Privacy Impact Assessment
for the

SharePoint Matter Tracking Systems

DHS/ICE/PIA-043

July 9, 2015

Contact Point
Lyn Rahilly
Privacy Officer
Immigration and Customs Enforcement
(202) 732-3300

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Immigration and Customs Enforcement (ICE) uses SharePoint as a matter tracking solution, allowing ICE program offices that do not have other matter tracking systems to more effectively manage the receipt, creation, assignment, tracking, and archiving of agency matters. The ICE SharePoint environment provides offices the ability to quickly and electronically meet their matter tracking business needs through the use of document, workflow, form, and records management as well as reporting, auditing, and organizational capabilities. In the interest of transparency to the public, ICE is conducting this Privacy Impact Assessment (PIA) to assess the privacy risk of SharePoint as a matter tracking tool. In order to ensure that this method of matter tracking does not erode privacy protections, ICE has developed and implemented processes that give effect to the Fair Information Practice Principles (FIPPs) while improving office efficiency, records management, and exchange of information. Lastly, the appendices to this PIA delineate ICE SharePoint systems used for matter tracking, which will be updated as new systems are deployed or changes to current systems take place.

Introduction

As the principal investigative arm of the Department of Homeland Security (DHS), ICE engages in criminal, civil, and administrative law enforcement as well as non-law enforcement activities. In support of the ICE mission, program offices must be able to effectively manage information and workflows, including the receipt, creation, distribution, tracking, and archiving of tasks, assignments, inquiries, and other correspondence or data (hereinafter referred to as "matter tracking") in a manner that is tailored to specific needs and requirements. ICE's agency-wide need for a more functional and secure matter tracking tool has recently increased amid a transition away from alternative methods, such as email or shared drive-based solutions or other more rudimentary database management systems. As a result, ICE will use Microsoft SharePoint as a tool available when program offices do not have other existing matter tracking or case management systems (*e.g.*, Enforcement Integrated Database (EID), Alien Criminal Response Information Management System (ACRIMe)).[1]

SharePoint is a commercial off-the-shelf (COTS) web-based application that provides a platform on which to build custom applications and features a suite of collaboration, document management, and communication tools, as well as a high degree of integration with other Microsoft Office products. SharePoint automates the matter tracking process, eliminating or reducing the need to manually track emails and manage paper-based documents and forms, and promotes a more efficient means of sharing, storing, searching, and reporting on agency information. Used as a matter tracking tool, the SharePoint platform enables secure data entry, standardizes the display of information, and supports data management and analysis by ICE personnel.

[1] *See* DHS/ICE/PIA-015 Enforcement Integrated Database and DHS/ICE/PIA-020 Alien Criminal Response Information Management System (ACRIMe) PIAs, *available at* www.dhs.gov/privacy.

ICE is conducting this PIA to provide information on the agency's use of SharePoint as a matter tracking tool, addressing SharePoint capabilities, broad categories of information that may be maintained in ICE's SharePoint matter tracking systems, sources from which information is collected or derived, and safeguards implemented in the SharePoint environment to mitigate privacy risks. In addition, this PIA uses FIPPs to evaluate SharePoint's privacy risks. Lastly, the appendices to this PIA list ICE matter tracking systems that use the SharePoint platform and describe the specific types of data maintained, purpose and use, access, individuals affected, sources of information, records retention, and System of Records Notice (SORN) coverage for each system. The appendices will be updated as new matter tracking systems are deployed or as changes to current systems take place.

SharePoint Capabilities

Although SharePoint is often used for document repository and team collaboration sites, ICE business owners have expanded their use of the product to include broader capabilities and enhanced functionality. The following provides a general description of ICE's use of SharePoint capabilities for matter tracking purposes:

- Forms management: Customized forms can be created within SharePoint so that the information gathered in the form can be stored in a SharePoint list or library for organization and analysis of data. These forms can access and display data from multiple sources and provide interactive features to aid in the collaboration and organization of information.
- Records management: SharePoint provides a method for systems to automatically archive or expire content based on criteria set forth by the business owner. For example, a system could delete items from a list if the items are labeled as "Status = Closed" and the items are greater than three years old. Similarly, SharePoint can move items to a separate archive list when they are better suited for long term retention.
- Reporting capabilities: SharePoint's suite of reporting tools offers reporting and business intelligence solutions while eliminating the need for writing custom code. These tools can be used on specific SharePoint systems so that users can run regular or ad hoc reports that suit their business needs. For example, reporting through SharePoint can be used to manage employee workloads, manage budgets, align resources with operational needs, or perform other trend-based or statistical reporting.
- Auditing capabilities: SharePoint automatically stores information on the identity of system users and logs the actions users take while navigating throughout the environment. Tools, such as version history, can be used on SharePoint pages, lists, or libraries to determine whether any changes were made, which user made the changes, and when the user made the changes.

- Microsoft Office Integration: SharePoint ties in very closely with Office products in an effort to bring some of the native capabilities of certain Office products into SharePoint sites and pages. For example, Excel Services provides the ability to present data from an Excel spreadsheet on a SharePoint page or leverage Excel data in a SharePoint list for manipulating data. This functionality can also help to present charts and graphs from Excel in SharePoint, which are automatically updated based on data changes that are made real time.

Categories of Information

ICE uses SharePoint to serve law enforcement and non-law enforcement purposes related to the agency's mission. Therefore, any ICE matter tracking system built on the SharePoint platform may include a variety of information about ICE or DHS employees, contractors, and members of the public. The specific information collected will depend on the nature and business process of the particular activity, project, or program that the matter tracking system is being used to support.

SharePoint matter tracking systems may be used to support the tracking of law enforcement activities within the scope of ICE enforcement authorities (*e.g.*, national security, customs violations, immigration benefits fraud, human smuggling, human rights violations, and gang investigations). The types of individuals on whom information is collected in these contexts varies on a case-by-case basis, but may include subjects of investigations, witnesses, victims, business associates, customers, relatives, or others whose information is collected during the course of a law enforcement investigation or activity.

SharePoint matter tracking systems used in support of non-law enforcement, administrative, or programmatic activities reduce ICE's reliance on paper records or other more rudimentary electronic systems and to make agency records accessible and searchable through electronic means. These systems may contain information that pertains solely to ICE or DHS personnel or may include information about members of the public.

This PIA covers different types personally identifiable information (PII), including employee and contractor contact information, as well as Sensitive PII, such as Social Security numbers, Alien Registration Numbers (A-Number), immigration information, criminal history information, medical information, and financial data. The SharePoint environment is not authorized to house classified, secret, or top secret information.

Sources of Information

Information contained within matter tracking systems is obtained from various sources by ICE personnel. Similar to the variances in categories of information, sources of information depend on the nature and business process of the particular activity, project, or program for which the system is used. Information may be collected directly from the individual or third

parties, or derived from other sources (*i.e.*, other paper-based or electronic systems).

Other sources of information include other ICE offices, DHS Headquarters and Components, other government agencies, Congress, the White House, nongovernmental organizations, and members of the public. The sources of information may or may not be reflected in the program office's matter tracking system. However, at a minimum, the sources are documented in the SORN[2] relative to the matter tracking system.

Privacy Safeguards

ICE has built safeguards into the SharePoint environment to help mitigate privacy risks (e.g., data spills, misuse of information, and unauthorized access). Each matter tracking system is equipped with visual cues, oversight mechanisms, and access controls:

- Visual cues: Templates are implemented on all systems that include visual cues as to whether Sensitive PII is authorized for posting in the system. Visual cues are described in additional detail in section 3 below.
- Oversight: All matter tracking systems have a designated point-of-contact (POC) who is responsible for determining the system's user base and ensuring that the system is used only for approved purposes. POCs are required to attend training and sign an agreement acknowledging understanding of the use of Sensitive PII in the ICE SharePoint environment. POCs are responsible for ensuring that users understand whether their system is authorized to contain Sensitive PII. When an inappropriate posting of Sensitive PII is found, POCs will ensure its immediate removal from the matter tracking system and report the posting as a privacy incident.
- Access controls: Role-based permissions are applied to all ICE matter tracking systems – from the system as a whole, down to individual files or items contained in the system. For systems that are authorized to contain Sensitive PII, POCs must ensure that only users with a verifiable need-to-know are granted access privileges to the information. Additional information about access controls is included in sections 4 and 7 below.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222 of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in

[2] All ICE SORNs are published in the *Federal Register* and on the DHS Privacy Office website at http://www.dhs.gov/system-records-notices-sorns.

the Privacy Act of 1974 and shall assure that technology sustains and does not erode privacy (*see* 6 U.S.C. § 142(a)(2)).

In response to this obligation, the DHS Privacy Office developed a set of FIPPs from the underlying concepts of the Privacy Act, which encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure. Given the particular technology and the scope and nature of its use, ICE conducted this PIA as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Information maintained in ICE SharePoint matter tracking systems will depend on the particular business processes for which the systems are established. Matter tracking systems serve law enforcement and non-law enforcement purposes related to ICE's mission; therefore, systems may include a variety of information from or about the public.

When possible and appropriate, ICE provides notice to individuals about the collection and use of their information. For example, individuals who call the Enforcement and Removal Operations (ERO) Detention Reporting and Information Line (DRIL) hear a brief message alerting them that their personal information may be collected in order for ICE to handle the matter about which they are calling. ERO DRIL enters information they collect directly into its SharePoint matter tracking system. Other ICE offices that do not collect information directly from an individual (*i.e.*, a third party) or use data derived from other sources (*i.e.*, other paper-based or electronic systems) or information collections are unable to provide notice. In these instances, the program office relies on the entity that engaged in the initial information collection to provide notice.

Matter tracking systems that contain PII are governed by the SORN and used in accordance with the purpose(s) enumerated in the SORN. The relevant SORN as well as this PIA also provide notice to the public about ICE's collection, use, and dissemination of their information. For each matter tracking system identified in the appendices, the relevant SORN is listed.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Individuals may access information collected and maintained by ICE through the Privacy Act and the Freedom of Information Act (FOIA)[3] processes. Individuals seeking notification of, access to, or correction of any record contained in a matter tracking system covered under this PIA, may submit a request in writing to ICE FOIA Officer, by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(866) 633-1182
http://www.ice.gov/foia/

Depending on the purpose and information contained in the matter tracking system, all or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Generally, ICE uses SharePoint matter tracking systems to track, manage, review, and report on matters related to its law enforcement and non-law enforcement activities. The specific purpose of the system and the use of the information maintained within depend on the nature of the program office and the business process for which the system is established.

Systems that contain PII are used in accordance with the purpose(s) enumerated in their relevant SORN. SORN coverage for the collection, use, and dissemination of the information is determined through the completion of a Privacy Threshold Analysis (PTA) and/or a SharePoint Matter Tracking System Template listed in Appendix A of this PIA.

All SharePoint matter tracking systems display visual cues indicating whether Sensitive PII is authorized to be posted on the system. There is slight variation with the visual cues implemented on different ICE program office systems.

For program offices in ICE ERO, Management & Administration (M&A), and the Office of the Director (OD), the visual cues are as follows:

- Sensitive PII-authorized system:

[3] See 5 U.S.C. § 552.

- Header on each page of the system that states "Notice: Sensitive PII is allowed on this site!" in green.
- Green banner fixed on the bottom of each page of the system that states "Notice: Sensitive PII is allowed on this site!" and includes a link to a privacy statement, explaining that the posting of Sensitive PII is authorized in the system.

- Sensitive PII not-authorized system:
  - Header on each page of the system that states "Warning: Sensitive PII NOT allowed on this site!" in red.
  - Red banner fixed on the bottom of each page of the system that states "Warning: Sensitive PII NOT allowed on this site!" and includes a link to a privacy statement, explaining that the posting of Sensitive PII is not authorized on the system. This link also explains the proper steps to take in the event that Sensitive PII is posted in the system.

For program offices in ICE Homeland Security Investigations (HSI), the visual cues are as follows:

- Sensitive PII-authorized system:
  - Green banner fixed on the bottom of each page of the system that states "Notice: Sensitive PII is AUTHORIZED on this site!"
  - Banner also includes a link to a privacy statement, explaining that the posting of Sensitive PII is authorized in the system.
- Sensitive PII not-authorized system:
  - Red banner fixed on the bottom of each page of the system that states "Notice: Sensitive PII is NOT ALLOWED on this site!"
  - Banner also includes a link to a privacy statement, explaining that the posting of Sensitive PII is not authorized in the system. This link also explains the proper steps to take in the event that Sensitive PII is posted in the system.

All SharePoint matter tracking systems also clearly display the name of the POC so users may contact the POC in the event that Sensitive PII is posted in systems that are not authorized to host Sensitive PII or Sensitive PII is improperly restricted on sites that are authorized to host Sensitive PII and is accessible to those without a need-to-know.

For each matter tracking system identified in the appendices, the purpose and use are described.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Using SharePoint for matter tracking provides a more secure platform for and more sophisticated access controls to the data contained within the systems. SharePoint supports access controls specific to each matter tracking system, depending on the business process for which the system is created and the sensitivity of the information stored within it. These controls are placed on the system as a whole, as well as specific files and items contained in the system so that only users with a need-to-know have access to the data. Alternative methods, such as email or shared drive-based solutions or other more rudimentary database management systems, do not typically provide such controls.

Records retention and disposition in matter tracking systems varies by the type of record collected. SharePoint provides a method for systems to automatically archive or expire content based on criteria set forth by the business owner. Any time a business owner requests this type of functionality, the criteria for retaining the respective information housed in the system is documented and maintained by the ICE SharePoint development teams.

For each matter tracking system identified in the appendices, the information collected is assessed against the purpose of the system prior to inclusion in this PIA. System purpose and use, data elements, access controls, and records retention are described in the appendices.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

ICE uses data for purposes related to matter tracking in furtherance of the ICE mission. The specific purpose of each matter tracking system is defined prior to the creation of the system. ICE POCs are responsible for determining the system requirements and user base and, once the system is created, ensuring that it is used only for approved purposes.

Through the use of SharePoint, the proliferation of data is limited. The SharePoint environment allows for data consolidation and eliminates or reduces the need for ICE program offices to retain both paper and electronic copies of documents or multiple electronic copies in more rudimentary database management systems.

Matter tracking systems are not made available to external entities, and data stored in the systems is not directly accessible by users or computer systems outside the ICE network. Any external sharing of information contained within a SharePoint application is made

pursuant to the Privacy Act.[4] For each matter tracking system identified in the appendices, the purpose and use are described and the relevant SORN is listed.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Information that is collected and stored in matter tracking systems will generally not be systematically checked for accuracy and timeliness. However, information that ICE uses as part of its law enforcement and non-law enforcement activities will be reviewed for accuracy as required by the particular activity and the laws and authorities, if any, applicable at the time the agency collects the records.

In some cases, information contained within matter tracking systems for law enforcement purposes may be known to be inaccurate. For example, records related to a fraud investigation may contain false or fictitious information. Nonetheless, maintenance of these records in a matter tracking system is necessary to support the investigation. Records pertaining to law enforcement activities may contain knowingly inaccurate information in addition to accurate PII, and must be maintained for the purposes of the particular activity.

The ICE employee or contractor entering the information into the matter tracking system is initially responsible for the accuracy of information. In general, the POC or administrative users will review incoming information, and any inconsistencies will be corrected by contacting the submitting employee or contractor. In addition, program offices may implement methods of ensuring accuracy on a system-by-system basis.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

All ICE matter tracking systems are internal-facing. Users must have access to the ICE network to gain access to systems. Only authorized users required to perform the stated purpose of the system will be granted rights to access and post data in the system; this access will be limited to a need-to-know basis. ICE establishes access controls for each matter tracking system created based the business process for which it is created and the sensitivity of the information stored within it. POCs are trained on how to use SharePoint's access controls, on a group or user-level, to systems, document libraries, and specific documents and items.

ICE personnel can gain access to a SharePoint system only after a business owner, POC, or site manager approves a particular user's access. The site manager program allows members of ICE organizational entities to gain a higher level of permissions to the ICE

[4] *See* 5 U.S.C. § 552a(b).

SharePoint environment upon successful completion of an exam and adherence to posted guidelines and rules of conduct. Site managers have additional permissions that allow them to make data and user-based modifications to a specific site they have been granted permission to manage. The ICE SharePoint development teams keep records of all site manager nominations as well as where these individuals have increased levels of permissions within the environment. For each matter tracking system identified in the appendices, the access controls are described.

In the event of a data incident – including misuse of data, unauthorized access to a SharePoint application, unauthorized posting of Sensitive PII, and inappropriate disclosure of Sensitive PII from the application – the incident will be reported and handled as a privacy incident. For cases in which misconduct is suspected, the incident will be reported to the ICE Office of Professional Responsibility for further investigation.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

SharePoint automatically stores information on the identity of system users and logs the actions users take while navigating through the environment. Tools, such as version history, provide visibility into where, when, and by whom changes are made in SharePoint pages, lists, and libraries. If more in depth tracing is necessary, the ICE SharePoint teams can reference the detailed audit logs to determine when and who performed actions within SharePoint.

The ICE Privacy and Records Office, in coordination with the ICE SharePoint development teams, trains all POCs on the privacy protocols associated with the use of SharePoint. POCs are also made aware of their responsibility to train users and that they are accountable for the actions of their users. Attendance at this training is mandatory before a program is provisioned a system that is authorized to contain Sensitive PII.

In addition, all ICE personnel are required to complete a SharePoint privacy training that discusses Sensitive PII, posting documents and information, and SharePoint auditing. Users are informed that their POCs will provide more detailed training on their specific SharePoint system and the information it can and cannot contain. Personnel are also required to complete annual security and privacy training, which emphasizes SharePoint best practices along with the DHS Rules of Behavior and other legal and policy restrictions on user behavior.

Responsible Officials

Lyn Rahilly, Privacy Officer

U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDICES

Appendix A – SharePoint Matter Tracking System Template

Program/System:

List the name of the agency, program office, and SharePoint matter tracking system.

Purpose and Use:

Provide a general description of the program/system and its purpose, including how the purpose of the program/system relates to ICE's mission and how the system operates/business process.

System Access:

Provide a general description of who has access to the system.

Individuals Impacted:

Provide a list of individuals (i.e., members of the public) whose information will be contained in the system.

Sources of Information:

Provide the sources from which information maintained in the system is derived.

Data Elements:

Provide a specific description of information that may be collected, maintained, and/or generated by the system. Highlight any collection and maintenance of PII and Sensitive PII.

SORN Coverage:

List the SORN(s) under which this data collection and maintenance is covered.

Records Retention Period:

List the retention period(s) for records maintained in the system.

Appendix B

Program/System:

ICE Enforcement and Removal Operations (ERO) Custody Programs Division (CP) Detention Reporting and Information Line (DRIL) Custody Assistance and Inquiry Resolution System (CAIRS)

Purpose and Use:

ERO CP operates the Detention Reporting and Information Line (DRIL) in an effort to resolve community-identified problems or concerns with ICE immigration and detention policies and operations. DRIL operators are responsible for answering inquiries (questions, requests, and complaints) sent to ICE via phone calls to the DRIL and emails to ERO CP's public email box. The majority of calls to the DRIL come from ICE detainees and involve immigration case information inquires, medical or mental health complaints, and parental or family-separation issues. After receiving an inquiry, DRIL operators may also coordinate any necessary follow-up with ERO CP's liaisons in ERO field offices and other select ICE program offices.

To manage information received during a DRIL call or in an email, CP uses the SharePoint-based Custody Assistance and Inquiry Resolution System (CAIRS). DRIL operators enter information received during the inquiry into forms built within CAIRS. After a supervisor reviews this information, operators can generate emails within the system that are sent to the appropriate ERO field office or other ICE office for real-time and priority-based actions. Once the office reviews and resolves the CAIRS referral, the designated CP liaison adds the referral disposition and closes the CAIRS entry.

CAIRS also provides a robust archival process, enabling DRIL operators to review historical notes related to previous inquiries associated with a particular Alien Registration Number (A-Number). DRIL operators can search for archived entries using an A-Number or a CAIRS-generated tracking number.

Finally, CAIRS is used to track calls pertaining to the ICE Victims of Immigration Crime Engagement (VOICE) Office. VOICE, established in 2017, supports victims of crimes committed by removable aliens through access to information and resources.[5] As part of that support, DRIL operators perform the following functions:

- Provide general information about the VOICE Office;
- Provide information about the Department of Homeland Security Victim Information Notification Exchange (DHS-VINE);[6]
- Disclose alien custody status updates to individuals eligible to receive such information; and
- Refer callers to victim service organizations.

When DRIL operators receive calls from victims or their agents (including family members,

[5] The VOICE Office was established pursuant to Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*, available at https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[6] *See* DHS/ICE/PIA-047 DHS Victim Information and Notification Exchange, *available at*: www.dhs.gov/privacy.

friends, legal representatives, or others acting at the victim's request), they record the caller's information in CAIRS. The information collected may include the caller's name, organization name (if applicable), address, phone number, and email address. The caller may also provide information pertaining to aliens, such as the alien's name, A-Number, date of birth, country of birth, and date of entry. Finally, any information the caller provides that would assist in identifying the alien or in resolving the inquiry may be recorded. All of this information is entered in CAIRS.

Depending on the inquiry, ICE may have to follow up with the caller at a later time via phone or email. In that case, DRIL operators will send an email to ERO Community Relations Officers (CROs) for follow-up action. CROs will also have access to the CAIRS database to update information from calls, and to indicate any actions taken to resolve the inquiry.

System Access:

Access to CAIRS is granted to DRIL operators, the CP chain of command, and CP liaisons in ERO field offices and other select ICE program offices.

Individuals Impacted:

Individuals who submit inquiries to the DRIL; individuals victims of crimes committed by removable aliens and agents of the victim (e.g., family members, friends, legal representatives); individuals who are the subjects of inquiries, including individuals arrested, encountered, or detained by ICE or held in ICE custody pending removal or removal proceedings under the Immigration and Nationality Act (INA).

Sources of Information:

Information within CAIRS may be collected directly from the individuals submitting inquiries through the DRIL. Additional information about a specific individual who has been arrested, encountered, or detained by ICE or held in ICE custody pending removal or removal proceedings under the INA may be inputted into CAIRS from ICE's EARM. Finally, information may also be collected by CROs who use CAIRS to update information on inquiries pertaining to the VOICE office.

Data Elements:

CAIRS will automatically assign all incoming calls, voicemails, and emails a unique tracking number, consisting of the date and a running call-count number. In addition, CAIRS will collect information on:

- The category of the inquirer (e.g., detainee, attorney of detainee, family member of detainee, advocate, member of the general public) and identifying information, including full name, organization name (if any), email, and phone number;
- Identifying information pertaining to the detainee, if the detainee is not the inquirer, specifically: full name, date of birth, country of birth, A-Number (if any), full mailing address, whether the person is in a detention facility and where, email address, and phone number; and

- The nature and description of the inquiry (e.g., general outreach inquiry, detention concern, enforcement issue, facilitation of return, national policy concern, VOICE,[7] or general information request).

SORN Coverage:

DHS/ALL-016 Department of Homeland Security Correspondence Records[8]

Records Retention Period:

ICE has submitted a proposed records retention schedule to the National Archives and Records Administration (NARA) for approval to retain CAIRS records for seven years after the record was entered into the system.

[7] There is a dropdown menu within CAIRS where DRIL operators can select the type of call received. VOICE is one of those options.
[8] DHS/ALL-016 Department of Homeland Security Correspondence Records, 73 FR 66657 (Nov. 10, 2008).

Appendix C

Program/System:

ICE Enforcement and Removal Operations (ERO) Segregation Review Management System (SRMS)

Purpose and Use:

ERO uses the Segregation Review Management System (SRMS), to track, review, and oversee ICE detainee segregation cases. Segregation – whether administrative or disciplinary – is the process of removing a detainee from the general detainee population into a separate, individual unit.

ERO field office personnel input information pertaining to a detainee's segregation case directly into the SharePoint based-SRMS. This input, and any subsequent inputs pertaining to the same detainee, comprise the detainee's segregation case within the system. The field office can update the case at any time to reflect changes in the segregation status, including removal from segregation. Within SRMS, ERO can sort and manage cases by priority, facilitate subject matter expert (SME) review of cases, and notify field office leadership and detention facility staff of actions affecting the segregation status of a detainee.

SRMS also provides an archival process, enabling ERO to determine and report on trends related to segregation practices and inquire into specific segregation cases. ERO users search for archived entries by A-Number or SRMS-generated case tracking number.

System Access:

Access to SRMS is granted to ERO field office leadership and their staff assigned to segregation management, the Segregation Review Coordinator and administrative support staff, SMEs subject matter experts from select ICE program offices, and select ICE Headquarters staff involved in segregation review. SRMS displays data in user-specific views, so the user has most immediate access to case information most relevant to him or her.

Individuals Impacted:

Individuals in ICE detention who are placed into administrative or disciplinary segregation.

Sources of Information:

SRMS receives information from ERO detention facility staff and from ICE's ENFORCE Alien Removal Module (EARM). Case notes from field office personnel or medical personnel may also be included in SRMS.

Data Elements:

SRMS automatically assigns a unique case reference number for all segregation cases submitted by field offices. In addition, information collected and stored within SRMS includes:

- Identifying information pertaining to the detainee, including full name, A-Number, language and language proficiency, and detention facility housed in at the time.

- Information determined to be relevant to the segregation decision, including type of segregation (i.e., administrative or disciplinary); reasons for the placement in segregation (i.e., conduct/behavior, heightened concern for a detainee's risk of victimization, or other special vulnerabilities); existing medical and mental conditions; and criminal, disciplinary, and immigration history.
- Information pertaining to ICE oversight and review of individual segregation cases, including data on dates of initial segregation and release from segregation, interviews with facility or medical staff, case review dates, analyses by SMEs, and decisions for field action (e.g., limit isolation, transfer to different facility, return to general population).

SORN Coverage:

DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE)[9]

Records Retention Period:

ICE intends to request NARA approval to retain SRMS records for seven years after the record was entered into the system.

[9] DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE), 80 FR 24269 (Apr. 30, 2015).

Appendix D

Program/System:

ICE Office of the Director AWARDS System

Purpose and Use:

The ICE Office of the Director uses the AWARDS system to accept and manage nominations for the annual ICE Director's Awards Ceremony in Washington, D.C. The nomination process, previously captured on electronic and paper-based spreadsheets, is automated and streamlined through AWARDS.

Select staff from the Director's Office, the ICE Office of Professional Responsibility, and the ICE Human Capital Office review nominations submitted through the AWARDS system. Some nominees are ultimately selected to receive an award from the ICE Director. ICE also conducts the review and selection process using the AWARDS system.

System Access:

AWARDS coordinators in each ICE program office and select Director's Office staff can access AWARDS.

Individuals Impacted:

Individuals who are nominated for an ICE Director's Award as well as officials, guests, and attendees of the annual Awards Ceremony.

Sources of Information:

Information within AWARDS may be collected directly from the individuals who are nominated for ICE Director's Awards as well as from individuals who submit nominations on behalf of others.

Data Elements:

The information maintained in the AWARDS system includes:

- Full names of nominees, officials, guests, and attendees of the Awards Ceremony.
- Contact information, including email addresses, phone numbers, and work addresses.
- Job-related information, including job title, program office name, and ICE network login username.

SORN Coverage:

- DHS/ALL-002 Department of Homeland Security Mailing and Other Lists System;[10] and
- DHS/ALL-004 General Information Technology Access Account Records System[11]

Records Retention Period:

[10] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (Nov. 25, 2008).
[11] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).

Nomination records in AWARDS are retained for two years pursuant to NARA General Records Schedule 1, Item 12. Lists of nominees, officials, guests, and attendees at awards ceremonies will be destroyed when superseded by the following year's list.

Appendix E

Program/System:

Homeland Security Investigations Field Office Workflow SharePoint

Purpose and Use:

Some HSI Field Offices are developing Microsoft SharePoint portals to gather, store, and disseminate essential agency resources, guidance, processes, and communication. The primary purpose for the SharePoint sites will be to upload high-level documents that require approval by agency supervisors. A few document libraries may contain official agency correspondence and forms (Agency Letters, Claims for Reimbursement of Business Expense, Foreign Travel Authorizations Requests, State and Local Over-Time Reimbursements, Subpoenas, Summons, etc.). The agency forms may contain PII and/or Sensitive PII about members of the public and ICE employees. Sensitive PII in these libraries is collected by existing ICE source systems and is accounted for in the privacy documentation of those systems. For example, if an agent needed a subpoena approved by a supervisor the document would be generated from the ICE Subpoena System[12] (ISS) and loaded onto the SharePoint site for the agent's field office. The authorized uses, safeguarding, and retention policies that govern records in ISS will govern the handling of the individual subpoena in SharePoint.

System Access:

Permissions-based access to subsites and libraries containing Sensitive PII will be restricted to agency supervisors and SharePoint site administrators only. Permissions-based access to subsites and libraries that do not contain Sensitive PII (either from ICE employees or members of the public) will be restricted to ICE employees with a verified need to know. Agency-vetted counterparts (e.g., task force officers) will be able to view administrative and mission support approval requests. ICE employees are advised not to provide Sensitive PII for administrative approvals.

Individuals Impacted:

HSI field personnel involved in creating administrative and investigative requests requiring approval by agency supervisors; and members of the public who are the subject of HSI investigations.

Sources of Information:

No other system is connected to the HSI Field Office SharePoint sites. Information is gathered directly from HSI field office personnel who create and upload documents requiring supervisor approval. HSI employees may derive information from case management systems

[12] *See* DHS/ICE/PIA-027 ICE Subpoena System, *available at* www.dhs.gov/privacy.

like the Investigative Case Management System (ICM)[13] or documents may be manually downloaded from systems like the ICE Subpoena System and uploaded to the site.

Data Elements:

Documents posted to a SharePoint approvals library may contain PII about members of the public, including, but not limited to: names, biographical information, identification document information (driver's licenses or passport numbers), status information, and criminal history information. All such information comes from programs and systems (e.g., the ICE Subpoena System) that are covered by separate privacy documentation. Information about HSI employees includes: name, employment information (office, group, position, and supervisor), and contact information (office location, phone numbers, and email addresses).

SORN Coverage:

HSI Field Office Workflow SharePoint sites do not retrieve file information by a personal identifier, and therefore do not require SORN coverage.

Records Retention Period:

HSI will only keep documents on the SharePoint sites as long as there is a business need. SharePoint administrators actively audit the sites to ensure outdated documents or information is deleted from SharePoint. All finalized documents will be uploaded into their source systems, which will be governed by separate record retention schedules.

[13] *See* DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), *available at* www.dhs.gov/privacy.

Appendix F

Program/System:

ICE Homeland Security Investigations (HSI) Forensic Interview Program (FIP)

Purpose and Use:

HSI uses the Forensic Interview Program (FIP) SharePoint Site to track information related to forensic interviews and other services FIP provides. Forensic interviews are investigative interviews of certain victims of crimes that HSI investigates, including United States Citizens, Lawful Permanent Residents, and aliens. FIP is used primarily, though not exclusively, in cases of child exploitation, human trafficking, traveling sex offenders, and human rights violations. FIP, which is a component of the HSI Victim Assistance Program, receives referrals to conduct forensic interviews from HSI Special Agents when they believe that they have identified or will identify victims during the course of a criminal investigation who will require FIP services. PII about victims is only ingested into the FIP SharePoint site once the victim has been identified.

Forensic Interview Specialists are trained to conduct forensic interviews to further an investigation. Forensic Interview Specialists will input case referral data, forensic interview data, and other associated data directly into fields on the FIP SharePoint site, which will then create a list of data entries within the site.

In addition to conducting forensic interviews, Forensic Interview Specialists assist Special Agents with operational planning, case consultations, and the Child Pornography Victim Notification process.[14] The FIP SharePoint Site allows HSI Forensic Interview Specialists to efficiently track referrals and forensic interviews conducted of victims, cross check to ensure that duplicate interviews are not being conducted, and keep accurate statistics regarding the Forensic Interview Program. Forensic Interview Specialists also use the FIP SharePoint to facilitate the Child Pornography Victim Notification process by linking victim information with HSI case agent/field office information and contacting the appropriate HSI case agent/field office to determine whether the victim wants to continue receiving notifications.

System Access:

Only DHS employees and contractors assigned to the FIP (including FIP leadership) with a need to know will have access to the SharePoint site. All users with access have full privileges to add information to the site.

Individuals Impacted:

[14] The Child Pornography Victim Notification process is mandated under the Crime Control Act of 1990 (42 U.S.C. § 10607) and the Crime Victims' Rights Act of 2004 (18 U.S.C. § 3771). The process is intended to inform victims and/or guardians of the unique circumstances surrounding child pornography investigations and when victim images may appear again in separate criminal investigations or in court proceedings at the federal, state, and/or local level. Victims and/or guardians may opt-in or opt-out of receiving notifications of when victim images may appear again.

Individuals currently under HSI investigation or who have been charged; the subject of the forensic interview (witness to or victim of the HSI-investigated crime); and the special agent, Forensic Interview Specialist, and any victim assistance specialist to whom the case was referred.

Sources of Information:

Information comes from the Forensic Interview Specialist inputting referral information, forensic interview information, and other associated information directly into fields on the site.

Data Elements:

The site primarily collects information about the forensic interview itself (e.g., the date of referral, type of case, case number, date of forensic interview, forensic interview location, language used in the interview, and case disposition).

The site contains the full name of the HSI Agent assigned to the case, the Forensic Interview Specialist to whom the case was referred, and the Victim Assistance Specialist to whom the case was referred.

The site also contains the target of investigation's full name, as well as the victim's full name, age, date of birth, gender, country of origin, and any victim's services needed (e.g., case consultation, operational planning, forensic interviews, and coordination with local agencies).

SORN Coverage:

DHS/ICE-009-External Investigations[15]

Records Retention Period:

FIP will only keep documents on the SharePoint site as long as there is a business need. Document owners will remove documents when the mission need ends. This includes when a finalized document is uploaded to a different system, a case is closed, or the document or the information contained therein is outdated. SharePoint administrators will be actively auditing the site (i.e., periodically checking the site for old documents, documents created by personnel no longer in the unit, or documents irrelevant to current operations) to ensure outdated documents or information is deleted from SharePoint. There is currently no records schedule for interviews, so records will be treated as permanent until there is an approved NARA records schedule. If any records are included in the investigative case file, those records are retained for twenty (20) years.

[15] DHS/ICE-009 External Investigations System of Records, 75 FR 404 (Jan. 5, 2010).

Appendix G

Program/System:

Sexual Abuse and Assault Prevention and Intervention (SAAPI) Case Management

Purpose and Use:

ICE Enforcement and Removal Operations (ERO) Custody Management, Custody Programs Division (CPD) owns the SAAPI Case Management system. The SAAPI Case Management system promotes compliance with ICE Policy No. 11062.2:[16] Sexual Abuse and Assault Prevention and Intervention (SAAPI) (May 22, 2014), which establishes the responsibilities of ICE detention facility staff and other ICE personnel with respect to prevention, response and intervention, reporting, investigation, and tracking of incidents of sexual abuse or assault. This system facilitates oversight by the ERO CPD, which has primary responsibility under this policy for incident review and reporting.

The primary function of the SAAPI Case Management system is to track the lifecycle of sexual abuse and assault allegations occurring in ICE detention facilities, hold rooms, and other forms of custody. The system is used to input data about incidents and provide transparency to system users about an allegation's status. In addition, the system allows users to follow progress about a particular incident and ensure that ICE policy requirements are being met. Lastly, the data in the system is used for collecting sexual abuse and assault allegation metrics and reporting aggregate sexual abuse and assault allegations.

System Access:

Only designated Prevention of Sexual Assault Coordinators (PSACs) at field offices and ICE Headquarters will receive access, as well as Lead PSACs from the Office of Professional Responsibility (OPR), Office of Detention Policy and Planning, and ERO CPD. These users only have access to case information relevant to their responsibilities.

Individuals Impacted:

Alleged victims of sexual abuse and assault; alleged perpetrators of sexual abuse and assault; witnesses, ICE employees, contractors, and volunteers if there is a nexus to an alleged case of sexual abuse or assault.

Sources of Information:

Information comes from the PSAC inputting all relevant case information into the SharePoint site. Information about relevant segregation cases involving alleged victims and perpetrators is received from the Segregation Review Management System (SRMS).[17] Sexual

[16] *See* ICE Policy No. 11062.2: Sexual Abuse and Assault Prevention and Intervention (SAAPI) (May 22, 2014) at https://www.ice.gov/doclib/detention-reform/pdf/saapi2.pdf.
[17] Segregation Review Management System is covered in a separate appendix within this PIA.

assault and abuse cases are recorded as a daily list in ICE's Significant Event Notification system (SEN),[18] and the daily list is then logged into SAAPI Case Management. SEN's primary function is to notify appropriate stakeholders of basic information around an allegation. SEN reports largely consist of free text fields, which are not conducive to ensuring standardized reports. SAAPI allows a standardized report to be generated and stored (including the end result of the investigation, which is not included in SEN). The detailed information contained in SAAPI is copied and pasted into the SEN report generated for the allegation in the free text field. If any information about an individual involved in an incident is missing, information contained in ICE's ENFORCE Alien Removal Module (EARM)[19] will be used to complete the individual's profile in SAAPI Case Management.

Data Elements:

The site contains information pertaining to the alleged victim and perpetrator, including full name, and as appropriate the Alien File Number (A-Number), country of birth, gender, self-identification as LGBTI, any pertinent disabilities, and primary language spoken.

The site also contains information determined to be relevant to the allegation, reporting timeline, and investigative findings, including description of the alleged incident, responsible investigating party (for example, DHS Office of the Inspector General (OIG), ICE OPR, ERO Administrative Inquiry Unit), sanctions or punishment enforced on the offender (such as segregation, transfer to a different facility, or loss of privileges), and incident details (location, date and time). Witness biographical information will also be captured, including full name and person type (e.g., ICE employee, contractor, volunteer, detainee).

SORN Coverage:

DHS/ICE-009 External Investigations[20] and DHS/ICE-011-Criminal Arrest Records and Immigration Enforcement Records (CARIER)[21]

Records Retention Period:

PSACs will only keep information on the SharePoint site as long as there is a business need. Document owners will remove documents when the mission need ends. This includes when a finalized document is uploaded to a different system, a case is closed, or the document or the information contained therein is outdated. SharePoint administrators will be actively auditing the site (i.e., periodically checking the site for old documents, documents created by personnel no longer in the unit, or documents irrelevant to current operations) to ensure outdated documents or

[18] *See* DHS/ICE/PIA-023 Significant Event Notification System at www.dhs.gov/privacy.
[19] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) at www.dhs.gov/privacy.
[20] DHS/ICE-009 External Investigations System of Records, 75 FR 404 (Jan. 5, 2010).
[21] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016) (previously called ENFORCE).

information is deleted from SharePoint. Information related to sexual assault and abuse investigations are retained for twenty-five (25) years.

Appendix H

Program/System:

Enforcement and Removal Operations (ERO) Removal Division SharePoint Site

Purpose and Use:

The ICE Enforcement and Removal Operations (ERO) Removal Division (RD) removes from the United States aliens who are subject to a final order of removal issued by an immigration court or following an administrative removability review. To assist in fulfilling its mission, RD has created a SharePoint site to store documents and track the progress of removal cases. RD consists of the Removal Management Division (RMD), the ICE Air Operations Division (IAO), and the International Operations Division (IOD). In addition to a home page, each division has its own page on the SharePoint site. RD also developed a separate page specifically to track removals of Cuban citizens. All pages on the ERO Removal Division SharePoint site contain repositories of internal documentation relating to the RD workflows as well as official documents related to the removal of aliens. Documents on this site include historical documents, broadcast messages, taskers, correspondence, meeting details, deferred action requests, travel document logs, RMD case logs, assignments, briefing materials, and case materials for Cuba removals.

System Access:

The SharePoint site is only accessible to authorized ICE employees who work to carry out or support the ERO Removal Division mission. ICE shares information from the Cuba Page with a Field Office Director (FOD) from United States Citizenship and Immigration Services (USCIS), but USCIS personnel do not have access to the site itself.

Individuals Impacted:

ERO personnel involved in creating and handling RD cases and administrative documents, other federal employees and contractors involved in cases covered by RD (including USCIS personnel), and members of the public who are aliens involved in removal proceedings.

Sources of Information:

No other system is connected to the ERO Removal Division SharePoint site. Information is gathered directly from RD personnel who create and upload documents requiring supervisor approval. RD employees may derive information from case management systems like the Enforcement Integrated Database (EID).[22]

Data Elements:

[22] *See* DHS/ICE/PIA-015 Enforcement Integrated Database, *available at* www.dhs.gov/privacy.

Documents posted to a SharePoint library may contain PII about members of the public, including: names, A-Number, biographical information, identification document information (driver's licenses or passport numbers), and immigration information. Information about ICE employees is limited to name and job title. Information about employees from other agencies is likewise limited to name and job title.

SORN Coverage:

DHS/ICE 011-Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN[23]

Records Retention Period:

ERO will only keep documents on the SharePoint site as long as there is a business need. Document owners will remove documents when the mission need ends. This includes when a finalized document is uploaded to a different system, a case is closed, or the document or the information contained therein is outdated. SharePoint administrators will be actively auditing the site (i.e., periodically checking the site for old documents, documents created by personnel no longer in the unit, or documents irrelevant to current operations) to ensure outdated documents or information is deleted from SharePoint. All finalized documents will be uploaded into their source systems, which will be governed by separate record retention schedules.

[23] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016) (previously called ENFORCE).

Appendix I

Program/System:

National Security Investigations Division (NSID) SharePoint

Purpose and Use:

NSID is a division within ICE Homeland Security Investigations (HSI) directorate that is dedicated to investigating vulnerabilities in the nation's border, infrastructure, economic systems, and transportation systems. NSID also prevents terrorism by targeting the money and materials that support criminal activities. It oversees the Operational Support Group (OSG), Counterterrorism and Criminal Exploitation Unit (CTCEU), Human Rights Violators and War Crimes Unit (HRVWCU), National Security Unit (NSU), National Security Liaisons, and the Student and Exchange Visitor Program. NSID units and sections participating in the NSID SharePoint are the OSG, NSU, CTCEU, and HRVWCU.

OSG provides mission support to all NSID units in various capacities including personnel, budget, property management, and facilities management. NSU oversees the national security investigations and counterterrorism efforts for the NSID, moderates HSI participation in the Joint Terrorism Task Force (JTTF) that ICE operates with the FBI, and works closely with other non-DHS agencies in the counterterrorism mission. NSU includes the Counterterrorism Section (CTS) that provides programmatic and investigative support to HSI Special Agents assigned to nation-wide JTTF's. HRVWCU is an NSID unit formed to investigate cases of war crimes and human rights violations to prevent the United States from being used as a safe haven for those who commit such atrocities.

NSID uses SharePoint for a variety of purposes such as tracking budgetary and personnel actions, information sharing with NSID agents in the field, and collaborating on investigations. All evidence, leads, and investigative work products are stored in ICE case management systems.[24]

Site functionalities include:

- Point of Contact (POC) lists and shared Calendars include name and contact information that are collected and stored on the site for internal communication, collaboration, and information exchange between NSID Personnel, Field POCs, and Task Force Officers. All individuals in the POC list are federal employees. Users are trained to refrain from referencing Sensitive PII in calendar posts and POC fields.
- NSID Programmatic Libraries include high level reports for the unit; information sharing agreements (e.g., MOUs, MOAs) between NSID and other agencies or

[24] *See* DHS/ICE/PIA-044 LeadTrac or DHS/ICE/PIA-045 Investigative Case Management System (ICM) *available at* www.dhs.gov/privacy.

programs; employee travel information; employee personnel actions (including disciplinary action); outreach materials and case studies; resume information for applicants to job vacancies in the unit; Onboarding & Offboarding documents for new NSID personnel; and official agency correspondence and forms.

- HRVWCU will use the SharePoint to store white papers and reports (including reports on investigations, or ROIs) in the libraries on the HRVWCU subsite. The information will include name and date of birth among other identifying information, as well as immigration history, case information, and case recommendations.
- Alien Files (A-Files), which include date of birth, A-Number, Social Security number (SSN), passport number, and family information will be stored on the CTS subsite to allow HSI field agents, Headquarters Project Managers, Headquarters analysts, and ICE national security attorneys the ability to review the file for possible JTTF disruption options while they are waiting for the physical A-File. A-Files are immediately removed from the site when the physical A-File arrives or there is no longer a need for the file.

System Access:

Permissions-based access to subsites and libraries that do not contain Sensitive PII will be restricted to NSID employees. Permissions-based access to subsites and libraries containing Sensitive PII (e.g., disciplinary action, performance evaluations) will be restricted to supervisors, SharePoint site administrators, and NSID personnel with a verified need to know. Need to know is determined on a document level. The site has a designated administrator that verifies users' need to know prior to granting access to all libraries, including those that may contain Sensitive PII. The site administrator also conducts routine audits to ensure that user permissions are applied appropriately and there is no unauthorized information posted to the site.

Individuals Impacted:

NSID personnel; federal employees partnered with NSID; subjects of counterterrorism investigations; and individuals suspected of human rights violations.

Sources of Information:

No other system is connected to the NSID SharePoint site. Information is gathered directly from NSID personnel who create and upload documents. During the investigative process NSID personnel search a variety of government databases and non-government sources, including open source systems on the internet and social media sites.

Data Elements:

Data elements collected by NSID varies based on the investigation conducted by the unit.

Members of the public:

- Identifying information including full name, date of birth, gender, country of birth, country of citizenship, resume information, visitor log entries, and phone number;
- Case Information including case status, immigration history, the relevant content of a subject's A-File, employment history, criminal history, associate details, investigation and case recommendations, clearance level, and social media account information;
- Identity document information including A-Number, passport/visa information, SSN, driver's license, address, email, fingerprint ID number, and SEVIS ID.

ICE personnel:

- Name (first, last), role, phone number, Unit/Office, Agency, Division, travel details (foreign travel), disciplinary action, performance evaluations, resume information, security clearance elevation, visitation logs, passport information;

Other Federal employees:

- Name (first, last), employer name, email, phone number, and resume information.

SORN Coverage:

- DHS/ICE-009 External Investigations SORN,[25] which outlines the collection of PII for administrative, intelligence, and law enforcement investigations;
- DHS/ALL-002 Mailing Lists SORN,[26] which covers the collection of contact information for administrative purposes;
- OPM/GOVT-1 General Personnel Records,[27] which covers the collection of personnel records files and reports of personnel actions relating to an employee's federal service;
- OPM/GOVT-2 Employee Performance File System Records,[28] which covers the collection of employee performance evaluations;
- OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers,[29] which covers the documentation of disciplinary actions of ICE employees contained in the SharePoint site;
- OPM/GOVT-5 Recruiting, Examining, and Placement Records,[30] which covers the collection of resumes for purposes of hiring; and

[25] DHS/ICE-009 External Investigations System of Records, 75 FR 404 (Jan. 5, 2010).
[26] DHS/ALL-002 DHS Mailing and Other Lists System, 73 FR 71659 (Nov. 25, 2008).
[27] OPM/GOVT-1 General Personnel Records, 77 FR 73693 (Dec. 11, 2012).
[28] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35342, 35347 (June 19, 2006).
[29] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction In Grade and Removal Actions, and Termination of Probationers, 65 FR 24732 (April 27, 2000).
[30] OPM/GOVT-5 Recruiting, Examining, and Placement Records, 79 FR 16834 (March 26, 2014).

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records,[31] which covers ICE's use of an individual's A-File for purposes of documenting and reviewing an individual's immigration history.

Records Retention Period:

NSID will only keep documents on the SharePoint site as long as there is a business need. Document owners will remove documents when the mission need ends. This includes when a finalized document is uploaded to a different system, a case is closed, or the document or the information contained therein is outdated. SharePoint administrators will be actively auditing the site (i.e., periodically checking the site for old documents, documents created by personnel no longer in the unit, or documents irrelevant to current operations) to ensure document owners are deleting outdated documents or information from SharePoint. All finalized documents will be uploaded into their source systems, which will be governed by separate record retention schedules. Information that reflects data gathered in NSID casework will also reside in source systems, such as LeadTrac or ICM. A-Files must be retained permanently.

[31] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).

Appendix J

Program/System:

ICE Office of the Chief Financial Officer (OCFO), Performance Audit and Tracking System (PATS)

Purpose and Use:

As a federal agency, ICE is subject to audit, inspection, and review (hereinafter referred to as "audits") by certain entities of the Legislative and Executive branches of government. Specifically, the U.S. Government Accountability Office, the U.S. Internal Revenue Service, and the Department of Homeland Security Office of Inspector General are authorized to examine all facets of activities of the agency and to acquire information from the agency during the audit process. DHS components are required to have a system for managing audits. PATS is built on the SharePoint platform and is the system that ICE uses for all facets and processes related to audits. ICE is subject to between 15 and 30 audits annually as well as audit follow-up reporting requirements.

Users in the Audit Liaison Office (ALO), a unit within OCFO, are able to create audit projects and task program offices with providing information and formal responses for the auditors. Program offices are able to create tasks for subject matter experts to respond to auditor requests. Responses to the tasks come in the form of documents created by the agency, documents in the possession of the agency, explanative narratives, and/or interviews. These documents are pulled by program offices in response to tasks and delivered to the requestor. The contents of the response are then saved in PATS under an identifying number or title related to the request, not the subject of the information. The title and the identifier do not contain PII.

By tracking both audit tasks and responses in the system, PATS enables ICE to demonstrate its responsiveness and timeliness in meeting auditor demands, demonstrating corrective actions taken to remediate audit findings, and maintaining historical information for use in tracking and reporting.

System Access:

Access to the SharePoint site is limited to individuals listed as Audit Coordinators for ICE program offices, as well as individuals identified as subject matter experts within relevant ICE program offices. These individuals will not have access to audits outside of their need to know. All users must request and be approved for SharePoint access by the site administrator prior to accessing the system.

Individuals Impacted:

DHS employees and contractors from ICE, as well as members of the public who are the subjects of ICE records. Any agency information not covered by attorney or executive privilege is available for audits.

Sources of Information:

PATS information is gathered by Audit Coordinators during an audit and entered manually. Barring any legal exemptions, PATS may contain information deemed relevant to an audit from any ICE system.

Data Elements:

PATS contains the following data about DHS employees and contractors:

- Full name;
- Contact information (e.g., address, phone number);
- SSN;
- Date of birth;
- Other identifying data (e.g., photographs, identification document numbers);
- Employment-related data (e.g., training, benefits, hiring, background, performance);
- Financial data (e.g., accounts, salary, transactions); and
- Income tax data.

Because auditors may collect any information not covered by attorney or executive privilege, audit records held within PATS may also contain the following about members of the public if deemed necessary to complete the audit:

- Full name;
- Contact information (e.g., address, phone number);
- SSN;
- A-Number;
- Other identifying data (e.g., photographs, identification document numbers);
- Criminal arrest records;
- Immigration-related data; and
- Medical information not covered by privilege.

SORN Coverage:

Because PATS is an audit system, information comes from other existing systems, which have their own individual SORNs. The sharing of PII for audit purposes is covered by the SORN of the system providing the information to PATS.

Records Retention Period:

PATS retains records of audits for three (3) years after the cut off, at which time the records are destroyed or deleted. Records are cut off once all recommendations for a given audit have been resolved (i.e., after final resolution and implementation of all findings and recommendations).

Appendix K

Program/System:

Counterterrorism and Criminal Exploitation Unit (CTCEU) SharePoint

Purpose and Use:

CTCEU is a unit within ICE's Homeland Security Investigations National Security Investigations Division (NSID) that focuses on preventing criminals and terrorists from exploiting the nation's immigration system. CTCEU primarily investigates non-immigrant visa holders who violate their immigration status or terms of admission. CTCEU also supports investigative efforts of other programs within DHS and the Federal Government that aim to reduce fraud and increase national security in the non-immigrant visa process.[32] CTCEU uses SharePoint to track cases, collaborate on investigations, and store working papers for its programs. All evidence, leads, and investigative work products are ultimately stored in ICE case management systems.[33]

Site Functionalities include:

- Point of Contact (POC) lists and shared Calendars: name and contact information are collected and stored on the site for internal communication, collaboration, and information exchange between CTCEU Personnel, Field POCs, and External POCs. External POCs can be members of the public (i.e., task force officers from local or state law enforcement). Users are trained to refrain from referencing Sensitive PII in calendar posts and POC fields.
- CTCEU Programmatic Libraries include case trackers, reports, and white papers, all of which may contain case information, including criminal and immigration information, on the subjects of CTCEU's investigations. Case information may also include the results of open source analysis on an individual's online identity. CTCEU also stores PowerPoint presentations on the SharePoint for purposes of outreach and education to other HSI field offices. These presentations may include immigration and criminal history of case study subjects.

System Access:

Permissions-based access to subsites and libraries containing Sensitive PII will be restricted to supervisors, SharePoint site administrators, and CTCEU personnel with a verified need to know. The site has a designated administrator who verifies users' need to know prior to granting access to libraries that may contain Sensitive PII. The site administrator also conducts routine audits to ensure that user permissions are applied appropriately and there is no unauthorized information posted to the site.

---

[32] All Information regarding CTCEU's investigative efforts and programs that it supports can be found in DHS/ICE/PIA-044 LeadTrac *at* www.dhs.gov/privacy.

[33] *See* DHS/ICE/PIA-044 LeadTrac or DHS/ICE/PIA-045 Investigative Case Management System (ICM) *at* www.dhs.gov/privacy.

Individuals Impacted:

- CTCEU personnel;
- Federal employees partnered with CTCEU;
- Foreign military personnel who are absent without leave (AWOL) or applying to a U.S. service academy;
- Applicants to TSA Transportation Worker Identification Credentials;[34]
- Applicants to become Student Exchange Visitor Program (SEVP) designated school officials;[35]
- Non-immigrant students;
- INTERPOL designated fugitives;
- Participants in the Department of Defense Military Accessions Vital to the National Interest program;[36] and
- Other non-immigrant visa holders from certain designated Department of State consular posts.

Sources of Information:

CTCEU routinely receives information from its partners in the Department of Defense, the Department of State, The Transportation Security Administration (TSA), the FBI's National Crime Information Center (NCIC)[37], and INTERPOL. During the investigative process, CTCEU personnel search a variety of government databases and non-government sources, to include open-source systems on the internet and social media sites.[38] CTCEU also derives information from LeadTrac[39] and the Investigative Case Management System.[40]

Data Elements:

Data elements collected by CTCEU vary based on the investigation conducted by the unit.

Members of the public:

---

[34] *See* DHS/TSA/PIA-012 Transportation Worker Identification Credential (TWIC) Program *at* www.dhs.gov/privacy.
[35] *See* DHS/ICE/PIA-001 Student Exchange Visitor Information System (SEVIS) and subsequent updates *at* www.dhs.gov/privacy.
[36] *See* Military Accessions Vital to the National Interest (MAVNI) Recruitment Pilot Program *at* https://dod.defense.gov/news/mavni-fact-sheet.pdf.
[37] *See* JUSTICE/FBI-001 National Crime Information Center 64 FR 52343 (September 28, 1999)
[38] For more information regarding CTCEU's sources of information *see* DHS/ICE/PIA-044 LeadTrac *at* www.dhs.gov/privacy.
[39] *See* DHS/ICE/PIA-044 LeadTrac *available at* www.dhs.gov/privacy.
[40] *See* DHS/ICE/PIA-045 Investigative Case Management System (ICM) *available at* www.dhs.gov/privacy.

- Identifying information including full name, date of birth, gender, country of birth, country of citizenship, and phone number;
- Case Information including AWOL location/disposition/status, case status, immigration history, employment history, criminal history, investigation and case recommendations, INTERPOL number, clearance level, and social media account information; and
- Identity document information including A-Number, passport/visa information, SSN, driver's license, address, email, fingerprint ID number, and SEVIS ID.

ICE employees and Federal employees:

- Name, job title, employer, business address, email address, and phone number.

SORN Coverage:

DHS/ICE-015 LeadTrac System of Records[41] and DHS/ICE-009 External Investigations[42]

Records Retention Period:

CTCEU will only keep documents on the SharePoint site as long as there is a business need. Document owners will remove documents when the mission need ends. This includes when a finalized document is uploaded to a different system, a case is closed, or the document or the information contained therein is outdated. SharePoint administrators will be actively auditing the site (i.e., periodically checking the site for old documents, documents created by personnel no longer in the unit, or documents irrelevant to current operations) to ensure document owners are deleting outdated documents or information from SharePoint. Information contained on SharePoint reflects data gathered in CTCEU casework that resides in source systems, such as LeadTrac.

[41] *See* DHS/ICE-015 LeadTrac System of Records, 81 FR 52700 (August 9, 2016).
[42] *See* DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010).

Appendix L

Program/System:

ICE Identity and Benefit Fraud Unit (IBFU) Accountability Section Tracker

Purpose and Use:

The Identity and Benefit Fraud Unit (IBFU) within HSI is charged with overseeing the disruption, investigation, and prosecution of immigration benefit fraud schemes as part of its mission. Often these investigations result in the identification of numerous beneficiaries who received a benefit to which they were not entitled. ICE IBFU will conduct case reviews and refer cases amenable for criminal prosecution to the appropriate ICE field office for investigation. Those cases not referred for prosecution by IBFU will be returned to the referring U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security unit for follow up to determine if administrative action (denial of benefits, etc.) is warranted.

In order to ensure coordinated oversight and a method of searching for information and providing statistical data on the outcome of referrals, IBFU uses a centralized repository of immigration benefit fraud case information. This SharePoint site maintains data regarding individual beneficiaries and is searchable by name and/or A-Number.

The maintenance of data on a centralized SharePoint site gives the IBFU greater oversight and accountability in cases where immigration fraud has been found, to ensure that information is referred to USCIS or to the appropriate ICE field office in a timely, standardized manner, and to ensure that individuals whose benefits were obtained through fraud are successfully investigated.

System Access:

Access to this SharePoint site is limited to IBFU personnel. Certain identifying information and information that substantiates a finding of fraud about a beneficiary may be sent via encrypted email as necessary to USCIS. USCIS personnel will not, however, have access to the site.

Individuals Impacted:

IBFU personnel and HSI field personnel involved in creating field office reports; ICE contractors; and members of the public who are the subjects of investigations involving potential benefit fraud.

Sources of Information:

IBFU personnel import information from field office reports in the form of Excel spreadsheets submitted by local USCIS and HSI field offices onto the SharePoint site. Additional data about beneficiaries, including the existence of criminal history and other derogatory

information, will be added manually by IBFU personnel from government databases such as the Investigative Management System (ICM)[43] or CBP TECS.[44]

Data Elements:

The site collects field office reports from HSI field personnel regarding individuals allegedly receiving fraudulent benefits. This includes information regarding members of the public as well as DHS employees.

- Information collected from members of the public: names, A-Numbers, dates of birth, petitions filed, and other identifiers, which may include SSNs, if the beneficiary has already applied for a SSN, and received one. The SharePoint site may also include derogatory information (i.e., criminal history) about the individuals.
- Information collected from DHS employee/contractors: names, business contact information, and job title.

SORN Coverage:

DHS/ICE-009 External Investigations SORN[45]

Records Retention Period:

IBFU will only keep documents on the SharePoint site as long as there is a business need. Document owners will remove documents when the mission need ends. This includes when a finalized document is uploaded to a different system, a case is closed, or the document or the information contained therein is outdated. SharePoint administrators will be actively auditing the site (i.e., periodically checking the site for old documents, documents created by personnel no longer in the unit, or documents irrelevant to current operations) to ensure document owners are deleting outdated documents or information is from SharePoint. Information contained on SharePoint reflects data gathered in IBFU casework that resides in source systems, such as ICM.[46]

[43] *See* DHS/ICE/PIA-044 LeadTrac or DHS/ICE/PIA-045 Investigative Case Management System (ICM) *at* www.dhs.gov/privacy.
[44] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing *at* www.dhs.gov/privacy.
[45] DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010).
[46] *See* DHS/ICE/PIA-044 LeadTrac or DHS/ICE/PIA-045 Investigative Case Management System (ICM) *at* www.dhs.gov/privacy.

Appendix M

Program/SharePoint Site:

ICE HSI Fugitive Tracking System SharePoint Site

Purpose and Use:

The purpose of the HSI Fugitive Tracking System (FTS) is to centralize all available information about fugitives at HSI headquarters to make information available to the HSI Fugitive Coordinators (via HSI Net), who then facilitate information dissemination to DHS, or other federal, state, local, tribal, or territorial (FSLTT) law enforcement partners. The product generated from FTS includes a "wanted" poster, like those used by the Federal Bureau of Investigation (FBI) and found at U.S. Postal Service facilities.[47]

HSI analyzes information collected from multiple sources (e.g., human sources/confidential informants, ICE source systems)[48] to determine which fugitives are priorities, and uses FTS to generate wanted posters to locate the fugitive's whereabouts so that agents can take appropriate enforcement action.[49] HSI also uses information in this system to determine which fugitives appear on an HSI wanted poster to be shared with other law enforcement agencies.

Site Access:

FTS is accessible to only HSI Fugitive Coordinators assigned to HSI Special Agent in Charge (SAC) offices and those who have a need-to-know. The Fugitive Coordinator positions are usually special agents/program managers only. Fugitive Coordinators access FTS using their DHS PIV card (via security controls and managed by authorized system administrators), through the HSI NET on the DHS ICE network.

Designated personnel in HSI headquarters will also be provided with special administrative access to all records in FTS to centralize access control and management, coordination, and oversight of the information maintained in the system; and for its designated users across the SAC Offices. While no additional training is provided for Special Agents/program managers with access to FTS, there is a handbook[50] outlining proper procedures for entering data into the system, creating the wanted poster, and emailing to law enforcement partners.

---

[47] Unlike FBI wanted posters, HSI does not post fugitive wanted posters in view of the general public or in post offices. While posters could be hung in areas accessed by the public, such as in secured federal buildings, or in behind-the-scenes operations centers at airports (where the public is typically not permitted, or most likely escorted), HSI's intended audience is federal, state, local, tribal, and territorial (FSLTT) law enforcement, and occasionally, foreign law enforcement.

[48] Human sources, also referred to as to Human Intelligence (HUMINT) collection, can be any human that provides information that assists law enforcement in locating the fugitive.

[49] FTS does not automatically perform this function; it is conducted by special agents based on the information contained in the system.

[50] Fugitive Handbook, OI HB 10-02, Chapter 5 (April 9, 2010).

Individuals Impacted:

- Individuals "at large" (criminal fugitives)[51];
- DHS/ICE employees include the ICE HSI Case Agent and Fugitive Coordinator, alternate Fugitive Coordinator, and designated HSI personnel with special administrative access.[52]

Sources of Information:

- Agent users. Agents may enter new information that they obtain from human sources or databases.
- Coordinators. Standard biographic information about individuals (known fugitives) is entered manually by the coordinator responsible for the assigned case(s) and for records related to their area(s) of responsibility. While new records are created using information from various source systems, existing records can be modified or updated as required if new information about an individual is located.
- Source systems. Source system PIA coverage is provided by the following. The Investigative Case Management (ICM) PIA DHS/ICE/PIA-045(a) addresses case file data such as photos and other biographic information. The CBP TECS PIA DHS/CBP/PIA-021 "TECS System: Platform" addresses data pertaining to the flow of people through border ports of entry.[53]
- FLSTT law enforcement officers. Photographs and other biographic information can be received from encounters with FSLTT law enforcement officers.
- Confidential sources. Information collected from human sources (i.e., Confidential Informants) during investigations.

Data Elements:

Information on the wanted posters is limited to:

- Place of birth (POB);
- Date of birth (DOB);
- Photograph;
- Demographics;
- Height;

[51] FTS is not focused on immigration enforcement; the focus is on HSI mission criminality.
[52] The only personnel that have access to the system are those designated by each SAC as the office's Fugitive Coordinator and alternate Fugitive Coordinator(s). Due to office size, there may be several alternates.
[53] *See* DHS/ICE/PIA-045 (2016) Investigative Case Management (ICM) and DHS/CBP/PIA-009(a) Primary and Secondary Processing National SAR Initiative (TECS System), *available at* www.dhs.gov/privacy.

- Weight;
- Eye color;
- Gender;
- Hair color;
- Scars & Marks;
- Last known location;
- Reward; and
- Synopsis for crimes wanted.

To ensure ICE posts information about the suspected individuals at large, a wider complement of (additional) biographic information is maintained in FTS:

- Name;
- Aliases;
- Tattoos;
- TECS Record ID;
- Immigration Status;
- Country of Citizenship; and
- Email.

Information collected about DHS employees include:

- ICE HSI Case Agent name;
- Fugitive Coordinator name; and
- Offices to which they are assigned.

SORN Coverage:

- DHS/ICE-009 External Investigations System of Records,[54] which covers collecting and maintaining records related to external investigations and support conducted by ICE offices, primarily HSI;
- DHS/ICE-010 Confidential and Other Sources of Information (COSI) System of Records,[55] which covers documenting and managing the identities of and information received from a number of sources, including Confidential Informants, regarding

[54] *See* DHS/ICE-009 External Investigations System of Records, *available at* www.dhs.gov/privacy.
[55] *See* DHS/ICE-010 Confidential and Other Sources of Information (COSI) System of Records, *available at* www.dhs.gov/privacy.

possible violations of law or other information in support of law enforcement investigations and activities conducted by ICE; and

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records,[56] which covers the identification, apprehension, and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act (INA), including fugitive non-citizens.

Records Retention Period:

All relevant documents produced or provided in accordance with this PIA must be maintained in accordance with an applicable National Archives and Records Administration (NARA) General Records Schedule (GRS) or a NARA-approved agency-specific records control schedule. In the event the records are subject to a litigation hold, they may not be disposed of under a records schedule until further notification.

[56] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, *available at* www.dhs.gov/privacy.

Appendix N

Program/System:

ICE HSI International Visitors Program (IVP) SharePoint Site

Purpose and Use:

ICE HSI International Operations manages the International Visitors Program (IVP) and coordinates the vetting[57] of foreign nationals who seek to meet with senior ICE officials and/or visit ICE controlled facilities. Coordination includes: vetting individual foreign nationals who request visits, tracking events, and producing reports for senior management. To track visits and events, HSI uses the IVP SharePoint site. This new stand-alone site is designed to: 1) replace the current paper tracking process; 2) track events including rosters, rooms, dates, attendance, and topics briefed; and 3) produce statistical reports. Data on the SharePoint site is retrieved both by name and by the DHS Integrated Security Management System (ISMS) case number.[58] While ISMS is a DHS system, IVP SharePoint is exclusively an ICE site.

In coordinating and tracking these visits, based on the information provided by the foreign national on the Foreign National Visit Access Request form (DHS Form 11052), HSI International Operations uses the IVP SharePoint site to track the names of the foreign visitors, their country of citizenship, and details of their proposed visit to an ICE facility or their visit with an ICE senior official.[59]

The site also tracks the DHS ISMS-generated case number associated with the foreign visitor subject, which is created when HSI enters the relevant information and the record is opened in the ISMS system. This case number is used in the SharePoint site as a quick way to look up a visitor in ISMS without doing a search by the individual's name. The SharePoint site also enables both HSI Intelligence (HSI Intel) Protective Intelligence and ICE Operational Security (OPSEC) to confirm whether a foreign visitor has been vetted.[60]

The SharePoint site contains a choice field (yes/no) to denote whether the respective foreign visitor was vetted and whether ICE found any derogatory information on the individual.

System Access:

The following offices access the IVP SharePoint site to confirm whether foreign visitors have been vetted: ICE International Operations, ICE HSI Intelligence, and ICE Operational Security (OPSEC).

---

[57] Vetting is defined as manual and automated processes used to identify and analyze information in U.S. Government holdings to determine whether an individual poses a threat to national security, border security, homeland security, or public safety, primarily, but not necessarily exclusively, in support of the U.S. Government's visa, naturalization, immigration benefit, immigration enforcement, travel, and border security decisions about an individual.

[58] *See* DHS/ALL/PIA-038(d) Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.

[59] *See* Department of Homeland Security Foreign National Visitor Access Request – DHS Form 11052-1 (07/05), *available at* https://www.aphis.usda.gov/is/downloads/visitors_center/DHS_ForeignVisitorForm-2012.pdf.

[60] HSI Intelligence may also be referred to as ICE Protective Intelligence.

Individuals Impacted:

- Foreign nationals who have proposed a visit to an ICE facility to meet with an ICE senior official;
- DHS/ICE employees/contractors to include the ICE senior official, and contractors working on behalf of DHS;
- Requester points of contact; and
- Visitor escorts.

Sources of Information:

The point of contact (POC)/requester of the visit submits requests to ICE. The POC is usually an ICE, DHS, FBI, or State Department employee; however, occasionally the POC may be a foreign national associated with a particular group such as a foreign law enforcement agency.[61] The ISMS case number associated with the individual provides another source of information. Visitors complete DHS Form 11052, then ICE International Operations manually enters Form 11052 information both into ISMS and into the IVP SharePoint site.[62]

Data Elements:

The IVP SharePoint site tracks the details of the foreign nationals' proposed visit to an ICE facility or visit with an ICE senior official; the ISMS case number associated with the individual; and any emails from the requestor of the visit.[63]

The request form has the following sections:

1. Visitor Request Information. DHS Form 11052 is the primary source of personally identifiable information (PII) collected and maintained. Information on the form includes: name of the person requesting the visit, visitor name (if different), topics of discussion, job title/employer, date of birth (DOB), gender, place of birth (POB), passport number with expiration date, and country of citizenship.
2. Escort Information (ICE host who receives the visitor). Escort name, job or position title, date of birth (DOB), gender, place of birth (POB), and country of citizenship.

Occasionally, foreign visitors (e.g., diplomats) may submit alternative PII instead of original passports, such as: photocopies of passports, copies of their visas/visa information,

[61] These U.S. government officials may make visit requests on behalf of foreign nationals. Foreign nationals may request to visit an ICE facility and meet with ICE personnel.

[62] This is the DHS Foreign National Visitor Access Request Form 11052-1 (07/05). In some cases, a DHS Foreign Access Management (FAM) Form 11055 (06/17) may be referenced.

[63] The foreign visitor form (not the SharePoint site) may contain a field for sensitive data elements including SSNs but the ISMS site does not specifically require a user to input SSNs. HSI Protective Intel and OPSEC use the data elements to access background check information but some data elements are not maintained or stored within ICE/SharePoint.

country of citizenship, resumes, biographies, position title, and ISMS number. This information is contained on the SharePoint site.

SORN Coverage:

- DHS/ALL-023 Personnel Security Management System of Records,[64] which covers the collection and maintaining of records of processing of personnel security-related clearance actions, to record suitability determinations, fitness determinations, whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position; and
- DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management System of Records,[65] which covers the collection and maintaining of records associated with DHS facility and perimeter access control, including access to DHS information technology and access to classified facilities, as well as visitor security and management.

Records Retention Period:

Records are retained in accordance with DHS-wide records schedule DAA-0563-2013-0001 Biometric with Limited Biographical Data, item 0004 threat assessment credentialing.

[64] DHS/ALL-023 Personnel Security Management, October 13, 2020, 85 FR 64511.

[65] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, February 3, 2010, 75 FR 5609.

Appendix O

Program/System:

ICE Medical-related Incident Reporting Tool

Purpose and Use:

The ICE Health Service Corps-Medical Quality Management Unit (IHSC-MQM) is responsible for ensuring that quality healthcare services are delivered appropriately, timely, and competently to all ICE detainees in custody (mainly in IHSC-staffed facilities). IHSC-MQM uses this SharePoint site-based tool to report patient safety concerns (e.g., medication errors) identified by members of the health care team. These safety concerns are classified as incidents based on an established set of categories (e.g., injuries, medication errors, malfunctioning equipment) and are selected from the event type dropdown and associated risk score.

The incident reporting process falls under the Risk Management (RM) component of MQM. The RM team along with the local Facility Health Care Program Manager (FHPM) review the report to identify any process vulnerabilities related to the care that a detainee received. After a report is submitted via SharePoint, a SharePoint workflow is triggered which sends email notifications to the FHPM instructing them to review the incident. At the discretion of the risk manager or the FHPM, the report can be referred to a subject matter expert or an IHSC leader. The referral of an incident report also generates an e-mail notification to the individual being asked to review the report.

During the review of the incident report, a process vulnerability is identified by comparing what happened during the specific event in question to what usually happens in a similar situation. Any deviation would be labeled as a process vulnerability. The risk matrix, a common risk assessment tool, is utilized by the risk manager and the FHPM to determine the risk score by taking into consideration how the process vulnerability may have negatively impacted the patient and the likelihood that this issue will occur again. The risk score indicates if the process vulnerability could be tracked and trended or if a root cause analysis is needed to mitigate the risk. Once a final risk score is determined and the risk manager marks the incident report as complete, an e-mail to the FHPM and any additional reviewers (e.g., subject matter expert, IHSC leader) is triggered letting them know the report is complete.

System Access:

Access to the SharePoint site by each facility is limited to the specific field site information and select users (select facility and IHSC HQ staff) for reporting data, and to minimize the risk of errors currently present in the manual reporting and input of data. Designated IHSC HQ staff has access to all collected data for purposes of review and analysis.

Individuals Impacted:

IHSC-MQM and IHSC HQ staff that use this SharePoint site and members of the public who are being held at detention centers.

Sources of Information:

IHSC-MQM personnel input the relevant information directly into the SharePoint site with information provided voluntarily by members of the public who are being held at detention centers that make a report.

Data Elements:

The site collects information regarding members of the public as well as DHS employees.

- Detainee information, including detainee name, date of birth, A-number, gender, past medical history, facility where the incident occurred, event type, details of the incident, name of individual reporting the incident (can be seen by a SharePoint administrator, but hidden in the report itself), and medical information related to the incident, health, treatment and services provided; and
- Employee/contractor, including the name (person entering the incident report) and job title.

SORN Coverage:

SORN coverage is provided by DHS/ICE-013 Alien Health Records System,[66] which covers the maintaining of records that document the health screening, examination, and treatment of aliens detained by ICE in facilities where the ICE Health Services Corps (IHSC) provides or oversees the provision of care.

Records Retention Period:

These records are unscheduled and must be preserved as permanent until a records schedule has been approved by National Archives and Records Administration. This will be addressed in the ICE Electronic Health Records (eHR) records retention schedule that is being developed. Records eligible for destruction based on an approved records schedule, must receive approval from the Records and Data Management Unit prior to destruction, via the 8-002 Records Disposal Form.

[66] DHS/ICE-013 Alien Health Records System, March 19, 2018, 83 FR 12015.

Appendix P

Program/System:

ICE Medical Affairs Unit Pre-Employment Process SharePoint Site

Purpose and Use:

The ICE Office of Human Capital (OHC), Medical Affairs Unit (MAU), Pre-Employment Medical Process is a SharePoint-based website for managing the medical review for new law enforcement officers (LEOs) on-boarding to ICE. New ICE employees who are not LEOs do not receive a medical review.

The ICE MAU works closely with the OHC Human Resources Operations Center (HROC), Pre-Employment Clearance Unit (PEC). These units process entry level clearances for new LEOs who must undergo a physical examination and receive a clearance. ICE HROC, PEC obtains an individual's demographic information from the USAJOBS application and enters it into the MAU SharePoint site to order a medical examination or drug test. The individual applying for an ICE LEO position must provide information pertaining to his/her medical history and brings a hard copy of the ICE Medical Examination and Report form to the medical appointment. During the physical examination, the medical examiner reviews the information, performs an exam, and provides medical information based on the exam (e.g., vision test, hearing test, vitals).

Applicants for ICE law enforcement positions complete and sign the ICE Medical Examination and History Report form in the presence of a witness. The form contains a detailed medical history to include past and current medical conditions. A complete list of medical information can be found in the form itself. Once completed, this form is then uploaded to the medical vendor's system as well as the MAU SharePoint site for review.

The ICE Occupational Health Nurse (OHN) reviews the medical exam and history report and any subsequent medical documentation provided or requested from the selectee. The OHN utilizes the ICE medical standards and compares any relevant medical history to determine if a selectee meets the agency medical standards or if they will need to request a waiver. The ICE medical officer makes the final recommendation and the selectee is notified by PEC whether he or she is medically cleared to become an ICE law enforcement professional.

System Access:

The MAU SharePoint site is only accessed by the following ICE personnel:

- Staff from the ICE MAU;
- Members of the ICE medical review board, consisting of one member from ICE Enforcement and Removal Operations (ERO), one from ICE Homeland Security Investigations (HSI), and one from ICE Office of Professional Responsibility (OPR);
- The ICE PEC; and

- An ICE designated Office of the Principal Legal Advisor (OPLA) attorney.

Administrator rights to view and edit reports and attachments will be limited to a select team members within MAU.

Individuals Impacted:

Applicants for ICE positions, examining physicians, and witnesses to document signing where applicable.

Sources of Information:

Information about the applicant and their examining physician comes directly from the applicant through USAJOBS and medical forms relevant for the job to which the applicant is applying.[67]

Data Elements:

Information about the applicant is limited to:

- Name;
- Social Security number (SSN) or equivalent Identification number;
- Date of birth;
- Veteran's preference eligibility;
- Gender;
- Current employment information (including performance evaluations);
- Purpose of examination; and
- Relevant medical information.

Information about the Medical Examiner is limited to:

- Name and address of examining facility;
- Name of examining physician; and
- Telephone number.

Information about the Case Manager is limited to:

- Name.

Information about the witness (i.e., doctor performing the medical exam) is limited to:

- Signature.

[67] *See* DHS/ALL/PIA-043(a) Office of the Chief Human Capital Officer Talent Acquisition, *available at* www.dhs.gov/privacy.

Information about any new ICE employee is limited to:

- Name;
- Address;
- SSN;
- Date of birth;
- Telephone number;
- Occupation;
- Program Office; and
- Drug testing result.

SORN Coverage:

- OPM/GOVT-010 Employee Medical File System Records,[68] which covers information about individuals who are existing federal employees or are selected for a position;
- OPM/GOVT-005 Recruiting, Examining, and Placement Records,[69] which covers information about individuals who are not selected for a position; and
- DHS/ALL-022 Department of Homeland Security Drug Free Workplace,[70] which covers collecting records from current and former employees of DHS and certain applicants for employment with DHS who are tested for or submit voluntarily or involuntarily to the illegal use, possession, distribution, or trafficking of controlled substances.

Records Retention Period:

MAU destroys records 30 years after employee separation or when the Official Personnel Folder (OPF) is destroyed, whichever is longer, in accordance with National Archives and Records Administration General Records Schedule 2.7: Employee Health and Safety Records, 060: Item 060 Occupational individual medical case files.

[68] OPM/GOVT-10 Employee Medical File System Records, June 21, 2010, 75 FR 35099.
[69] OPM/GOVT-5 Recruiting, Examining, and Placement Records, March 26, 2014, 79 FR 16834.
[70] DHS/ALL-022 Department of Homeland Security Drug Free Workplace, October 31, 2008, 73 FR 64974.

Appendix Q

Program/System:

Immigration and Customs Enforcement (ICE) Health Service Corps (IHSC) Managed Care Guidelines (MCG) Evidence-Based Care Guidelines Solution SharePoint site

Purpose and Use:

The Immigration and Customs Enforcement (ICE) Health Service Corps (IHSC), a division of Enforcement and Removal Operations (ERO), provides medical, mental health and dental (collectively, "medical") care to detainees/residents[71] in ICE custody. IHSC has been using a license to access an independent, stand-alone, web-based subscription service called MCG Evidence-Based Care Guidelines solution to allow authorized IHSC personnel to review outside medical care provided to detainees in ICE custody. IHSC will use a tracker created by the Utilization Management Program Administrator that is housed in the ICE/ERO/IHSC SharePoint to document review findings. The IHSC-owned and operated Utilization Management Program/Utilization Review Data Tracker (collectively, "UR Data Tracker") will be used to evaluate and complete prospective, concurrent or retrospective reviews for the outside community medical care that the detainees/residents need, are receiving or have received. IHSC personnel will then document the findings reached from consulting the guidelines and enter the findings in the IHSC UR Data Tracker. The IHSC UR Data Tracker will provide IHSC personnel with pertinent information to plan, evaluate and track the medical care provided or planned for detainees/residents in ICE custody.[72]

System Access:

The MCG Evidence-Based Care Guidelines solution license allows an unlimited number of IHSC authorized personnel access to the following resources, functions and tools, including:

- Accessing evidence-based medical guidance or references with accompanying evidence grades, based on real case studies that show the strength of clinical recommendations, and associated links;
- Providing administrative and medical support for the provision and tracking of care determinations;
- Using built-in tools designed to promote care progression, transition of care, discharge planning, and optimal recovery course within the utilization review process;

[71] Residents are families staying at a Family Residential Center (FRC). To be eligible to stay at an FRC, the family cannot have a criminal history and must include a non-U.S. citizen child or children under the age of eighteen accompanied by his/her/their non-U.S. citizen parent(s) or legal guardian(s). With limited exceptions, the stay is generally limited to twenty (20) days.

[72] The MCG Evidence-Based Care Guidelines solution vendor cannot access the IHSC UR Data Tracker.

- Managing and storing utilization reviews with their related workflows, notifications, and documentation;
- Creating, assigning, and managing workflows and reviews;
- Communicating with other IHSC users for higher level reviews and assignments;
- Generating and creating reports for data and trend analysis;
- Customizing reporting features; and
- Printing completed reviews in PDF.

IHSC staff will generate an arbitrary, unique case identification (ID) number[73] for each subject's case in the MCG Evidence-Based Care Guidelines solution; however, that number is related to the utilization review and not linked to any other identifier (such as a name or other identifying number) concerning the subject. Therefore, although IHSC enters medical information associated with the IHSC-generated arbitrary IHSC UR Data Tracker number, only IHSC personnel can link that number with an individual. Thus, there is no Personally Identifiable Information (PII) in the MCG Evidence-Based Care Guidelines solution (or in anything accessible by the vendor). Once IHSC completes its research and reviews activities in the MCG Evidence-Based Care Guidelines solution, a PDF record is printed out and uploaded to IHSC's ICE/ERO/IHSC HPMU SharePoint site. At this point, all information in the MCG Evidence-Based Care Guidelines solution is deleted, and the IHSC UR Data Tracker is closed.

There is no integration or connection between the MCG Evidence-Based Care Guidelines solution and any ICE/DHS platform or system.

Individuals Impacted:

ICE employees and contractors, as well as any members of the public who are the subjects of ICE records.

Sources of Information:

The sources of information on the SharePoint site are authorized IHSC employees and contractors, and detainees/residents in ICE custody.[74]

Data Elements:

About the subject detainee/resident:

- IHSC-generated UR Data Tracker number (not a nationally recognized unique identifier);
- Date of review;

[73] The Case ID Number is the year plus the order in which access is logged in to conduct research, e.g., 2021.01, 2021.02, and so forth.
[74] *See* DHS/ICE/PIA-037 electronic Health Records System, *available at* www.dhs.gov/privacy.

- Type of review;
- International Classification of Diseases, Tenth Revision, Clinical Modification, (ICD) 10 Code;
- Managed Care Guidelines (MCG) guide reference used for the review;
- Optimal recovery course;
- Goal - length of stay;
- Barriers to discharge/milestones;
- Dates and services covered by review;
- Next review date;
- Date/review discussed with attending physician;
- Date/review discussed with supervisor;
- Date/review referred to physician advisor.

The information entered or collected above includes medical information, such as a description of past or present medical condition, diagnosis, and planned course of treatment, as well as the guidance provided by the resources in the MCG Evidence-Based Care Guidelines solution. However, this information is associated only with the IHSC-generated UR Data Tracker number and is not linked to any other identifier. Once IHSC staff completes its evaluation and review process for a subject, they print out the records in PDF, and close the case or review by deleting all review notes in the MCG Evidence-Based Care Guidelines solution.

About individuals other than the subject:

- Vendor-supplied log-in username for the authorized IHSC employee/contractor under the license; and
- User-supplied password (reset, but not maintained, by the vendor).

This information is also deleted when the records are deleted from the MCG Evidence-Based Care Guidelines solution at the conclusion of a case.

SORN Coverage:

- DHS/ICE-013 Alien Health Records System[75], which documents and facilitates the provision of medical, dental, and mental health care to individuals in ICE custody in facilities where care is provided by IHSC.

Records Retention Period:

There is no retention schedule for the information in the MCG Evidence-Based Care

[75] DHS/ICE-013 Alien Health Records System, 83 FR 12015 (Mar. 19, 2018).

Guidelines solution. Upon completion of their research and tracking activities, IHSC staff print out the reports in PDF, and delete the information in the MCG Evidence-Based Care Guidelines solution. IHSC uploads the PDF report to ICE SharePoint, where the retention is ten (10) years for subjects who are eighteen (18) years and older. For individuals seventeen (17) years and younger, the information in SharePoint is kept until they reach twenty-seven (27) years of age. The schedule for the information in SharePoint is ICE Detainee Records Schedule DAA-0567-2015-0013 (June 2019).

Appendix R

Program/System:

Homeland Security Investigation (HSI) Polygraph SharePoint Site.

Purpose and Use:

The Homeland Security Investigations Forensics Laboratory (HSI-FL) Polygraph Unit uses an HSI-Net SharePoint site to receive polygraph requests from field agents; track polygraph requests and examinations; assign SharePoint-generated case numbers; generate Reports of Investigation (ROI) (for each polygraph examination (PE)); and maintain completed examinations.

This Appendix covers two ICE collections: (1) the HSI-FL Polygraph Unit HSI-Net SharePoint site, and (2) the Transnational Criminal Investigative Unit (TCIU) Security Questionnaire. All functionalities and uses of the HSI-FL Polygraph Program HSI-Net SharePoint site and the Transnational Criminal Investigative Unit Security Questionnaire operate within the guidelines of source system and corresponding vetting PIAs.[76]

The HSI-FL Polygraph Unit conducts three types of PEs:

- Specific issue in support of HSI Criminal Investigations
- National Security Screenings
- TCIU Screenings

PEs may be requested for a variety of purposes. HSI Special Agents request a PE for a criminal investigation by submitting a Polygraph Services Request to the HSI-FL Polygraph Unit via SharePoint. HSI Special Agents or Task Force Officers (TFO) submit PE requests for employees who will have access to national security information. HSI Office of International Operations requests PEs for foreign nationals who would like to work with HSI unit/taskforces abroad. Other federal, state, and local law enforcement agencies may submit a Polygraph Services Request to the HSI-FL Polygraph Unit in support of joint criminal investigations. HSI authorizes the use of PEs as an investigative aid. PEs can establish a subject's credibility and identify additional leads, suspects, and assets. They are only administered to individuals who agree or volunteer to take a PE and in accordance with existing laws, regulations, and policy.

ICE uses the "TCIU Security Questionnaire" to collect information about foreign law enforcement personnel who wish to work with ICE HSI. This form allows ICE HSI International Operations to complete a PE on foreign law enforcement officials (hereafter "applicants") as part of the vetting process to serve in a United States Government Agency Vetted Unit and work with HSI personnel overseas in conducting investigations pursuant to ICE's law enforcement authorities. The applicant completes the form prior to the date of the PE. The applicant submits

[76] *See* DHS/ICE/PIA-045 Investigative Case Management, DHS/ALL/PIA-038, Integrated Security Management System (ISMS), and DHS/ALL/PIA-048 Foreign Access Management System (FAMS), *available at* https://www.dhs.gov/compliance.

the completed form to the HSI requesting official, or one of their designees, who reviews the questionnaire with the applicant for completeness, and accuracy. On the date of the examination, the HSI Polygraph examiner reviews the information on the form to determine if the individual is withholding information. The completed questionnaire forms are kept in the respective HSI Attaché office where the polygraphs were conducted (e.g., HSI Bogota, HSI Panama City, HSI Manila). The completed questionnaires are filed alphabetically and kept in a locked cabinet at the respective HSI Attaché office/at-post. HSI Attaché Representatives (Federal criminal investigators) will have access to original questionnaires. Program Managers and Operations Chiefs at ICE Headquarters can request copies, if needed. Once the questionnaire form is completed, it is scanned and uploaded to the HSI Polygraph SharePoint site. Only designated employees with a need to know have access to PII on the SharePoint site.

System Access:

Designated employees with a need to know have access to the PE files and other PII on the SharePoint site. Individuals without a need to know can only view the request form and his or her submitted requests.

Individuals Impacted:

- Members of the public (U.S. persons, including U.S. Citizens and Lawful Permanent Residents, and non-U.S. Persons);
- DHS employees and contractors (e.g., ICE employees); and
- U.S. Department of Justice (DOJ), Assistant United States Attorneys (AUSAs).

Sources of Information:

HSI personnel create documents (e.g., the HSI Polygraph examiner completes the information on the ICE Polygraph Examination Interview Worksheet (also known as biographical/medical form) in its entirety about the examinee for one of the three types of PE. The HSI Polygraph examiner also collects information on medical conditions and medications before every PE to ensure examinees are both fit (e.g., pregnancy; heart conditions; stress induced asthma; or polygraph examinees who are prone to seizures) for the exam and not under the influence of substances that can affect results. The final polygraph file also contains any form completed during the pre-test phase, the actual charts that were collected, and used to render a decision. The final polygraph file is similar to a streamlined electronic case file, containing anything HSI-FL created as part of the testing process. At the completion of the examination, depending on the outcome, the polygraph examiner may conduct a post-test interview of the subject. Once this examination concludes, the polygraph examiner will provide the case agent with all originally collected documents and a subsequent written report of the examination.

Polygraph examinees complete forms (e.g. TCIU Security Questionnaire; ICE Polygraph Statement of Consent form; and the Statement of Rights and Waiver Form) based on one of the three HSI PEs being administered.

Sources of information include:

- Members of the public (U.S. and non-U.S. Persons);
- DHS Employees/Contractors (ICE, DHS, HQ); and
- Employees of other federal agencies: U.S. Department of Justice (DOJ), Assistant United States Attorneys (AUSAs).

Data Elements:

The information maintained on the HSI-Net SharePoint site varies according to the type of information necessary for a specific PE. The HSI-Net SharePoint site stores documents which may contain:

- Name;
- Date of birth (DOB);
- Place of birth (for criminal investigations, national security, and foreign vetting of law enforcement personnel abroad);
- Height;
- Weight;
- Gender;
- Eye and hair color;
- Address;
- Phone number;[77]
- Email address;
- Social Security number (SSN) (for criminal investigations, National Security);
- A -Number (for criminal investigations only);[78]
- Driver's License/State ID number (for criminal investigations, and National Security); [79]

[77] Phone numbers are collected on the "TCIU Security Questionnaire."

[78] The polygraph examiner checks the examinee's A-Number to confirm they are the individual that the polygraph examiner is supposed to polygraph but does not collect it. A case agent could discuss an examinee's A-Number with a polygraph examiner.

[79] The polygraph examiner checks the examinee's Driver's License number to make sure it is the subject the polygraph examiner is supposed to polygraph but do not record it, write it, or keep it as a practice. The polygraph examiner just checks it to make sure *John Doe* is the *John Doe* in the room.

- National Identification number used in lieu of an SSN. The National Identification number is being used in lieu of an SSN to uniquely identify the polygraph examinee (e.g., local identification (for foreign vetting of TCIU personnel abroad);
- Country of citizenship (for criminal investigations, national security, and foreign vetting of TCIU personnel abroad);
- Employment Information (e.g., occupation, month/year employed, employer, reason for leaving) (for criminal investigations, national security, and foreign vetting of TCIU personnel abroad);
- Medical history information (e.g., medication, including type, and reason for consulting a doctor for a nervous or mental condition) (for criminal investigations, national security, and foreign vetting of TCIU personnel abroad);
- Criminal history information (e.g., month/year, offense, disposition) (for criminal investigations, National Security, and foreign vetting of TCIU personnel abroad);
- Education information (e.g., education level, last school attended degree/major) (for criminal investigations, national security, and foreign vetting of TCIU personnel abroad);
- Military service information (e.g., service, rank, discharge) (for criminal investigations, national security, and foreign vetting of TCIU personnel abroad);
- Social media information (e.g., social media handle/ID) (for criminal investigations, national security). Polygraph examiners do not include any social media information or content within HSI Polygraph SharePoint files. If a PE revealed derogatory or concerning information regarding an individual's online activities, it would be noted in an investigative ROI or ICE Investigative Case Management (ICM)[80] report that is stored on the HSI Polygraph SharePoint site as part of a complete Polygraph file.

Due to the nature of the documents this may not be an exhaustive list of data elements collected by the site.

SORN Coverage:

- DHS/ICE-009 External Investigations,[81] which provides coverage for information on criminal investigation PEs collected, and stored in HSI Polygraph SharePoint site;
- DHS/ICE-010 Confidential and Other Sources of Information,[82] which provides coverage for criminal investigation PEs is used to verify information furnished by an informant;

[80] *See* DHS/ICE/PIA-045 Investigative Case Management, *available at* https://www.dhs.gov/compliance.
[81] *See* DHS/ICE-009 External Investigations, 85 FR 74362 (Nov. 20, 2020).
[82] *See* DHS/ICE-010 Confidential and Other Sources of Information, 78 FR 7798 (Feb. 4, 2013).

- DHS/ALL-023 Department of Homeland Security Personnel Security Management,[83] which provides coverage information collected for the purpose of processing personnel security-related actions and verifying eligibility for assignment to a sensitive position, including for the national security, and foreign law enforcement vetting PEs;
- DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management,[84] which covers foreign law enforcement vetting polygraph candidates are provided access to FLETC as students; and
- DHS/ALL-039 Foreign Access Management,[85] which covers the foreign national law enforcement vetting PE, and foreign national law enforcement who are provided access to FLETC.

Records Retention Period:

The Polygraph schedule has not been approved, to date, so all records are considered permanent until an approved schedule has been published. Currently, the polygraph records are retained by the HSI Forensic Lab as the following:

PE files are saved in SharePoint and copies of those files are burned to a compact disc (CD/DVD) at the end of each fiscal year. These compact discs are stored in the Polygraph Storage Room, which is secured, and physical access is restricted/limited to designated individuals at the Laboratory.

Polygraph administrative files are saved on the laboratory's shared server and electronic access is restricted/limited to management and members of the Polygraph Unit.

[83] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 85 FR 64511 (Oct. 13, 2020).

[84] *See* DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).

[85] *See* DHS/ALL-039 Foreign Access Management System of Records, 83 FR 19078 (May 1, 2018).

Appendix S

Program/System:

U.S. Immigration and Customs Enforcement (ICE) Health Service Corps (IHSC)/Health Care Compliance Division Unified Patient Tracking System (UPTS)

Purpose and Use:

UPTS centralizes ICE noncitizen clinical data ingestion from IHSC and non-IHSC facilities,[86] and provides automated notifications, and generates clinical case reports in accordance with, and in support of, *IHSC Directive 03-32 - Significant Detainee Illness* and *IHSC Directive 01-25 - Significant Event Notification and Significant Medical Case Reporting*.

Significant events are defined in policy as events that occur at ICE facilities including, but not limited to, abuse or neglect, serious injury, medical or psychiatric emergencies, medical errors, suicide attempts, hunger strikes, hospital admissions and discharges, death, and sexual assault.

On receipt of a Significant Event Notification from ICE ERO, IHSC is required to intake the Significant Event Notification and ensure appropriate delivery to stakeholders which may include IHSC leadership, IHSC unit chiefs, regional clinical directors, and others. Currently, Significant Event Notifications are being transmitted via email to the required parties resulting in inconsistent messaging, lack of central visibility of the flow of information, and lack of ability to query Significant Event Notification data. Furthermore, incidents may be identified by IHSC staff prior to an ICE ERO Significant Event Notification. These cases are designated as Pre-Significant Event Notifications as an ERO Significant Event Notification. These are cases that may or may not follow ERO criteria, but are required for IHSC visibility. UPTS allows IHSC to centralize clinical case data, provide consistent notifications, and allow for Pre-Significant Event Notification and Significant Event Notification data to be reportable.[87]

System Access:

Only the three groups of UPTS users listed below have access to the data in UPTS, which is managed through Microsoft 365. These three groups are:

- Managed care coordinators (MCCs);
- Case points of contact (POCs); and
- IHSC leadership.

Individuals Impacted:

IHSC staff that use this site and members of the public who are the subjects of ICE records.

[86] *See* DHS/ICE/PIA-037 Electronic Health Records System (her), *available at* https://www.dhs.gov/compliance.
[87] *See* DHS/ICE/PIA-023 Significant Event Notification System, *available at* https://www.dhs.gov/compliance.

Sources of Information:

Granted IHSC users (see System Access above) input information into the system. Information may come directly from medical staff at IHSC or non-IHSC facilities. Information may also be relayed from off-site medical staff when a noncitizen is off-site, such as during an inpatient hospitalization.

Data Elements

UPTS assigns each case a specific case number. Initial case entry also automatically creates a case ID. Additional case information contains noncitizen's A-Number, first and last name, date of birth, country of citizenship, date of arrival, case point of contact (POC) (IHSC staff responsible for updates), case status (open/closed), Significant Event Notification status, Significant Detainee Illness (SDI) status, facility name, notification recipients, and a running list of case narrative updates. The following respective case types have specific additional information collected:

- Hospital Admission and Discharge case type collects the additional fields: admit date, discharge date, current diagnosis, relevant medical history, serious injury indicator, serious injury location (if applicable), discharge plan, condition on discharge, attending physician, reporting staff name, reporting staff title.
- Emergency Department Referral case type collects the additional fields: referral date, discharge date, referral reason, current diagnosis, relevant medical history, attending physician, reporting staff name, reporting staff title.
- Hunger Strike case type collects the additional fields: relevant diagnosis/history, reason for hunger strike, initial stats (accepting/refusing care), initial medical status (stable/unstable), date hunger strike declared, days on hunger strike, date of first missed meal, first meal missed (breakfast/lunch/dinner), court order obtained (for force feed), date force feed initiated, number of forced feedings, date of intake at facility hunger strike declared, intake weight, intake height, date of last recorded weight before hunger strike, last body mass index prior to hunger strike, date of most current weight, most current weight, most current body mass index (BMI), current status, current medical status, weight change from pre-hunger strike, percent weight change from pre-hunger strike, whether transferred to different facility, if transferred date of transfer, receiving facility, receiving facility name, whether transported to emergency department/hospital, date hunger strike terminated.
- Suicide Attempt case type collects the additional fields: date of entry into ICE custody, IHSC behavioral health unit (BHU) POC, date of current attempt, current attempt method, current attempt location, current status, date placed on suicide watch, date removed from suicide watch, whether transported to emergency department/hospital, history of prior suicide attempt(s), relevant diagnosis/history, date of post-attempt mental health evaluation, whether higher level of care required.

- Psychiatric Emergency case type collects the additional fields: IHSC BHU POC, whether transported to emergency department/hospital, relevant diagnosis/history, date of last psychiatric evaluation, current status, medical classification level, psychiatric/mental health classification level, whether compliant with psychiatric medication regimen.
- Death case type collects the additional fields: IHSC executive leadership notification, date of death, time of death, cause of death, place of death, relevant diagnosis/history, date of last assessment/evaluation.
- Pregnancy case type collects the additional fields: initial specialty consultation date, date of last menstrual period, expected delivery date, current trimester, pregnancy risk status, nursing/breastfeeding status, relevant history/diagnosis, taking prenatal vitamins, date of last assessment/evaluation, current updates to include any special needs, gravida/para/abortion, delivery date, whether higher level of care required.
- Transgender case type collects the additional fields: preferred name, facility date of transgender identification, date removed/released from facility, identify as male/female.
- Abuse or Neglect case type collects the additional fields: IHSC Behavioral Health Unit (BHU) Point of Contact (POC), referral reason, date abuse/neglect occurred, location of abuse/neglect, whether transported to emergency department/hospital, relevant diagnosis/history, date of last physical assessment/evaluation, current status, whether higher level of care required,
- Sexual Assault case type collects the additional fields: prior sexual assault activity, location sexual assault occurred, current facility location, date assault occurred, whether transported to emergency department/hospital, relevant diagnosis/history, date of last physical assessment/evaluation, current status, whether higher level of care is required, medical classification level, whether referral to specialist is required, whether referred to a specialist.

SORN Coverage:

- DHS/ICE-013 Alien Health Records System,[88] which covers the collection, maintenance, and sharing of medical information for individuals in the interest of public health, especially in the event of a public health emergency, such as an epidemic or pandemic.

Records Retention Period:

Records maintained in the UPTS are unscheduled. The records must be maintained permanently until a schedule has been approved by National Archives and Records Administration (NARA).

[88] DHS/ICE-013 Alien Health Records System, March 19, 2018, 83 FR 12015.

Appendix T

Program/System:

Victim Assistance Program (VAP) Database SharePoint Site.

Purpose and Use:

The ICE Homeland Security Investigations (HSI) Victim Assistance Program (VAP) is responsible for implementation of the HSI mission pertaining to victim-centered investigations and victim-related issues. The VAP provides victim-centered assistance throughout investigations, and provides technical assistance to HSI Special Agents, Victim Assistance Specialists (VAS), and Forensic Interview Specialists. HSI Victim Assistance Specialists assist thousands of victims investigated by HSI annually to ensure compliance with statutes pertaining to victims of federal crimes. The majority of VAP investigated cases include: human trafficking, child exploitation, and traveling child sex offenders.

The HSI VAP Database (VAD) is a SharePoint site that allows HSI to track cases regarding victims who either contact, or are contacted by, the VAP. The SharePoint site generates crime victim statistical reports for internal U.S. Government use, and for external reporting purposes. The SharePoint site currently consists of a dashboard with a drop-down menu and free-text fields that include information on: the victim, nature of the crime, the designated Special Agent in Charge office (SAC office), referral type, type of investigation, and operation name. Examples of referral type, type of investigation include: child exploitation, human trafficking, and female genital mutilation.

System Access:

Only designated HSI personnel with a need to know have access to the files and other PII on the SharePoint site. Individuals without a need to know can only view the request form and his or her submitted requests.

Individuals Impacted:

Members of the public as well as ICE employees and contractors.

Sources of Information:

Information comes from the Victim Assistance Specialist and Coordinators inputting referral information, and other associated information directly into fields on the site.

Data Elements:

The site contains Victims of Immigration Crime Engagement Office (VOICE)[89] data which fell within the VAD that is no longer being captured or actively used.

[89] On April 26, 2017, former U.S. Department of Homeland Security Secretary John F. Kelly announced the official launch of the U.S. Immigration and Customs Enforcement (ICE) Victims of Immigration Crime Engagement Office. (VOICE). The VOICE office will assist victims of crimes committed by noncitizens.

Victim Data continues to include:

- Month/year of birth;
- Age;
- Gender;
- Date referred;
- Minor (Yes/No;)
- Citizenship;
- Type of victimization;
- Type of victim service referral;
- Casen number (Investigative Case Management (ICM)) System;[90]
- Case Agent name (first and last);
- Victim Assistance Coordinator name (first and last);
- Time spent per case; and
- Special Agent in Charge office.

SORN Coverage:

- DHS/ICE-009-External Investigations[91]

Records Retention Period:

VAP records are currently unscheduled. The records must be maintained permanently until a records schedule has been approved by NARA.

[90] *See* DHS/ICE/PIA-045 Investigative Case Management (ICM), *available at* https://www.dhs.gov/privacy-documents-ice.
[91] DHS/ICE-009 External Investigations System of Records, 85 FR 74362 (November 20, 2020).

Appendix U

Program/System:

National Security Division (NSD) SharePoint

Purpose and Use:

The Homeland Security Investigations (HSI) National Security Division (NSD) is a key component of the U.S. Immigration and Customs Enforcement (ICE) HSI Directorate and plays a key role in advancing the ICE mission. The National Security Division leads the effort to identify, disrupt, and dismantle transnational criminal enterprises and terrorist organizations that threaten the security of the United States.

The National Security Division protects the United States through the following activities:

- Enhancing national security through criminal investigations;
- Preventing acts of terrorism by targeting the people, money, and materials that support terrorist and criminal activities; and
- Identifying and eliminating vulnerabilities in the nation's border, economic, transportation, and infrastructure security.

The National Security Division mission is strengthened by the unique combined investigative authorities that HSI commands. HSI's combined authorities for enforcing immigration and customs law serve as a powerful tool in national security investigations.

The National Security Division is led by a Senior Executive Service - Assistant Director who oversees two programmatic functions and is directly supported by the National Security Programs Support Group. The National Security Division uses SharePoint for a variety of purposes such as mission support collaboration and record keeping, communication, and information sharing within and across National Security Division, and some coordination with external partners. All evidence, leads, and investigative work products are stored in ICE case management systems.[92]

Site functionalities include:

- The National Security Division Document Libraries include high level reports for the division; signed information sharing agreements (e.g., Memoranda of Understanding and Memoranda of Agreement); mission support records such as budget, personnel, performance, property, and security; official correspondence templates; working documents and records at the unit and section levels; as well as leadership photos, contact information, biographies, and branded challenge

[92] *See* DHS/ICE/PIA-044 LeadTrac and DHS/ICE/PIA-045 Investigative Case Management System (ICM), *available at* https://www.dhs.gov/compliance.

coins. The National Security Division SharePoint site is a primary repository for Division mission support records which include PII.

- The Counterterrorism Section private subsite stores A-Files, which include date of birth, A-Number, Social Security number, passport number, and family information, to facilitate file sharing with field HSI Joint Terrorism Task Force agents, HSI Headquarters Joint Terrorism Task Force Program Managers and Analysts, and attorneys from the Office of the Principal Legal Advisor-National Security Law Division. The A-Files are immediately removed from the site when the physical A-File arrives or there is no longer a need for the file.

System Access:

Access to the SharePoint site is restricted to the National Security Division federal employees and limited contracted or external staff currently working with the National Security Division. Access to subsites and libraries containing Sensitive Personally Identifiable Information (SPII) or program-specific content is restricted to SharePoint site administrators, related leadership, and the National Security Division personnel with a verified need to know. The site has three designated administrators to manage permissions, functionality/design, and site use.

Individuals Impacted:

The subjects of counterterrorism investigations, and federal employees and contractors.

Sources of Information:

No other system is connected to the National Security Division SharePoint site. Information is gathered directly from personnel who create and upload documents. During the investigative process the National Security Division personnel search a variety of government databases and non-government sources, including open-source systems on the internet and social media sites.

Data Elements:

Data elements collected by the National Security Division varies based on the mission of the program, group, or unit.

Information collected from ICE employees include:

- Name;
- Date of birth;
- Job title;
- Phone number;
- Social Security number;
- Unit/Office;

- Agency;
- Division;
- Work email address;
- Work and home addresses;
- Travel details;
- Disciplinary action;
- Resume information; and
- Security clearance.

Information collected from other federal employees (i.e., Task Force Officers) include:[93]

- Name;
- Employer;
- Email; and
- Phone number.

Information collected from subjects of counterterrorism investigations includes the relevant contents of an individual's A-File. Those data elements include, but are not limited to:

- A-Number;
- Receipt file number;
- Full name and aliases;
- Physical and mailing addresses;
- Phone numbers and email addresses;
- Social Security number;
- Date of birth;
- Place of birth;
- Country of citizenship;
- Country of residence;
- Gender;
- Physical characteristics;

[93] This includes Federal Bureau of Investigations Task Force Officers.

- Government-issued identification information;
- Military membership and/or status;
- Federal Bureau of Investigation (FBI) Identification Number/Universal Control Number; Fingerprint Identification Number;
- Immigration enforcement history and status;
- Family history;
- Travel history;
- Education history;
- Employment history;
- Criminal history;
- Professional accreditation information;
- Medical information; and
- Social media handles and aliases associated identifiable information, and search results.

Information collected from prospective National Security Division employees and visitors to the National Security Division include:

- Name;
- Date of birth;
- Job title;
- Phone number;
- Social Security number;
- Unit/Office, agency, and division;
- Contact information: email, work, and home addresses; and
- Resume information.

SORN Coverage:

- DHS/ICE-009 External Investigations SORN,[94] which outlines the collection of PII for administrative, intelligence, and law enforcement investigations;

[94] DHS/ICE-009 External Investigations System of Records, 85 Fed. Reg. 74362 (Nov. 20, 2020).

- DHS/ALL-002 Mailing Lists SORN,[95] which covers the collection of contact information for administrative purposes;
- OPM/GOVT-1 General Personnel Records,[96] which covers the collection of personnel records files and reports of personnel actions relating to an employee's federal service;
- OPM/GOVT-2 Employee Performance File System Records,[97] which covers the collection of employee performance evaluations;
- OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers,[98] which covers the documentation of disciplinary actions of ICE employees contained in the SharePoint site;
- OPM/GOVT-5 Recruiting, Examining, and Placement Records,[99] which covers the collection of resumes for purposes of hiring; and
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records,[100] which covers ICE's use of an individual's A-File for purposes of documenting and reviewing an individual's immigration history.

Records Retention Period:

The National Security Division will keep documents on the SharePoint site if there is a business need and/or in accordance with the HSI General Records Schedule. Document owners will remove documents when either deadline is met. SharePoint administrators will periodically audit the site to ensure document owners are deleting outdated documents or information from SharePoint. Information that reflects data gathered in the National Security Division casework will reside in source systems, such as LeadTrac or the Investigative Case Management System. A-Files must be retained permanently.

All data within the National Security Division SharePoint site is considered temporary and/or duplicate data. Official records are retained in case files, A-Files, or ICE case management systems such as LeadTrac or the Investigative Case Management System.

SharePoint site administrators will routinely audit the site for old and unused files. HSI supervisors will ensure that all information will be disposed or deleted in accordance with ICE evidentiary custodial protocols.

---

[95] DHS/ALL-002 DHS Mailing and Other Lists System, 73 Fed. Reg. 71659 (Nov. 25, 2008).

[96] OPM/GOVT-1 General Personnel Records, 80 Fed. Reg. 74815 (Nov. 30, 2015).

[97] OPM/GOVT-2 Employee Performance File System Records, 80 Fed. Reg. 74815 (Nov. 30, 2015).

[98] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, 80 Fed. Reg. 74815 (Nov. 30, 2015).

[99] OPM/GOVT-5 Recruiting, Examining, and Placement Records, 80 Fed. Reg. 74815 (Nov. 30, 2015).

[100] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (Sept. 18, 2017).

Appendix V

Program/System:

ICE Freedom of Information Act (FOIA) SharePoint Site

Purpose and Use:

ICE FOIA is a unit within ICE's Office of Information Governance and Privacy (OIGP) program office that provides access to agency records to requesters unless those records are protected from public disclosure by exemptions of the FOIA (5 U.S.C. § 552) and the Privacy Act of 1974 (5 U.S.C. § 552a). The ICE FOIA SharePoint Site will be used as a temporary repository for responsive records.[101] ICE FOIA will not be processing FOIA requests on the SharePoint Site. This portion of the SharePoint site will serve as method for ICE program offices to send ICE FOIA responsive records that are too large to be sent via email and/or cannot be uploaded directly to SecureRelease[102] by the program office. The SecureRelease system has file type and size limitations. Additionally, ICE FOIA Litigation does not release their productions through SecureRelease. This portion of the SharePoint Site will serve as a holding location for these documents.

The ICE FOIA SharePoint Site will also be used to gather, store, and disseminate Standard Operating Procedures (SOP), guidance, and training. Point of contact (POC) lists (e.g., name, contact information) are stored on the site for internal communication, collaboration, and information exchange between ICE FOIA personnel, ICE program office points of contact, and external points of contact. ICE FOIA will also use the ICE FOIA SharePoint to track the approval and posting of proactive disclosures[103] on the public facing ICE FOIA Library, as required by the FOIA.

System Access:

Only designated employees, and limited contracted or external staff, currently working with the ICE FOIA Unit with a need to know have access to the ICE FOIA records on the internal SharePoint site. Individuals without a need to know can only view the request form and their submitted requests. The site has a designated administrator who verifies a users' need to know prior to granting access to the site and libraries that may contain Sensitive PII. The site administrator also conducts routine audits to ensure that user permissions are applied appropriately and there is no unauthorized information posted to the site.

[101] A responsive record is a record that refers to a document that fits the specific set of records requested.

[102] SecureRelease is a cloud-based platform for FOIA and transparency management, *see* https://www.securerelease.us/.

[103] A proactive disclosure is a disclosure where agencies make their records publicly available without waiting for specific requests from the public.

Individuals Impacted:

ICE employees and contractors involved in processing FOIA requests, and members of the public (e.g., U.S. Citizens, Lawful Permanent Residents, non-U.S. persons) who are the requesters and subjects of FOIA requests.

Sources of Information:

Information is provided to the Department by: individuals who submit FOIA and/or Privacy Act requests; individuals who appeal DHS' denial of their FOIA and/or Privacy Act requests; individuals whose requests, appeals, and/or records have been referred to DHS by other agencies; and, in some instances, attorneys or other persons representing individuals submitting such requests and appeals; individuals who are the subjects of such requests; Department of Justice (DOJ) and other government litigators, and/or DHS personnel assigned to handle such requests or appeals. Information provided to the Department for FOIA and/or Privacy Act requests is done voluntarily. FOIA and Privacy Act requestors are not required to submit any of the information recorded in the Department's systems, but without it, DHS may be unable to properly respond to requests. Other sources of information sent to the Department's FOIA and Privacy Act program includes:

- Internal DHS components;
- Other federal agencies;
- Congressional offices;
- State and local governments;
- Foreign officials or governments;
- U.S. and foreign corporations;
- Non-government organizations, such as media or watchdog groups; or
- Others in the general public.

Data Elements:

All agency records under the control of ICE can be the subject of a FOIA request, resulting in the records being posted in FOIA. Documents posted to the ICE FOIA Unit SharePoint site may contain PII about members of the public, including, but not limited to, name, date of birth, country of birth, gender, address, phone number, identification information (e.g., driver's license number, passport number, A-Number, Social Security number), photographs, criminal arrest records, immigration-related data, personnel records, and medical records. All such information comes from programs and systems (e.g., the ICE Enforcement Integrated Database[104]) that are covered by separate privacy documentation. Information about ICE FOIA personnel includes name,

[104] *See* DHS/ICE/PIA-015 Enforcement Integrated Database, *available at* www.dhs.gov/privacy.

employment information (e.g., office, group, position, training, supervisor), and contact information (e.g., office location, phone numbers, email addresses).

SORN Coverage:

- DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System,[105] which covers the processing of record access requests and administrative appeals under the FOIA, as well as access, notification, and amendment requests and administrative appeals under the Privacy Act, whether DHS receives such requests directly from the requester or via referral from another agency; and
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS),[106] which covers how DHS collects PII in order to provide authorized individuals access to, or interact with DHS information technology resources, and allow DHS to track use of DHS Information Technology resources.

Records Retention Period:

FOIA access and disclosure request files must be retained in accordance with GRS 4.2 Information Access and Protection Records Item 010, destroy six years after final agency action or three years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.

FOIA-related Standard Operating Procedures, guidance, and policies must be retained in accordance with DHS Administrative and Operational Records Common to All Offices schedule DAA-0563-2019-0008-0005, Administrative Directives, cutoff when superseded or cancelled, destroy seven years after cutoff.

[105] DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, 79 FR 6609 (Feb. 4, 2014).
[106] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).