance

a. Instruction for contract file content is in accordance with Component and Contracting Officer's instructions.

b. If you have any questions or problems, please contact the Contract Specialist, (b)(6);(b)(7)(C) or 202-732-(b)(6) or the Contracting Officer, (b)(6);(b)(7)(C) or 202-732-(b)(6);

10. Appointment Effective Date and Termination Date

a. Your appointment as the COR under the above numbered task order is effective upon receipt of this Appointment Letter. The termination date is effective upon receipt of a written notice of termination from the Contracting Officer, a successor to the Contracting Officer, or a higher level of authority.

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)
Contracting Officer

Signature

6/13/13
Date

11. Acknowledgement of Receipt and Acceptance of Appointment

a. Please acknowledge receipt and acceptance of this appointment by signing and returning this acknowledgement section to the Contracting Officer or Contract Specialist.

b. I understand and accept my appointment as the COR under Task Order HSCETC-13-F-00030 with Palantir Technologies Inc for FALCON Operations and Maintenance (O&M) Support Services as outlined above.

(b)(6);(b)(7)(C)
COR

Signature

Date