



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,

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.



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.

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 SORN² 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.

² All ICE SORNs are published in the *Federal Register* and on the DHS Privacy Office website at <http://www.dhs.gov/system-records-notice-sorn>.



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 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.

³ See 5 U.S.C. § 552.



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:
 - 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

⁴ See 5 U.S.C. § 552a(b).



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 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.

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 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.



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, or general information request).

SORN Coverage:

DHS/ALL-016 Department of Homeland Security Correspondence Records⁵

Records Retention Period:

ICE intends to request National Archives and Records Administration (NARA) approval to retain CAIRS records for seven years after the record was entered into the system.

⁵ 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)⁶

Records Retention Period:

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

⁶ 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;⁷
DHS/ALL-004 General Information Technology Access Account Records System⁸

⁷ DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (Nov. 25, 2008).

⁸ DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).



Records Retention Period:

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.