Privacy Impact Assessment

for the

Information Technology Service Management - ServiceNow

DHS Reference No. DHS/ICE/PIA-059

January 12, 2020

Homeland Security

Abstract

The U.S. Immigration and Customs Enforcement (ICE) Office of the Chief Information Officer (OCIO) operates the Information Technology Service Management (ITSM) - ServiceNow enterprise solution (ServiceNow). To better support its mission of streamlining the management of time-sensitive service requests, OCIO implemented a software as a service (SaaS) cloud-based tool that can be customized based on the needs of ICE program offices to provide support to ICE personnel (i.e., employees, contractors) and non-ICE personnel who have access to ICE systems for official business. ICE is publishing this Privacy Impact Assessment (PIA) to provide a thorough analysis of the privacy risks associated with ServiceNow's collection, use, and maintenance of personally identifiable information (PII).

Overview

ServiceNow specializes in the delivery of ITSM applications to commercial and government customers. It has an array of applications and functionalities that allow for workflow automation and incident management, thus making the management of service requests more efficient. ServiceNow uses its request management function to streamline service delivery for user requests, eliminates the duplication of efforts, ensures information accuracy, and reduces operational costs through a published catalog of information technology (IT) services, all driven by automated workflows, approval rules, and service level agreements. Moreover, email notification updates keep end users informed about the status of their service requests.

ServiceNow is used by U.S. Department of Homeland Security (DHS) Headquarters and component offices. Within ICE, the IT Service Desk and other ICE program offices, such as the Office of Enforcement and Removal Operations (ERO) and the Office of Human Capital (OHC), use ServiceNow to allow ICE personnel and non-ICE personnel[1] to create service requests, report technical issues, manage agency taskers, track and automate business processes, and generate reports. For example, OHC uses ServiceNow to create and track human resource-related inquires/questions. This PIA includes appendices that provide further details on each ICE program's use of ServiceNow. The types of information collected by ServiceNow depends on the business purpose for its use. This may include information about the IT system, software, or technology-related information, and/or information about individuals (i.e., PII).

Accessibility and Functionality

The ICE ServiceNow software is hosted in the Federal Risk and Authorization

[1] Non-ICE personnel in this context includes any DHS employee who has been vetted and granted access to the ICE network. This may include personnel from Cybersecurity and Infrastructure Security Agency (CISA), Federal Protective Service (FPS), Office of Biometric Identity Management (OBIM), DHS Headquarters (DHS HQ), U.S. Citizenship and Immigration Services (USCIS), and U.S. Customs and Border Protection (CBP). This also includes employees of other federal agencies detailed to ICE.

Management Program (FedRAMP)-certified ICE cloud. The Management, Instrumentation, and Discovery (MID) servers that provide integration capabilities are also hosted on the ICE cloud. ServiceNow is made available to each ICE program office on individual ICE ServiceNow Server Sites[2] and is available to users on the secured ICE intranet (IRMnet). However, accessibility and functionality restrictions are defined by user roles based on Access Control Lists (ACL). Each user role has defined and limited access authority to view and edit data sets by an ICE ServiceNow master administrator.

The authorized master administrators have full access to create/modify all aspects of the configuration including but not limited to: data entry screens, workflows, databases, reports, and libraries; and provide fully automated audit capabilities of all configuration changes. Other user roles include:

- Security Administrator – security administrators are similar to master administrators, but they have read-only access to everything except the application's audit logs page which is maintained by ICE OCIO. Only security administrators and master administrators can view, export, and clear the audit;
- Administrator – administrators have permission to view and edit any information to which they have access. Administrator accounts are assigned to those who have a need to access, edit, or configure the organization's projects, continuous assessment settings, and reports;
- Auditor/Executive – auditor/executive accounts are similar to administrators but have read-only access. Executive accounts are intended for managers who need to monitor progress, compliance, and risk levels;
- End Users – user accounts are typically given to analysts (i.e., service representatives) who will require basic access to the system. Users typically must be assigned to a project in order to access it. Users do not have administrative rights over their projects.
- Requestors – ICE personnel may create tickets for themselves or on behalf of others and are able to the view the status of their own tickets.

[2] A Server Site is a collection of users, groups, and content walled-off from any other site's content on the same instance of ServiceNow server.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

ICE is authorized to collect this information pursuant to 5 U.S.C. § 301 "Departmental Regulations", 8 U.S.C §§ 1101, 1103, 1104, 1201, 1255, 1305, 1360 "Aliens and Nationality", and 44 U.S.C. § 3101 "Records Management by Federal Agency Heads".

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Coverage for the information managed in ServiceNow is provided by the below SORNs. Additional SORN coverage may be outlined in the appendices of this PIA as new ServiceNow use cases arise.

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS),[3] which outlines how DHS collects information from employees in order to provide authorized individuals with access to DHS information technology resources;
- DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System,[4] which covers the collection and management of PII for the purpose of issuing credentials for access to DHS facilities and information systems;
- DHS/ALL-033 Reasonable Accommodations Records System,[5] which covers records collected on applicants for employment, as well as employees with disabilities who requested or received reasonable accommodations by the Department;
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[6] which discusses information collected to support the detention and removal of individuals unlawfully entering or present in the United States;
- DHS/ICE-013 Alien Health Records System,[7] which outlines how ICE documents

[3] *See* DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792 (Nov. 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[4] *See* DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System, 74 FR 30301 (June 25, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.
[5] *See* DHS/ALL-033 Reasonable Accommodations Records System, 76 FR 41274 (July 13, 2011), *available at* https://www.dhs.gov/system-records-notices-sorns.
[6] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[7] *See* DHS/ICE-013 Alien Health Records System, 83 FR 12015 (Mar. 19, 2018), *available at*

and facilitates the provision of medical, dental, and mental health care to individuals in ICE custody in facilities where care is provided by the ICE Health Service Corps (IHSC); and

- OPM/GOVT-1 General Personnel Records,[8] which covers records maintained by the Office of Personnel Management (OPM) and agencies to provide a basic source of factual data about a person's federal employment while in the service and after his or her separation.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The ICE ServiceNow System Security Plan (SSP) was completed on April 24, 2020. The ServiceNow Authority to Operate (ATO) was completed on June 3, 2020.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The NARA General Records Schedule (GRS) DAA-GRS-2013-0005-0004, Item 020 covers the records in ServiceNow. Records are retained for three (3) years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected in ServiceNow is not subject to the PRA as information is not collected directly from members of the public.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

ICE collects different information about the IT system, software, technology-related information, and/or individuals. The ServiceNow user interface allows ICE users to initiate a service request or submit an inquiry through the ICE Service Desk or specific ICE program office's

https://www.dhs.gov/system-records-notices-sorns.

[8] *See* OPM/GOVT-1 General Personnel Records, 80 FR 74815 (Nov. 30, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

instance of a self-service portal.[9] If a user seeks support via email or phone, an ICE technical support or customer service representative (hereafter "service representative") confirms the user's identity by mapping the identity information provided by the user to the user's account information in the ICE Active Directory.[10] Once the information is appropriately entered in ServiceNow, the system generates a unique ticket number and assigns it to the appropriate service representative. The ticket number is used to track the progress and to provide status updates to the user.

ServiceNow also offers a chat function to enhance communication with a service representative, and users may upload any relevant document directly into the self-service portal to assist with their request.[11] Only ICE personnel have access to the self-service portal to upload files that may contain PII (including Sensitive PII (SPII)) and are relevant to users' requests for service, inquiry, or support.[12]

Aside from collecting limited business and contact information when creating service tickets, ServiceNow allows program offices the capability to securely transmit and ingest information from ICE systems associated with the specific ICE operation, making the data available to ICE employees for workflow management, tracking, and reporting purposes. The information that may be ingested from other ICE source systems include:

- Biographic and biometric information;
- User information and log-in credentials;
- Human Resource (HR)-related information;
- Health and medical information;
- Criminal history information;
- Description of service request; and
- Other identification information.

The Appendices included in this PIA, provide further details on each type of information collected by each ICE program's use of ServiceNow.

[9] Information collected on program office A's portal cannot be viewed by program office B.
[10] Active Directory is Microsoft's directory service that is used by computers running Microsoft Windows to identify machines, networks, and users (similar to an electronic rolodex).
[11] The ICE Privacy Unit is working with OCIO to implement a warning banner in ServiceNow to remind users that PII/SPII should only be entered into the ticket and/or uploaded when required to complete service requests. Additionally, ICE service representatives are trained to contact the ICE Security Operations Center (SOC) and the ICE Privacy Unit to report any unnecessary PII/SPII that users provide via the self-service portal
[12] Non-ICE personnel can submit service requests or inquiries via phone or email.

2.2 What are the sources of the information and how is the information collected for the project?

ServiceNow collects information directly from ICE personnel and non-ICE personnel with vetted access to ICE systems. Only ICE personnel may upload attachments, which are used to aid in the remediation of incidents, respond to an HR-inquiry, or resolve technical issues. These attachments may contain PII or SPII about ICE employees and the public (e.g., benefit requestors, beneficiaries). The uploaded information is used only for reference purposes and is not transferred, accessed, or manipulated by any other system. System administrators provide their own information for system access and/or to perform their duties.

ServiceNow also ingests data from other ICE source systems, such as the ICE Enforcement Integrated Database (EID),[13] in order to manage and track program initiatives.[14]

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, ServiceNow does not use any commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The user provides his or her information directly through the self-service portal. ServiceNow prepopulates the user's information (e.g., name, work location) from the user's ICE Active Directory account for identification and authentication. Alternatively, if an individual contacts the ICE Service Desk either for technical support, to submit an inquiry, or to report a security incident, the service representative confirms the user's identity by mapping the identity information provided by the user to the user's account information in the ICE Active Directory.

The accuracy of data from manual uploads/attachments depends on the collection methods of the user and the originating source system. If a user manually uploads information into ServiceNow as part of a service request, it is the responsibility of the user to ensure that the information is accurate and relevant. The accuracy of the data ingested from other ICE systems is ensured by the source systems themselves.[15]

---

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[14] Additional information about the ingesting of data from other ICE source systems is provided in the Appendices.

[15] For example, if a user submits a ServiceNow request containing information from ICE's EID system, then it is incumbent upon the EID system owner and administrators to ensure data accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information will be included in the system that is not necessary or relevant to accomplish the system's purpose.

Mitigation: This risk is partially mitigated. ICE mitigates this risk by requesting only the minimum amount of information (e.g., name, work contact information) from the user when creating a service request ticket or submitting an inquiry. ICE personnel who have access to the self-service portal may upload additional supporting documents when creating a service request ticket. Although ServiceNow has technical safeguards in place to limit the types and sizes of the uploaded files, there are no technical restrictions on the type of PII/SPII the uploaded documents may contain. The ICE Privacy Unit is working with OCIO to implement a warning banner in ServiceNow to remind users that PII/SPII should only be entered into the ticket and/or uploaded when required to complete service requests. Additionally, ICE service representatives are trained to contact the ICE Security Operations Center (SOC) and the ICE Privacy Unit to report any unnecessary PII/SPII that users provide via the self-service portal, at which point the PII/SPII spill will be investigated and processed as a potential privacy incident. The PII/SPII is also scrubbed from ServiceNow according to guidance in the ICE Service Desk Standard Operating Procedure (SOP). If users must input PII/SPII to fulfill a service request, such as for OHC inquiries, only OHC-approved personnel and ICE ServiceNow administrators have the ability to view the information.

Privacy Risk: There is a risk that information included in service requests received by phone will be inaccurately entered into ServiceNow.

Mitigation: This risk is mitigated. ICE service representatives ensure that the information entered into ServiceNow is attributed to the appropriate individual by asking a series of questions to confirm the individual's identity when creating a service request ticket by phone. The information gathered by the service representative is compared to the individual's ICE Active Directory account.

Information collected from system administrators is deemed accurate as those individuals self-report their information for system access and/or to perform their duties, and can request to have their information corrected, in the event that there are discrepancies.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

ServiceNow offers workflow automation and incident management, thus making the management of service requests more efficient. Users submit limited information in the self-

service portal or via phone, when submitting service requests, inquiries, or reporting incidents. The information collected is used to verify the identity of the user and to provide technical support and other service-oriented support for ICE systems and applications and ICE employees.

Some ICE program offices (e.g., ERO) use ServiceNow to deploy specific solutions that manage and track program initiatives.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. ICE ServiceNow does not use its database for predictive patterns or abnormalities.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, only ICE personnel with a valid need-to-know can access the self-service portal to submit service requests or inquiries. Non-ICE personnel with vetted access to ICE systems can submit service requests or inquiries via phone or email.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that an individual will gain unauthorized access to ICE ServiceNow or inappropriately use information from it.

Mitigation: This risk is mitigated. ICE mitigates this risk through the implementation of appropriate administrative and technical safeguards such as privileged accounts that restrict access to authorized personnel with a valid need-to-know to perform official duties. ServiceNow is made available to each ICE program office on individual ICE ServiceNow Server Sites that are walled-off from any other site's content; thus, ensuring that one program office does not have access to another's information or data. System administrators set user roles to ensure appropriate access and use. Additionally, users access ServiceNow using Single Sign-On (SSO) for validation with Personal Identification Verification (PIV) card authentication[16] which authenticates the user by mapping to his/her ICE Active Directory account information.

[16] SSO is a method of access control that enables a user to log in at a single point and gain access to the resources of multiple software systems by using credentials stored on shared, centralized authentication servers. PIV-card authentication provides an extra layer of security by storing a user's SSO credential on a physical card that must be present at login.

When a user initiates the chat function of the ServiceNow self-service portal, prior to submitting a request, a warning message pops up to discourage unauthorized or improper use, access, or the processing of classified information in the system.

OCIO conducts regular audits of users and maintains audit logs of activity in the system in accordance with DHS 4300A Sensitive Systems Handbook.[17] These logs provide information on which files have been accessed, date/time they were accessed, who accessed them, and whether any records were updated or modified.

All ICE personnel take the annual Cybersecurity Awareness Training (CSAT) which emphasizes various topics from phishing, password management, data privacy, and other security topics. ICE's information security policy and acceptable use policy is also communicated to ICE personnel on an annual basis, and when they access ICE systems/applications.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

ICE users receive a general notice of the collection, intended use, and sharing of their information through the publication of this PIA and the DHS/ALL-004 GITAARS SORN. Additionally, the ICE Privacy Unit is working with OCIO to implement a warning banner in ServiceNow to remind users that PII/SPII should only be entered into the ticket and/or uploaded when required to complete service.

Since information maintained in other ICE systems (e.g., EID) may be ingested into ServiceNow, the notices provided by those originating source systems via their respective PIAs and SORNs, justify the collection and use of information derived from those systems.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

ICE users can choose to not provide their information to address their service request. However, failure to provide certain information may prevent service representatives from addressing the individual's matter in an efficient and effective manner.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware that their information is

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK (2015), *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

contained within ServiceNow.

Mitigation: This risk is partially mitigated. ICE mitigates this risk through the public notice provided by this PIA and the DHS/ALL-004 GITAARS SORN, and the corresponding ICE source system PIAs and SORNs for the ingested data. This risk is further mitigated as service representatives give verbal notice to users who submit requests via phone, concerning the use of their data during the identity verification process. For users who submit their information through the self-service portal, they will have notice of the collection and use of their information at the time of collection.

However, as information may be from ICE source systems covered by the DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) and DHS/ICE-013 Alien Health Records System SORNs, not all individuals will be aware that their information is being used in ServiceNow.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

The NARA-approved schedule for ServiceNow (identified in Section 1.4) allows for the destruction of records three (3) years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded. ICE may retain the records for more than three years, if required for business use or investigation.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained in ServiceNow for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: This risk is mitigated. ServiceNow records are retained in accordance with the NARA-approved GRS for agency activities related to the operations and maintenance of the basic systems and services used to support the agency and its staff. These types of system access records are appropriate in length given the agency's mission and the purpose of collection. DHS 4300A and the ICE Service Desk SOP outline the standardized process of deleting tickets and file types to ensure proper removal of records from the system.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

No. ICE does not share ICE ServiceNow information with external entities.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Not applicable.

6.3 Does the project place limitations on re-dissemination?

Not applicable.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Not applicable.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no privacy impact related to external information sharing because ICE does not share ServiceNow information with external entities.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to any of the records covered by this PIA may submit a request in writing to the ICE Freedom of Information Act (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
(202) 732-0660
http://www.ice.gov/foia/

U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information.

All or some of the requested information may be exempt from access pursuant to the Privacy Act and FOIA in order to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target 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.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a Privacy Act request in writing to the ICE Office of Information Governance and Privacy by mail:

U.S. Immigration and Customs Enforcement
Office of Information Governance and Privacy
Attn: Privacy Unit
500 Street SW, Stop 5004
Washington, D.C. 20536-5004
http://www.ice.gov/management-administration/privacy

All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests.

7.3 How does the project notify individuals about the procedures for correcting their information?

ICE provides general notice on the ICE's public-facing website about the procedures for submitting Privacy Act requests.[18] In addition, ICE provides notice to individuals via the applicable SORNs referenced in Section 1.2. Individuals may also have the option to seek access to and correction of their data directly from the ICE source systems from which data is ingested into ServiceNow.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to participate meaningfully in the use of their data as maintained in this system or determine whether the system maintains records about them.

Mitigation: This risk is mitigated. Much of the information in ServiceNow is input by the individual when submitting a request. They have access to this data and can correct it as needed. Further, redress and correction are provided by the Privacy Act and FOIA, when applicable. ICE notifies individuals of the procedures for correcting their information in this PIA and applicable SORNs, as well as through the ICE internal and public-facing websites.

[18] More information is *available at* https://www.ice.gov/foia/request.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

ICE users must complete ICE privacy and security training to include rules of behavior, appropriate uses of system data, uploading records, disclosure and dissemination of records, and system security before they gain access to ICE systems and applications. Users receive a notice reminding them that unauthorized or improper use or access may result in disciplinary action, as well as civil and criminal penalties, when they initiate the chat function in ServiceNow.

The ServiceNow system administrator monitors all account and user activity to the information system through monthly operation system scans and quarterly database scans. System administrators use automated tools (i.e., Splunk) to assist them in monitoring, analyzing, and reporting activities in the system.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

OCIO develops and disseminates ICE Privileged User Training to users with significant security responsibilities accessing ICE networks and systems. ICE Privileged User Training encompasses role-based training and as required by DHS supplemental guidance, OCIO assigns user's role and responsibilities. In addition to ICE Privileged User Training, all personnel who have access to the ICE network are required to take annual privacy and security training. The annual privacy and security training emphasize the importance of appropriate and authorized use of personal data in government information systems.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

ServiceNow technical safeguards (e.g., role-based access controls) ensure that only authorized users with a valid need-to-know have access to the information in the system to accomplish their assigned tasks. ICE ServiceNow accessibility and functionality restrictions are defined by user roles based on ACL. Each user role has defined and limited access authority to view and edit data set by an ICE ServiceNow Master Administrator. The user roles are determined on a need-to-know to perform official duties.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

ICE does not share information maintained in ServiceNow with organizations either within or outside the Department. However, should this change, bilateral information sharing agreements made with agencies external to DHS are vetted and reviewed by the appropriate ICE program and oversight offices and the external agency prior to being finalized and sent to DHS for formal review and clearance.

Contact Official

Rachelle B. Henderson
Chief Information Officer
Office of the Chief Information Officer
U.S. Immigration and Customs Enforcement
(202) 732-2000

Responsible Official

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement
(202) 732-3000

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: ICE Service Desk Ticketing and Incident Reporting System

Purpose and Use:

ServiceNow replaced Remedy, the legacy centralized IT ticketing system used to track IT issues reported by ICE users.[19] The ICE Service Desk serves as the single point of contact for logging, assigning, tracking, reporting, and resolving service requests. ServiceNow allows ICE users to create Service Desk tickets and report incidents. It also allows ICE Service Desk personnel to log tickets, classify tickets according to impact and urgency, assign to appropriate groups, escalate incidents, and manage tickets through to resolution.

ICE users can initiate a Service Desk ticket through the self-service portal, called the ICE IT Service Portal, or by contacting the Service Desk by phone or email.[20] ICE users can create tickets for themselves and can view the status of their own tickets. The categories of services include: reporting spam and phishing attempts; email account and software installation requests; group mailbox requests; and new ICE employee onboarding and personnel exit requests.

Relevant SORNs:

- DHS/ALL-004 General Information Technology Access Account Records (GITAARS)[21]
- DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System[22]
- OPM/GOVT-1 General Personnel Records[23]

Categories of Information:

Depending on the user submitting a Service Desk ticket or reporting an incident, ICE collects different information about the IT system, software, or technology-related information, and the user. This information includes:

- Employee name;
- IRMnet User ID;

[19] ServiceNow does not support Service Desk tickets for public users seeking IT support for public-facing systems.
[20] Non-ICE personnel with vetted access to ICE systems can submit service requests via phone or email only. They do not have direct access to the ICE IT Service Portal.
[21] *See* DHS/ALL-004 General Information Technology Access Account Records (GITAARS), 77 FR 70792 (Nov. 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[22] *See* DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System, 74 FR 30301 (June 25, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.
[23] *See* OPM/GOVT-1 General Personnel Records, 80 FR 74815 (Nov. 30, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Job title;
- Supervisor name and phone number;
- Agency and program office;
- Current location (i.e., home address, ICE office; temporary duty);
- Shipping address;
- Office/room number;
- Work phone number;
- Device affected (i.e., host name and Internet Protocol (IP) address);
- Employment type (i.e., employee, contractor, task force office, intern, and 287G);[24]
- Description of service request; and
- Any document relevant to the request.

If the user submits a request online, the user's information is automatically pre-populated based on his or her PIV card profile from the ICE Active Directory. Users may also upload documents to assist with their request. The uploaded information is used only for reference purposes and is not transferred, accessed, or manipulated by any other system. Once the information is appropriately entered in ServiceNow, the system generates a ticket with a unique number and assigns it to the appropriate Service Desk personnel to handle as appropriate. The ticket number is used to track the progress and to provide immediate update to the user.

The self-service portal also offers a chat interface to enhance communication between the Service Desk personnel and the user that submitted the request. Once the user initiates the chat function, the user's name is pre-populated based on his or her PIV card profile. Then the user can provide a short summary of the request in a free-text field before connecting with a Service Desk representative to obtain service support.

Service Desk personnel verify the identities of users and scrub unnecessary PII/SPII uploaded into the self-service portal in accordance with the ICE Service Desk SOP.

[24] The 287G program enhances the safety and security of communities by creating partnerships with state and local law enforcement agencies to identify and remove noncitizens who are amenable to removal from the United States. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE 287G PROGRAM, DHS/ICE/PIA-014 (2009), *available at* https://www.dhs.gov/privacy-documents-ice.

Appendix B: ICE Office of Human Capital Inquiry Portal

Purpose and Use:

The ICE Office of Human Capital (OHC) leverages ServiceNow to create and track OHC-related inquires/questions (e.g., retirement and benefits, payroll, human resources (HR) reporting, staffing and classification, employee relations), compile reports, and otherwise manage HR workflows that were previously handled via email. This gives OHC users greater visibility into their HR-related activities and ensures proper reporting and metrics.

ICE users can submit OHC-related inquiries by phone, email, or through the ICE OHC Service Portal available through ICE's intranet site. Users select from a drop-down menu to indicate the request is HR-related. The system delivers the request to specific OHC employees to process based upon the nature of the request.

Relevant SORNs:

- DHS/ALL-004 General Information Technology Access Account Records (GITAARS);[25]
- DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System;[26]
- DHS/ALL-033 Reasonable Accommodations Records System;[27] and
- OPM/GOVT-1 General Personnel Records.[28]

Categories of Information:

The information provided to OHC is only collected to identify and process documents associated with the individual, or to confirm and ensure data accuracy. This includes general work profile information, such as:

- Name;
- Location (i.e., home address, ICE office, temporary duty); and
- Description of the inquiry.

If the user submits an HR-request through the OHC-customized self-service portal, the user's general work information is pre-populated based on his or her PIV card profile. Once

[25] *See* DHS/ALL-004 General Information Technology Access Account Records (GITAARS), 77 FR 70792 (Nov. 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[26] *See* DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System, 74 FR 30301 (June 25, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.
[27] *See* DHS/ALL-033 Reasonable Accommodations Records System, 76 FR 41274 (July 13, 2011), *available at* https://www.dhs.gov/system-records-notices-sorns.
[28] *See* OPM/GOVT-1 General Personnel Records, 80 FR 74815 (Nov. 30, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

submitted, a system-generated ticket with a unique ticket number is created and assigned to the appropriate OHC personnel to handle as appropriate.

Users may also upload any relevant documents to assist with their request into the self-service portal. The information uploaded may contain SPII associated with the user or his or her family member, as appropriate. This may include:

- Name;
- Social Security number (SSN);
- Date of birth (DOB);
- Contact information;
- HR information (e.g., employment-related data, including positions, training, benefits, hiring, background, and performance; financial data, including accounts, salary, transactions, and income tax information);
- Supplemental Security Income (SSI) related to employees, retirees, and their family members;
- Medical data, related to benefits, reasonable accommodations, and law enforcement personnel;
- Drivers' license number;
- Military identification;
- Passport information;
- Birth certificates (employee and family members);
- Marriage and divorce paperwork; and
- Child-support related information.

The information uploaded is viewable by only the user as well as the OHC personnel assigned to process the request. System administrators also have full access to the information collected and further ensure that access to information is restricted based on the user's verified need-to-know.

Appendix C: ICE ERO Title 8 Aliens Nationality Program

Purpose and Use:

The mission of the Office of Enforcement and Removal Operations (ERO) is to identify, arrest, and remove noncitizens who present a danger to national security or are a risk to public safety, as well as those who enter the United States illegally or otherwise undermine the integrity of the nation's immigration laws and our border control efforts. To accomplish its mission, ERO relies on multiple information systems, databases, spreadsheets, and paper-based solutions to navigate within and across phases. Although some ERO information systems interface with partner systems in the Immigration Enterprise, Deportation Officers are routinely forced to re-enter case information over the course of the immigration lifecycle. Redundant data entry introduces process inefficiencies and data quality issues that exacerbate operational and reporting challenges.

ERO uses ServiceNow in the development of the Title 8 Aliens Nationality Program Agile Software Development and Tier III Software Support Services.[29] This includes the deployment of tools to reduce repetitive and manual processes that will enhance decision-making and improve mission effectiveness.

Relevant SORNs:

- DHS/ALL-004 General Information Technology Access Account Records (GITAARS);[30] and
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER).[31]

Title 8 is comprised of multiple programs, each containing a portfolio of projects intended to satisfy operational gaps and modernize business processes. The specific services include:

1. ICE Air Operations – Charter

Using ServiceNow, ICE ERO developed a solution that provides a centralized location to create and track the lifecycle of charter air flights to remove noncitizens in accordance with the Immigration and Nationality Act (INA). This solution includes a portal for ERO field offices to request seats on scheduled flights and ICE Air Operations to manage those requests against available flight plans. The system ingests the following data from the ICE Enforcement Integrated Database (EID)[32] in order to allow the Enforcement Removal Assistant in the ICE Air Operation

[29] 8 U.S.C §§ 1101, 1103, 1104, 1201, 1255, 1305, 1360.
[30] *See* DHS/ALL-004 General Information Technology Access Account Records (GITAARS), 77 FR 70792 (Nov. 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[31] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[32] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and

Center to assign a seat on a deportation flight. Once the seats on the flight have been assigned, a Flight Manifest (Form I-216)[33] will be generated for recordkeeping purposes.

Categories of Information:

- Biographic information including name, aliases, DOB, country of birth (COB), citizenship (nationality), gender;
- Contact information, including phone number, email address, address;
- Health care Information;
- Criminal history Information, including gang affiliation; and
- Other identification information, including Federal Bureau of Investigations (FBI) number, A-number, Federal Tax ID Number (FINS), State ID number, passport number, birth certification number, Military ID/Discharge, Automated Biometric Identification System (IDENT)[34] number, uploaded documents, digital signatures, and photographs.

2. ICE Air Operations – Commercial

Using ServiceNow, the commercial flight request management solution provides ERO with a centralized location to create and track the lifecycle of a commercial air removal. The ICE AirOps – Commercial application ingests the below data from EID. This data is used to request seats on a commercial airline via the government travel reservation system for both the escorting ERO officer and the noncitizen being deported.

Categories of Information:

- Biographic information, including name, aliases, DOB, COB, citizenship, gender;
- Risk Classification Levels;
- Contact information, including phone number, email address, address;
- Criminal history information, including gang affiliation; and
- Other identification information, including FBI number, A-number, FINS; State ID number, passport number, birth certification number, Military ID/Discharge, IDENT

subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[33] Form I-216: Record of Persons and Property Transferred is accessible through ICE ENFORCE only and is a manifest accounting for the transfer or removal of noncitizen detainees in DHS custody. The Form is *available at* https://icegov.sharepoint.com/sites/insight/_layouts/download.aspx?SourceUrl=/sites/insight/forms/Documents/pdf/i216.pdf.

[34] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) DHS/OBIM/PIA-001 (2012), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

number, uploaded documents, digital signatures, and photographs.

3. Leads Management

ICE ERO is responsible for identifying, apprehending, detaining, and removing deportable noncitizens from the United States. Using ServiceNow, the Leads Management application provides a single location for officers to create, manage, and log work for various lead types and populate lead information in Field Operations Worksheets (FOW). The Leads Management application ingests the below data from the ICE Alien Criminal Response Information Management System (ACRIMe)[35] and the Department of Justice (DOJ) National Crime Information Center (NCIC).[36]

Categories of Information:

- Biographic information, including name, aliases, DOB, COB, citizenship gender;
- Contact information, including phone number, email address, address;
- Criminal History Information, including gang affiliation, ICE custody status of information; and
- Other identification information, including naturalization certificate number, protected status, A-number, FBI number, FINS, State ID number, IDENT number, driver's license number, vehicle registration Information, baptismal certificates, marriage licenses, uploaded documents, digital signatures, and photographs.

4. Bed Request Tracker, aka, Detention Request Tool

Using ServiceNow, ERO developed a bed request management solution that provides bed space requestors and coordinators a centralized portal to request beds for a detainee, process bed requests, and provide relevant documentation to accompany the bed assignment. The Bed Request Tracker, also known as the Detention Request Tool application, ingests the below data from EID. This information is used to determine which detention facility the detainee will be placed in.

Categories of Information:

- Biographic information, including name, DOB, COB, country of citizenship, gender;
- Health information, including medical and mental health issues;
- Risk Classification Levels; and

[35] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ALIEN CRIMINAL RESPONSE MANAGEMENT SYSTEM (ACRIME), DHS/ICE/PIA-020 (2010 and subsequent updates) *available at* https://www.dhs.gov/privacy-documents-ice.
[36] *See* U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION NATIONAL CRIMINAL INFORMATION CENTER (NCIC), *available at* https://www.fbi.gov/services/cjis/ncic.

- Other identifying information, including A-number, protected status.[37]

5. Comprehensive Search and Query

Using ServiceNow, ERO developed the Comprehensive Search and Query, which is an informational interface where an ERO officer can perform a federated search across multiple target systems to view a unified criminal and immigration history for a noncitizen. The following data is ingested form EID and passed to the Unified Immigration Portal (UIP)[38] as a timeline service call using the Representation State Transfer (REST) interface.[39] UIP will return to a timeline depicting all case updates and changes for the specific noncitizen and the requested time frame.

Categories of Information:

- Biographic information, including name, DOB, COB, citizenship, gender; and
- Other identifying information, including A-number, FBI number, FINS, naturalization certificate number.

[37] Protected status information is collected to determine if the detainee needs to be placed in a separate cell or area.
[38] UIP is a federated technology platform that permits agencies to efficiently manage their collective data from the first to last encounters in the immigration process and across agency boundaries. For example, UIP utilizes different tools such as a dashboard, timeline, and network information to help ICE prepare for detainee transfers. *See* U.S. DEPARTMENT OF HOMELAND SECURITY U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CBP ENTERPRISE ANALYTICS, DHS/CBP/PIA-063 (2020), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection. Additionally, a UIP-specific PIA is forthcoming.
[39] REST a standard Application Programming Interface (API) approach currently used in most of the ERO applications today.

Appendix D: ICE Huddle/ServiceNow Integration

Purpose and Use:

ICE ERO uses ServiceNow to interact with Huddle using an Application Programing Interface (API)[40] to securely transmit and ingest coronavirus (COVID-19) data and make that data available to ERO employees for tracking and reporting purposes. Huddle is a FedRAMP-approved Software as a Service (SaaS) that provides cloud-based online collaboration and document sharing solutions for users and businesses. OCIO identified Huddle as the best solution to manage and organize the data collected about detainees at high risk of contracting COVID-19 because it provides the ability to securely communicate and transfer the medical information to/from third-party providers and detention facility personnel. When ERO health care personnel (primarily the ICE Health Service Corps (IHSC)) and contracted providers upload the COVID-19 data into the Huddle collaboration platform, ServiceNow retrieves the uploaded documents and extracts the data into a database table viewable by the ERO employees with a need-to-know. The data presented in the ServiceNow database is read-only and may also be exported into Excel spreadsheets for additional data analysis and use.

Relevant SORNs:

- DHS/ALL-004 General Information Technology Access Account Records (GITAARS);[41] and
- DHS/ICE-013 Alien Health Records System.[42]

Categories of Information:

The information collected, generated, or retained on the subject ERO detainees consist of:[43]

- Biographic and biometric information, including name, alias, DOB, age, A-number, gender, subject ID, county of origin, distinguishing characteristics (i.e., scars, marks, tattoos), weight, height, body mass index (BMI), electronic signatures;
- Contact information, including phone number and address;
- Health and medical information, including medical conditions, diagnostic data (tests ordered/test results), symptoms reported, signed refusal forms, signed information consent

[40] An API is a software intermediary that allows two applications to talk to each other.
[41] *See* DHS/ALL-004 General Information Technology Access Account Records (GITAARS), 77 FR 70792 (Nov. 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[42] *See* DHS/ICE-013 Alien Health Records System, 83 FR 12015 (Mar. 19, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[43] Similar types of information may be collected from individuals other than detainees should other program areas (such as ICE Office of Homeland Security and Investigations (HSI)) or other DHS component agencies elect to use Huddle.

forms, treatment records, mental health records, prescription drug records, dental history (including X-rays), correspondence related to medical/dental care, special needs/accommodation information (e.g., requires a cane, wheelchair, special shoes); device identifiers, do not resuscitate (DNR) orders, death certificates; and

- Detention information, including unit, bed assignment, custody status, basis for detention, risk factor, risk description, release status, deportation status, detention location.

The information collected, generated, or retained on health care providers (DHS employees/contractors and external contacted care providers, such as doctors) consists of:

- Name and contact information, including phone number, email address, and work location;
- User information and log-in credentials;
- Area of Responsibility (AOR) information;
- Date/time stamps associated with specific actions using the system; and
- Work schedule and work assignment/tasks.

Appendix E: ICE Arrest Approval and Reporting Tool

Purpose and Use:

On February 18, 2021, the Acting Director of the U.S. Immigration and Customs Enforcement (ICE) issued "Interim Guidance: Civil Immigration Enforcement and Removal Priorities (CIEP)."[44] The interim priorities do not require or prohibit the arrest, detention, or removal of any noncitizen. Rather, ICE officers and agents are expected to exercise their discretion thoughtfully, consistent with ICE's national security, border security, and public safety mission. Enforcement and removal actions not reflected in the specific criteria for each priority may be justified, but they are subject to advance review and will require preapproval from the Field Office Director (FOD) or Special Agent in Charge (SAC). In requesting this preapproval, officers or agents must submit a written justification through their chain of command.

In response to these requirements, ERO/HSI developed an electronic approval ServiceNow platform, the Arrest Approval and Reporting Tool (AART), to aid officers and agents in obtaining approval for actions not reflected in the CIEP to be routed to the FOD/SAC for review. Once the FOD or SAC makes a final decision (i.e., approve or deny the request), the requestor and courtesy recipient (i.e., chain of command) will be notified. Enforcement actions that fall under one of the enumerated priorities will be entered into the AART tool for reporting purposes only.

The FOD/SAC can approve a request by responding to the system notification that is sent to his or her email,[45] or by accessing and approving the request within AART. The FOD/SAC will not be able to change his or her decision after it has been made.[46] If the submission contains incorrect information or has been denied by the FOD/SAC, a new request will need to be created should a user want to resubmit with new or corrected information. By default, AART requestors cannot access the dashboard, but field office management can delegate this access to their staff on a case-by-case basis. Approved requests are printed and enclosed in the subject's A-file.

Relevant SORNs:

- DHS/ALL-004 General Information Technology Access Account Records (GITAARS),[47] which covers how DHS collects information from employees in order to provide authorized individuals with access to DHS information technology resources;

[44] ICE, *Interim Guidance: Civil Immigration Enforcement and Removal Priorities*, 11090.1 (Feb. 18, 2021), *available at* https://www.ice.gov/doclib/news/releases/2021/021821_civil-immigration-enforcement_interim-guidance.pdf.
[45] Within the email notification, the FOD/SAC will click on the "Click here to approve" link at the top of the message. A new email will open, and the approver will need to click "Send" to finish the approval. All contents of the email will be pre-populated for the approver.
[46] There is no "appeal" process. The review and approval process is very robust. The originator can have any number of individuals review and edit the form before it is submitted for approval by FOD/SACs.
[47] DHS/ALL-004 General Information Technology Access Account Records (GITAARS), 77 Fed. Reg. 70792

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records,[48] which describes records maintained relating to the adjudication of benefits, investigation of immigration violations, and enforcement actions in A-Files; and
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[49] which discusses information collected to support the detention and removal of individuals unlawfully entering or present in the United States.

Categories of Information:

The information collected, generated, or retained on subjects include:

- Enforcement action (i.e., arrest, detainer, and removal);
- Enforcement action date and time;
- Planned location (i.e., residence, worksite, traffic stop effectuated by ICE, courthouse, sensitive location,[50] other);[51]
- Immigration enforcement priority (i.e., National Security, Border Security, Public Safety, Field Office Priority);
- Name (first, middle, and last);
- A-Number;
- Enforcement Integrated Database (EID) Subject ID;[52]
- Country of Birth;
- Country of Citizenship;
- Date of Birth (DOB);
- Age - this is automatically calculated based on the DOB entered.
- Immigration history (yes or no);

(Nov. 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[48] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (Sept. 18, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.
[49] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[50] Sensitive location includes, but is not limited to, medical treatment and healthcare facilities, schools, places of worship, religious or civil ceremonies, or a public demonstration
[51] If "Other" is selected, the requester will be prompted to enter a specific location.
[52] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

- Outstanding warrant(s) (yes or no);
- Flight risk (yes or no); and
- Other aggravating or mitigating factors (yes or no).

The information collected, generated, or retained on the requesting officer/agent include:

- Requesting Officer/Agent name - this information is prepopulated from the ICE Active Directory;
- Area of Responsibility (AOR);
- Component (i.e., ERO or HSI); and
- Chain of command name for courtesy notifications.

The tool also includes a free-text field for the requestor to submit a justification for the arrest authorization request.

Privacy Impact Assessment

Privacy Risk: There is a risk that information will be included in the system that is not necessary or relevant to accomplish the system's purpose.

Mitigation: This risk is partially mitigated. ICE users who have access to AART may submit a justification of the arrest authorization request in a free-text field. Currently, there is no disclaimer in AART that informs the requestor to limit the personally identifiable information (PII) entered in the justification to only what is required to obtain the approval. However, ICE Privacy is working with the Office of the Chief Information Officer (OCIO) to add the following disclaimer, "PII should only be entered into this field as required to complete and obtain approval for the request" to remind users about limiting the proliferation of unnecessary PII. Additionally, all ICE personnel complete mandatory ICE privacy and security training, which includes rules of behavior (ROB), appropriate uses of ICE system data, uploading records, disclosure, and dissemination of records before they gain access to ICE systems and applications. Any unnecessary PII that users provide via the tool, is also scrubbed from ServiceNow according to guidance in the ICE Service Desk Standard Operating Procedure (SOP). Should unnecessary PII be included, the ICE Privacy unit will investigate the matter as a potential privacy incident.

Privacy Risk: There is a risk that FODs/SACs will make a determination based on inaccurate information.

Mitigation: This risk is mitigated. Officers and agents submit requests to obtain approval for enforcement actions not reflected in the CIEP via AART. Once a request has been submitted, the FOD/SAC approves the request by responding to the system notification that is sent to his or her email, or by accessing and approving the request within AART. The FOD/SAC will not be

able to change his or her decision after it has been made. If the submission contains incorrect information or has been denied by the FOD/SAC, a new request will need to be created should a user want to resubmit with new or corrected information. The approval process is very robust and the requestor can add authorized individuals within their AOR chain of command, with a valid-need-to-know, to review and confirm the accuracy of the information before it is submitted for approval.

Appendix F: ERO Field Office Appointment Scheduler (FOAS)

Purpose and Use:

U.S. Customs and Border Protection (CBP) officers and agents may release individuals and family units (FAMU) apprehended at the border into the interior of the United States via Prosecutorial Discretion (PD).[53] Due to the increase in the number of migrants, CBP releases these noncitizens from its custody via an exercise of PD without the issuance of charging documents, such as a Notice to Appear (NTA).[54] CBP leverages the U.S. Immigration and Customs Enforcement (ICE) Field Office Appointment Scheduler (FOAS), which is an appointment scheduling and management tool developed by ICE to facilitate the scheduling of noncitizen individuals and FAMU. FOAS is built on the ICE ServiceNow platform and provides a streamlined way for noncitizens to schedule appointments at a local ICE Enforcement and Removal Operations (ERO) office without needing to call or appear in person to create the appointment. Additionally, the capability reduces the risk of large numbers of noncitizens showing up at ERO field offices without advanced notification, resulting in ERO's inability to process the cases efficiently. This ServiceNow tool has two components: 1) an internal application that is available to ERO and CBP personnel only, and 2) an external public-facing website that is accessed by the general public to schedule appointments.[55]

When CBP releases a noncitizen at the border, CBP issues Form I-385, Alien Booking Record,[56] with instructions for the noncitizen to report to a local ERO office for continued processing. Using the public-facing FOAS website, noncitizens may search for and select a local ERO field office to view available appointment days and times (as defined by the Appointment Manager) on which they will report to the selected office.[57] In order to make an appointment, the noncitizen (or a CBP agent/officer acting on the noncitizen's behalf) must enter their name, country of birth, and the subject identification (ID) number from the Form I-385 into the FOAS ServiceNow tool. The information entered will enable the local ERO officer receiving the appointment request to validate the identity of the noncitizen and match the individual with their associated information in the ICE Enforcement Integrated Database (EID), Enforce Alien Removal Module (EARM)[58] prior to the visit. The information in EARM will also provide the ERO officer

[53] Prosecutorial Discretion (PD) is the longstanding authority of an agency charged with enforcing the law to decide where to focus its resources and whether or how to enforce, or not to enforce, the law against an individual.
[54] The NTA lists the charges that DHS is bringing against the respondent, specifying the removability grounds and factual allegations to establish removability.
[55] The external URL which the public will use to schedule appointments is https://checkin.ice.gov.
[56] Form I-385 is not publicly available. It is issued to the noncitizen by CBP at the time of release. An example form is displayed at https://checkin.ice.gov.
[57] The FOAS Appointment Manager will allow each ERO Area of Responsibility (AOR) to pre-select available timeslots for appointments.
[58] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent

with information about the individual's family unit members who may also be part of the field office visit.

Once all required information has been entered, reviewed for accuracy, and submitted, the noncitizen will receive a confirmation number, along with appointment details. Noncitizens will have the option to receive an email, a text, or to print the confirmation details for future reference. Individuals have the option of providing their email address and/or telephone number for Short Messaging Service (SMS) text messages (contact information) for appointment reminders, as well. FOAS will store the noncitizen's name, country of birth and subject ID number. It will also store the optional contact information (i.e., email address and telephone number), if provided, for the purpose of sending appointment confirmation and/or reminders in advance of scheduled appointments. The contact information will not be used for any other purpose at this time. All other information (i.e., name, subject ID, and country of birth) will remain in EID.

Relevant SORNs:

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER)**,**[59] which discusses information collected and maintained by EID to support the detention and removal of individuals unlawfully entering or present in the United States.

Categories of Information:

The information collected from the noncitizen that is required to schedule the appointment includes:

- Name;
- Subject ID number; and
- Country of birth.

If the noncitizen wants an appointment confirmation and/or reminder, they will need to provide their contact information (i.e., email and telephone number). Information about FAMU members is pulled from, but remains in, EID. This is also limited to the family unit members' name, subject ID, and country of birth (as required fields).

CBP and ERO personnel access the internal FOAS platform using Single Sign-On (SSO), via the ICE ServiceNow SSO feature, which maps the user's identity information in the Active Directory.

updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[59] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

Appendix G: ERO Contact Center of Operations (ECCO) Custody Assistance and Inquiry Resolution System (CAIRS)

Purpose and Use:

The ERO Custody Programs Division (CPD) operates the ECCO in an effort to resolve community-identified problems or concerns with ICE immigration and detention policies and operations. The majority of calls to the ECCO come from members of the public attempting to locate someone they believe is in ICE custody. Calls from detainees typically concern immigration case information inquiries, medical or mental health complaints, and/or parental or family-separation issues. ECCO operators are responsible for answering inquiries and coordinating any necessary follow-up with CPD's liaisons in ERO field offices and ICE program offices.

CPD uses the ServiceNow-based CAIRS to manage information received during an ECCO call. ECCO operators enter information received during the inquiry into forms built within CAIRS. After a supervisor reviews the information, operators generate emails within the system that are sent to the appropriate ERO field or other ICE office for real-time, priority-based actions. Once the receiving office reviews and resolves the CAIRS referral, the designated CPD liaison enters the referral disposition and closes the entry in CAIRS.

CAIRS also provides a robust archival process, enabling ECCO operators to search for archived entries and review historical notes related to previous inquiries associated with a particular A-Number or a CAIRS-generated tracking number.

System Access:

The system administrator grants CAIRS access to ECCO operators, CPD leadership, and CPD liaisons in ERO field offices and select ICE program offices.

Individuals Impacted:

ECCO operators collect information directly from the individuals that are submitting inquiries. They may enter additional information about a specific individual who has been arrested, encountered, or detained by ICE or held in ICE custody pending removal or in removal proceedings under the INA from ICE's ENFORCE Alien Removal Module (EARM).[60]

Categories of Information:

Information from individuals calling ECCO with inquiries; subjects of inquiries, including individuals arrested, encountered, or detained by ICE or held in ICE custody pending removal or in removal proceedings under the Immigration and Nationality Act (INA).

[60] There is a prerecorded message that the caller hears explaining that they do not have to provide additional information, only information necessary to provide assistance.

CAIRS will automatically assign all incoming calls a unique tracking number consisting of the date and a running call-count number. In addition, CAIRS has data fields to gather information on:

- The category of the caller (e.g., detainee, attorney of detainee, family member of detainee, advocate, member of the general public), identifying information (full name, organization name (if any), and contact information, including 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 applicable);
    - Address;
    - Email address;
    - Phone number;
    - The facility location if the person is in detention facility; and
    - The nature and description of the inquiry (e.g., general outreach inquiry, detention concern, enforcement issue, facilitation of return, national policy concern).

Relevant SORN:

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records,[61] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens; and
- DHS/ALL-016 Department of Homeland Security Correspondence Records,[62] which covers correspondence records submitted by the general public, DHS personnel, and others.

[61] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[62] *See* DHS/ALL-016 DHS/ALL-016 Correspondence Records, 83 FR 48645, (September 26, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

The SORNs list the authorities for maintenance of these records.

Privacy Impact Assessment

Privacy Risk: There is a risk that information included in the system will be inaccurate because the ECCO operators entered the wrong information, or because the information provided by the third-party callers is inaccurate.

Mitigation: This risk is mitigated. The ECCO analysts enter the information received directly into the CAIRS ServiceNow tool. Supervisory review helps ensure that the information the ECCO analysts enter into CAIRS is accurate, and that the users are using the information for its intended purposes.

Records Retention Period:

Records created within CAIRS are retained for seven years under National Archives and Records Administration (NARA) schedule DAA-0567-2015-0013-0007.

Appendix H: Segregation Review Management System (SRMS)

Purpose and Use:

ERO uses 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, often into a separate, individual unit. Administrative segregation is a non-punitive form of separation from the general population and is authorized only as necessary to ensure the safety of the detainee, facility staff, and other detainees; the protection of property; or the security or good order of the facility. Disciplinary segregation is authorized only pursuant to the order of a facility disciplinary panel following a hearing in which the panel determines the detainee committed serious misconduct in violation of a facility rule.

ERO field office personnel enter information pertaining to a detainee's segregation case directly into the ServiceNow-based SRMS. The appropriate ERO field office updates the case to reflect changes in the segregation status, including removal from segregation. Within SRMS, ERO personnel 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 a detainee's segregation status.

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:

Only users granted access are authorized to view SRMS information. These users are: ERO field office leadership and their staff assigned to segregation management; the Segregation Review Coordinator and administrative support staff; SMEs 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 immediate access only to information about the cases relevant to the particular user.

Individuals Impacted:

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

Categories of Information:

SRMS receives information from ERO detention facility staff and from ICE's ENFORCE Alien Removal Module (EARM).[63] SRMS information includes case notes from field office personnel or medical personnel (ICE Health Service Corps staff).

[63] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

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 proficiency; and
  - Detention facility housed in at the time.
- Information relevant to the segregation decision, including:
  - Type of segregation (i.e., administrative or disciplinary);
  - Reasons for the placement in segregation (e.g., conduct/behavior, heightened concern for a detainee's risk of victimization, other special vulnerabilities);
  - Existing medical and mental health conditions;
  - Criminal history;
  - Disciplinary history; and
  - Immigration history.
- Information pertaining to ICE oversight and review of individual segregation cases, including:
  - Dates of initial segregation and transfer 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).

Relevant SORN:

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records,[64] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the

[64] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens.

The SORN lists the authorities for maintenance of the records.

Privacy Impact Assessment

Privacy Risk: There is a risk that users will make use of the information in the program for purposes that are not described in this PIA or in the relevant SORN or use the information in a manner that is not one of the user's relevant authorities or responsibilities.

Mitigation: This privacy risk is mitigated. The ERO Custody Programs Division (CPD) programs incorporate user roles and access, which limit user capabilities so that only those with a need-to-know can access the program information. Data maintained in the programs are displayed in user-specific views where the user only has access to the case information that is relevant to his/her responsibilities. Users undergo mandatory privacy and security training that stress the importance of authorized use of personal information in government programs and systems. Anyone who is found to have used the system in an unauthorized manner can be disciplined in accordance with ICE policy and/or federal law.

Records Retention Period:

Segregation reports are maintained in accordance with National Archives and Records Administration (NARA) approved schedule DAA-0567-2015-0013-0008. Records are retained for seven years after the end of the fiscal year in which a detainee is transferred from segregation.

Appendix I: Sexual Abuse and Assault Prevention and Intervention Case Management System (SAAPICM)

Purpose and Use:

SAAPICM is used to track the lifecycle of sexual abuse and assault allegations occurring in ICE detention facilities (i.e., in hold rooms or in any custodial location). The SAAPICM system promotes compliance with Sexual Abuse and Assault Prevention and Intervention (SAAPI), an ICE policy that establishes the responsibilities of ICE detention facility staff and other ICE personnel with respect to prevention, response, intervention, reporting, investigation, and tracking of incidents of sexual abuse or assault. The directive also contains reporting requirements.

The system is used to input data about incidents and provide transparency to users about an allegation's status. SAAPICM facilitates oversight by ERO Custody Programs which has primary responsibility under this policy for incident review and reporting. The system also allows users to track a particular incident and ensure that ICE policy requirements are being met. The data in the system is used for collecting sexual abuse and assault allegation metrics and reporting aggregate sexual abuse and assault allegations.[65]

System Access:

Access to SAAPICM is based on roles that ICE personnel have in the submission and oversight process. Site access is granted to those designated as Prevention of Sexual Assault Coordinators (PSAC) at the ERO field offices and ICE Headquarters levels. The Office of Professional Responsibility (OPR) and ERO Custody Programs grant access to the lead PSACs. Data maintained on the site is displayed in user-specific views; the user has access only to the case information relevant to the user's responsibilities.

Individuals Impacted:

Individuals who are the subjects (i.e., alleged victims, perpetrators, or witnesses) of sexual abuse and assault allegations, including individuals whom ICE arrested, encountered, or detained or held in custody pending removal or removal proceedings under the Immigration and Nationality Act (INA).

Categories of Information:

SAAPICM collects information directly from the individuals submitting the allegations

[65] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), and U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE SIGNIFICANT EVENT NOTIFICATION SYSTEM, DHS/ICE/PIA-023, *available at* https://www.dhs.gov/privacy-documents-ice.

and from witnesses to sexual abuse and assault incidents. Case notes from field personnel may also be included in the system. Field personnel are interviewed if they are witnesses to sexual abuse and assault incidents.

The SAAPICM ServiceNow site will automatically assign a unique case reference number for all sexual abuse and assault allegation cases submitted by field offices. In addition, information collected and stored within SAAPICM includes:

- Identifying information pertaining to the alleged victim and perpetrator, including:
    - Full name;
    - A-Number;
    - Country of birth;
    - Date of birth;
    - Gender;
    - Self-identification as lesbian, gay, bisexual, transgender, and intersex (LGBTI) or nonconforming;
    - Any pertinent disabilities; and
    - Primary language spoken.
- Information relevant to the allegations, including:
    - Reporting timeline and investigative findings, including description of the alleged incident;
    - Responsible investigating party (e.g., DHS Office of the Inspector General (OIG), ICE Office of Professional Responsibility (OPR), ERO Administrative Inquiry Unit);
    - Sanctions or punishment enforced on the alleged assailant (e.g., segregation, transfer to a different facility, loss of privileges);
    - Incident details (location, date, and time); and
    - Witness biographical information, including full name and person type (e.g., ICE employee, contractor, volunteer).

Relevant SORN:

- DHS/ICE-009 External Investigations,[66] which covers (1) documenting external audits,

[66] *See* DHS/ICE-009 External Investigations, 85 FR 74362 (Nov 20, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

inquiries, and investigations performed by ICE pertaining to suspected violations of laws regulating the movement of people and goods into and out of the United States in addition to other violations of other laws within ICE's jurisdiction; (2) To facilitate communication between ICE and foreign and domestic law enforcement agencies for the purpose of enforcement and administration of laws, including immigration and customs laws; (3) To provide appropriate notification to victims in accordance with federal victim protection laws; (4) To support inquiries and investigations performed to enforce the administrative provisions of the INA; and (5) To identify potential criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety; and

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[67] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens.

The SORNs list the authorities for maintenance of these records.

Privacy Impact Assessment

Privacy Risk: There is a risk that information included in the system will be inaccurate because the ICE personnel entered the wrong information, or because the information provided by the third-party callers to ICE is inaccurate.

Mitigation: This risk is mitigated. Administrators employ access controls to make sure that only authorized users can access the data maintained in the ERO Custody Programs Division (CPD). Additionally, users only have access to the information necessary for their positions, based on the user's job responsibilities. The system administrators implement this role-based access. Individuals who no longer require access have their user access to the programs terminated. Supervisory review helps ensure that the information the assigned personnel entered into the program is accurate, and that the users are using the information for its intended purposes. If a supervisor or administrator notices that an individual has used the program in violation of ICE or CPD policy, the user will be disciplined accordingly.

Prior to using the system, all users must review the program's or system's Standard Operating Procedures (SOP) to understand how it operates and to ensure that they are handling PII appropriately. The SOPs provide significant detail on the proper collection, use, maintenance, and

[67] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

disposal of PII. All users take annual privacy, security, and information assurance awareness training before the administrator grants access. These trainings ensure that users understand the proper handling of PII, as well as relevant security processes and procedures. Users also must complete system-specific training to certify that they know how the system in which the program resides and operates and that they can properly handle information contained within the programs.

Records Retention Period:

Sexual abuse and assault records are maintained in accordance with National Archives and Records Administration (NARA)-approved schedule DAA-0567-2015-0013-0001. Records are retained for 25 years after case closure.

Appendix J: ERO Non-Telephonic Reporting (ENTR) Non-Telephonic Inquiry System (NTIS)

Purpose and Use:

The ENTR team in the ERO Custody Programs Division's (CPD) Custody Reporting & Strategy Unit operates the NTIS, a Microsoft Access database that tracks inquiries, referrals, communications, and leads from the following sources:

- DHS Office of the Inspector General (OIG)/Joint Intake Center (JIC) inquiries;
- ERO.INFO e-mail inbox inquiries; ICE.GOV web form entries;
- ERO Contact Center of Operations (ECCO) submission (ECCO.LEADS); and
- Reasonable Accommodations (RA) Active Cases.
    - ENTR analysts use NTIS to manage, enter, and track the content of inquiries from the above mailboxes, which are routed to CPD from the following:
- The general public;
- ICE detainees;
- DHS Office of Inspector General (OIG); and
- U.S. Customs and Border Protection (CBP) Joint Integrity Case Management System (JICMS) repository.[68]

DHS OIG/JIC inquiries: The ERO JIC mailbox receives complaints from the OIG Hotline, Office of Civil Rights and Civil Liberties (CRCL), and the JIC. The messages typically include a PDF attachment from DHS OIG documenting what the call center received (fax, email, a scanned letter, or a web entry to OIG or JICMS). The ENTR team reviews and logs the communication for status tracking in NTIS, and forwards actionable cases to the subject matter experts at ERO Field Offices or ICE headquarters.

ERO.INFO e-mail inbox inquiries: The ENTR team reviews, tracks, and responds to requesters' inquiries that are emailed directly to the ERO.INFO public mailbox or submitted using a fillable web form on ICE.gov, which then generates an email that is sent to ERO.INFO@ice.dhs.gov.

ICE.GOV web form entries: These requests come from the online ERO Contact Form located at https://www.ice.gov/webform/ero-contact-form and reach the ENTR team through the

[68] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE JOINT INTEGRITY CASE MANAGEMENT SYSTEM (JICMS), DHS/CBP/PIA-044 (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

ERO.INFO mailbox. The ENTR team processes these in the same manner as other requests from the ERO.INFO mailbox.

ECCO.LEADS submissions: The ECCO responds to a variety of internal and external communications from detainees, family members, attorneys, and stakeholders. ECCO.LEADS is a dedicated mailbox that receives emails containing law enforcement leads from the public and local law enforcement. ENTR analysts review, document and track the emails received via ECCO.LEADS in NTIS and send the leads to the ERO Field Offices for action.

Reasonable Accommodations (RA) Active Cases: ICE tracks requests and provision of reasonable accommodations for detainees with certain disabilities per ICE Directive 11071.1, in compliance with section 504 of the Rehabilitation Act (RA) of 1973. Detainees, ERO Field Offices, or external parties (such as attorneys, family members, members of the community, or non-governmental organizations) may initiate RA inquiries. The mailbox itself also includes communications related to an RA inquiry within CPD. Detainees or their representatives initiate most inquiries, which typically concern case information, medical or mental health issues, facility questions, or concerns related to parental issues or family separations. ENTR analysts may also re-direct inquiries, communications, leads and/or concerns from the RA mailbox to the ERO field offices and ICE program offices.

System Access:

NTIS data

Users require CPD leadership approval to access the folder where the NTIS database is stored, and the user's Personal Identity Verification (PIV) card encodes folder access. NTIS is a stand-alone tracking system and does not connect to or share data with any other system. Access to the NTIS database is limited to the ENTR analysts, CPD subject matter experts (SMEs) and CPD leadership with responsibility over the program. CPD supervisors manage access to CPD mailboxes. Individual users must have permission to be included in the designated mailbox distribution list.

ERO JIC mailbox

Individuals with access to the JICMS Information in the ERO JIC mailbox can retrieve information by using their PIV card. The individuals then access the cases assigned to them. The ICE Office of Professional Responsibility (OPR) grants JICMS access following approval of a formal request.

ERO.Info mailbox

Access to the ERO.Info mailbox is provided to CPD Leadership and ENTR contractor analysts who require access to NTIS to perform their duties. Access requires submission of an IT Help Desk ticket with final approval from CPD Leadership.

ECCO.LEADS mailbox

As in the ERO.Info mailbox, CPD Leadership and ENTR contractor analysts have access to the ECCO.LEADS mailbox to perform their duties. Access requires submission of an IT Help Desk ticket with CPD Leadership granting final approval.

Reasonable Accommodations mailbox

Access to the Reasonable Accommodations mailbox is provided to CPD Leadership, the ERO Disability Access Coordinator (EDAC), the back-up EDAC and contractor staff who require access to perform their duties supporting the RA portfolio. Access to this mailbox requires submission of an IT Help Desk ticket with CPD Leadership granting final approval.

Individuals Impacted:

Individuals who submit inquiries (e.g., detainee, attorney of detainee, family member of detainee, advocate, any member of the general public who submitted an inquiry, ICE contractors and employees) to ENTR; individuals who are the subjects of inquiries, including individuals whom ICE arrested, encountered, detained or held in ICE custody pending removal or removal proceedings under the Immigration and Nationality Act (INA).

Categories of Information:

Analysts enter data from ICE ENFORCE Alien Removal Module (EARM),[69] and data collected by an ERO Detention & Deportation Officer (DDO) for case documentation, and information that individuals submitted in inquiries through the ENTR mailboxes in the original message.

ENTR analysts assigns a unique tracking number to all incoming inquiries. In addition, NTIS has data fields to gather the following information:

From ERO.JIC:

- Biographical information of the reporting party, including A-number (if a detainee);
- Biographical information of the subject detainee, including A-number;
- Name and category of the non-detainee inquirer or reporting party
    - Contractor;
    - Family member;
    - Government staff;

[69] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

  - Attorney;
  - Self;
  - Volunteer;
  - Other.
- Facility in which the reported event occurred; and
- Text documenting the statement received or sent.

From ERO.INFO:

- The email subject line (may include A-Number);
- Category of the inquiry (drop-down menu):
  - Detainee Locator;
  - Facilitation of Return Request;
  - Field Office Inquires; and
  - General Questions.
- Historical ERO.INFO records;
- Requester's and subject's biographical information, including A-number.

From ECCO.LEADS:

- Source Tracking Number;
- Requester's biographical information, including A-number, (if a detainee);
- Subject's biographical and identifying information, including:
  - A-Number;
  - ENFORCE Subject ID;
  - Fingerprint Identification Number (FIN);
  - Federal Bureau of Investigation (FBI) Number;
  - Social Security number (SSN);
  - Country of birth;
  - Country of citizenship;
  - LEADS subject's street address;

- Phone number;
- Driver's License number; and
- Photograph (if supplied).

From RA:

- Biographical information, including A-Number; and
- Detention facility.

Relevant SORN:

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[70] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens; and
- DHS/ALL-016 Department of Homeland Security Correspondence Records,[71] which covers correspondence records submitted by the general public, DHS personnel, and others.

The SORNs list the authorities for maintenance of the records.

Privacy Impact Assessment

Privacy Risk: There is a risk that information included in the system will be inaccurate because the detainee, a third-party inquirer, or another program office provided inaccurate information to the ENTR analysts.

Mitigation: This risk is mitigated. The ENTR analysts use NTIS to manage, enter, and track the content of inquiries from various mailboxes, which are routed to CPD. Most of the inquiries concern detainees or their families and representatives providing information directly to ICE about detention-related issues.

Records Retention Period:

The records are retained for seven years under National Archives and Records Administration (NARA) schedule DAA-0567-2015-0013-0007.

[70] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[71] *See* DHS/ALL-016 DHS/ALL-016 Correspondence Records, 83 FR 48645, (September 26, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

APPENDIX K: Disabilities Case Tracker

Purpose and Use:

The Disabilities Case Tracker (the "Tracker"), which the Reasonable Accommodations (RA) team manages, tracks, and maintains the names of detainees with mobility and/or cognitive disabilities or impairments at all ICE detention facilities, including the type of condition and the detainees' age category. It also monitors the facilities' compliance with DHS/ICE policies and directives and keeps a record of the Disability Accommodation Notifications (DAN) that the Field Offices send to ICE Headquarters.

The tracker manages the availability of resources that facilities may use to help ensure that all detainees have equal access to detention programs, services, and activities while in ICE custody (e.g., outdoor recreation, indoor recreation, religious services, law library access). The tracker also helps the team monitor the facilities' compliance with applicable detention standards and policies. The Supporting Disability Access Coordinator (SDAC) for each Field Office sends the ERO Disability Access Coordinator at ICE Headquarters a DAN via the ERO Reasonable Accommodations (ERO.RA) inbox, which is the team's email inbox at ICE Headquarters. The Disabilities Case Tracker tracks the DANs that the team receives from all the Field Offices.

System Access:

The dashboard and the information that the tracker collects are stored on the ICE ERO CPD shared drive, which requires CPD leadership approval to access the folder in which the database is stored.

Individuals Impacted:

Detainees with a reported or observed disability or impairment (e.g., detainee is using a wheelchair or has a prosthesis).

Categories of Information:

ICE personnel enter their observation that a detainee has a disability or an impairment if the detainee informs ICE personnel that he or she has a disability or an impairment. Information is also collected when ICE personnel submit a DAN via ERO.RA, which is the team's email inbox at ICE Headquarters.

The names of detainees with mobility and/or cognitive disabilities or impairments at all ICE detention facilities, including:

- Name;
- A-Number;
- Date of birth;

- Type of condition, and the detainees' age category;
- Area of Responsibility (AOR) and facility;
- Nature of disability;
- Accommodations requested/provided;
- Facility Accommodation Plan; and
- If an accommodation is denied, what was requested, and why was it denied.

Relevant SORN:

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[72] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens.

The SORN lists the authorities for maintenance of the records.

Privacy Impact Assessment

Privacy Risk: There is a risk that information included in the system will be inaccurate.

Mitigation: This risk is mitigated. The Reasonable Accommodations (RA) team enters information on detainees based on the detainees' self-reported or ICE personnel's observed mobility and/or cognitive disabilities or impairments of the detainees.

Records Retention Period:

These records are unscheduled and must be treated as permanent until the National Archives and Records Administration (NARA) establishes a schedule.

[72] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

Appendix L: Lesbian, gay, bisexual, transgender, and intersex (LGBTI) ERO Contact Center of Operations (ECCO)/Joint Intake Center (JIC) Status Tracker

Purpose and Use:

The LGBTI ECCO/JIC Status Tracker records complaints or inquiries from or about LGBTI detainees, which ICE receives through the ECCO or JIC and are relayed to the LGBTI Detainee Care team. The tracker additionally records CPD outreach to the field and case resolutions or transfers of detainees to other ERO Custody Management program areas. This tracker enables the team to improve response time to address the inquiries and concerns of or about the LGBTI detainees and allows CPD to comply with ERO Memorandum - Further Guidance Regarding the Care of Transgender Detainees ("Transgender Care Memorandum"), which complements existing ICE detention standards and policy.

System Access:

Access is limited to CPD federal employees and contractors who have a need to know.

Individuals Impacted:

The identified LGBTI detainee, or, in some cases, the lawyer(s) of detainees who have a current form G-28 on file.

Categories of Information:

The LGBTI detainee, attorney, or family member; the ICE employee informed of the status.

Intake information

- The ECCO number; and
- The JIC case tracking number.

Information about the detainee

- The subject detainee's biographical information:
- Full name;
- A-Number; and
- Location of the detention facility.

Nature of the inquiry

- The nature and description of the inquiry, for example:

- The caller's specific concern (such as a detention or enforcement issue or a general concern);
- Request for information;
- Information relating to the detainee's sexual orientation or gender identity; and
- Details relevant to the Sexual Abuse and Assault Prevention and Intervention (SAAPI) allegation.

Special protected class (SPC) information

- Whether the individual's information is protected by 8 U.S.C. § 1367 (Violence Against Women Act – VAWA, T visa, or U visa);
- Supplemental information from other ICE sources;
- Information and notes about the detainee located in the ENFORCE Alien Removal Module (EARM) or provided by the ICE Office of Partnership and Engagement (OPE);
- The detainee's A-Number;
- The name of the individual making the complaint or inquiry (i.e., the detainee, the detainee's representative, or a third party);
- The date of the inquiry/complaint;
- Details of the inquiry/complaint; and
- Any past communication with or about the detainee to determine if the detainee or the detainee's family member or legal representative had previously contacted ICE on the detainee's behalf.

ECCO Call Analyst's recommendation and follow-up

- The ERO Field Office's response and action; and
- Case resolution.

ICE/ERO personnel information

- The ERO Headquarters point of contact (POC) handling the case;
- The ERO Field Office POC;
- Names of personnel; and
- Area of Responsibility (AOR) or assigned field office(s).

Recommended SORN:

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[73] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens.

The SORN lists the authorities for maintenance of the records.

Privacy Impact Assessment

Privacy Risk: There is a risk that information included in the system will be inaccurate because the detainee, a third-party inquirer, or another program office provided inaccurate information to ICE personnel.

Mitigation: This risk is mitigated. Information is provided directly to ICE from the detainees or their families and representatives. ERO's national LGBTI coordinator generally looks through the cases and reaches out to the ERO Field Office to confirm any information that may be inaccurate. For example, the coordinator will reach out to the Field Office if a detainee is marked as transgender but there are no notes in the EARM/encounter to back that assertion up. The coordinator will also reach out to the Field Office to interview the noncitizen if a third party (e.g., attorney) claims the detainee is transgender.

Records Retention Period:

These records are unscheduled and must be treated as permanent until the National Archives and Records Administration (NARA) establishes a schedule.

[73] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

Appendix M: Parental Interests Portfolio Data Tracker

Purpose and Use:

The Parental Interests Portfolio Data Tracker is used as a case management tool to track and maintain select information on detained parents/legal guardians, children and other family members who are involved in parental interest-related case inquiries, which CPD receives through the ERO Contact Center of Operations (ECCO) hotline, the Parental.Interests@ice.dhs.gov mailbox, or direct communication with a team member. The tracker documents the volume of inquiries, length of time to resolve a request, and the types of parental/familial interest inquiries that the team handles.

The Parental Interests Team ("PI Team") primarily checks DHS systems, but they may also check other government systems, such as court systems in local jurisdictions, for any notes/records on possible domestic conflicts (e.g., evidence of U or T Visa, informal records) before releasing any information in response to an inquiry. The PI Team records the requests on the tracker, which assists the PI Team in the management of cases to support timely resolution and reporting functions. Reports reflecting the types of information, such as those listed below, are manually produced for leadership on a weekly basis:

- Requests seeking the location of, and/or communication between, a detained parent/guardian and the detainee's child in the custody of the U.S. Department of Health and Human Services (HHS), Office of Refugee Resettlement (ORR), or in other immigration-related custody;
- Requests seeking the location of, and/or communication between, the subject detainee and related individuals (e.g., minor or adult children, siblings, spouses, grandparents), whether or not these individuals are in immigration-related custody;
- Requests for release, transfer, or removal (e.g., a detainee requests to be released from ICE detention to care for family in the U.S.;
- Requests to be transferred to an ICE facility that is closer to family members;
- Requests to be removed to his or her home country;
- Requests for reunification prior to removal (e.g., a detainee requests to be reunified or to be repatriated together with a minor or adult child or with other related individuals in immigration custody such as a spouse or parent);
- Requests for alternative care arrangements (e.g., a detainee requests an alternative caregiver because his/her child(ren) or other family member is perceived to be a danger, or the current caregiver is claimed to be financially unsuitable);

- Requests regarding or resulting in state/child welfare involvement (e.g., the detainee parent/guardian has a chemical dependency issue, or the detainee has custody or guardianship claims);
- Requests involving a detainee who has a child in state Child Protective Services (CPS) custody or has child support issues; and
- Requests for service of process of legal documents and/or for information about court appearances, visitations, compliance with state court proceedings, interviews with state child welfare personnel.

Reports reflecting the above types of information are manually produced for leadership on a weekly basis.

System Access:

The tracker is stored in a folder within the ICE ERO CPD shared drive, which requires IT approval for access. The tracker itself requires permissions to open, view and edit the stored contents. A designated user with administrative rights is granted permission to access the database, and a user cannot open the database without the proper permissions. Currently, the tracker is operated by the PI Team lead and CPD policy/data analysts. The PI Team manually enters and manages the data that is stored in the tracker. The tracker is a stand-alone system with no links to other ICE/DHS systems.

Individuals Impacted:

Detained parents/legal guardians; the detainee's minor or adult children and related family members (e.g., siblings, grandparents); detainees' representatives with a Form G-28 (Notice of Entry of Appearance as Attorney or Accredited Representative) on file.

Categories of Information:

The source of the information collected will come primarily from detainees, family members, detainees' representatives with a Form G-28 (Notice of Entry of Appearance as Attorney or Accredited Representative). ICE also enters information found on other DHS systems or in public records, such as court documents.

The database is a case management system that collects and maintains the following specific data:

Information on the detainee

- Personal Information
    - Name;
    - A-Number;

  - Date of birth; and
  - Country of birth/citizenship.
- Apprehension and detention location and details
  - Apprehension at border? Yes/No; and
  - Apprehension in the interior? Yes/No
- Detention facility name and location;
- U.S. Marshals Service (USMS) custody (Yes/No).

Familial relationships

- Identification of familial relationships of detainee to other detained individuals (e.g., spouses, siblings, grandparents);
- Identification of detainee's minor or adult child(ren), whether or not in immigration-related custody (e.g., in Office of Refugee Resettlement (ORR) or ICE facility).
- Detainee's minor or adult child(ren); and
- Personal information, including:
  - Name;
  - A-Number;
  - Date of birth;
  - Country of birth/citizenship;
  - Is the child a U.S. Citizen (USC)/Legal Permanent Resident (LPR)? (Y/N); and
  - Address or location of child, if living in the U.S.
- Apprehension location of child (border or interior);
- Detention facility name (if in ORR or in ICE custody);
- Separation details
  - Where did separation occur (border or interior)?; and
  - When did it occur?;

Welfare proceedings involving detainee's minor child(ren)

- State/child welfare proceedings Yes/No; and
- Jurisdiction(s) involved.

Case administration/management information

- Date the PI Team received the case;
- Inquiry source (e.g., subject detainee, other parent, other family member, guardian, friend, internal ICE stakeholder; non-ICE stakeholder);
- Method of inquiry (e.g., calls to ECCO hotline, the Parental.Interests@ice.dhs.gov mailbox or direct contact to a PI team member);
- The case issue type(s). For example:
    - Detained parent seeking location/communication with a child;
    - Location/communication involving a detained non-parent family member;
    - Persons seeking location/communication with a detained parent;
    - Care arrangements;
    - Request release/transfer;
    - Reunification prior to removal;
    - State child welfare involvement; and
    - Other (e.g., inquiries/complaints that are out of the scope of the parental interest portfolio¸ and deferred to another office, such as alleged kidnapping or legal access rather than Parental Interest).

Status of a case (open/closed);

- The date the case closed (if applicable); and
- The PI team member assigned to the case, contact information, and user rights.

Relevant SORN:

- DHS/ICE-009 External Investigations,[74] which covers (1) documenting external audits, inquiries, and investigations performed by ICE pertaining to suspected violations of laws regulating the movement of people and goods into and out of the United States in addition to other violations of other laws within ICE's jurisdiction; (2) To facilitate communication between ICE and foreign and domestic law enforcement agencies for the purpose of enforcement and administration of laws, including immigration and customs laws; (3) To provide appropriate notification to victims in accordance with federal victim protection laws; (4) To support inquiries and investigations performed to enforce the administrative

[74] *See* DHS/ICE-009 External Investigations, 85 FR 74362 (Nov 20, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

provisions of the INA; and (5) To identify potential criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety; and

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[75] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens.

The SORN lists the authorities for maintenance of these records.

Privacy Impact Assessment

Privacy Risk: There is a risk that information included in the system will be inaccurate.

Mitigation: This risk is mitigated. Information will be collected primarily from detainees, family members, and detainees' representatives with a Form G-28 (Notice of Entry of Appearance as Attorney or Accredited Representative). Although these individuals are ultimately responsible for the accuracy of the information provided, the PI Team reviews the information collected and checks DHS data systems, other government systems (e.g., court systems in local jurisdictions), and public records to verify and supplement information in the PI data tracker.

Records Retention Period:

These records are unscheduled and must be treated as permanent until the National Archives and Records Administration (NARA) establishes a schedule.

[75] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

APPENDIX N: Krome Behavioral Health Unit (KBHU) Mental Health Data Tracker

Purpose and Use:

The KBHU Mental Health Data Tracker, a Microsoft Access database, tracks and maintains program records of male detainees over 18 of age who are receiving care at the KBHU. The housing unit provides subacute patient care using a Modified Therapeutic Community (MTC) model for detainees who exhibit debilitating symptoms of psychological distress/disorders that may interfere with their ability to actively participate in immigration proceedings. ICE Health Service Corps (IHSC) and the ERO field office at the Krome Service Processing Center (SPC), in Miami, Florida, leads the local effort.

The tracker maintains the demographic, program participation, and administrative information of detainees receiving care at the KBHU that is unrelated to health records, such as court information, country of citizenship, and language spoken. This information is analyzed to identify trends, evaluate the success of the program (based on program objectives), and help inform administrative and programmatic changes. For example, this data helps measure the patients' improved mental health well-being (by looking at how weekly check scores and weekly therapy session scores change over time) and evaluate active participation in immigration court proceedings (by looking at court appearances attended and court appearances missed).

System Access

The KBHU Tracker software is hosted only on:

- The IHSC shared drive dedicated for the KBHU, which requires IHSC approval to access files stored within the dedicated folder; and
- The ICE ERO CPD shared drive, which requires CPD leadership approval to access the folder the database is stored within.

There are two separate and distinct approval processes to gain access to each shared drive. The Office of the Chief Information Officer (OCIO) grants access after CPD senior leadership or IHSC Krome leadership approves access to their respective shared drives. The KBHU Tracker itself requires permissions to open and view the stored contents. ICE Headquarters KBHU administrator grants permission to access the database. No one can access the database without the proper permissions. Currently, the KBHU Tracker is operated by the KBHU program advisor and two additional data analysts (for reporting purposes).

Individuals Impacted:

Male detainees who are 18 years of age and over and are receiving care at the KBHU, their legal representatives with a Form G-28 (Notice of Entry of Appearance as Attorney or Accredited

Representative) on file, and ICE employees (business contact and system user information) for accessing and using the tracker.

Categories of Information:

The information collected come from the detainees enrolled at the KBHU; information provided by the detainees' attorney of record or family member, and clinical providers who cared for and/or evaluated the detainee.

The database maintains the following information:

On the detainee

- Name;
- A-Number;
- Primary language;
- Immigration status;
- Disciplinary incidents;
- Segregation;
- Court attendance;
- Participation in therapy sessions;
- Therapy progress;
- Detention information;
- Token economy information; and
- Medical information limited to the admitting diagnosis for the KBHU (e.g., depression).

On the ICE employee/contractor

- Name;
- User's email; and
- User's access rights (which determines if the ICE representative has access and the ability to edit/add information).

Relevant SORN:

- DHS/ICE-013 Alien Health Records System,[76] which covers information relating to

[76] *See* DHS/ICE-013 Alien Health Records System, 83 FR 12015 (March 19, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.

medical care; and

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[77] which covers records documenting ICE's criminal arrests, and those documenting most of ICE's immigration enforcement actions, such as the issuance of immigration detainers; the arrests, charging, detention, and removal of non-citizens for administrative immigration violations; the search for and apprehension of fugitive aliens; and ICE decisions concerning the grant or denial of parole to aliens

The SORNs list the authorities for maintenance of the records.

Privacy Impact Assessment

Privacy Risk*:* There is a risk that the information in the system is incorrect.

Mitigation: This risk is mitigated. The information collected comes from the detainees enrolled at the KBHU, a family member, the detainees' attorney of record, or clinical providers who cared for and/or evaluated the detainee. Although these individuals are ultimately responsible for the accuracy of the information provided, ICE data analysts regularly review the data to identify and correct errors and inconsistencies.

Records Retention Period:

These records are unscheduled and must be treated as permanent until the National Archives and Records Administration (NARA) establishes a schedule.

[77] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 Fed. Reg. 72080 (Oct. 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

Appendix O: Customer Identity and Access Management (CIAM)

Purpose and Use:

U.S. Immigration and Customs Enforcement (ICE) works with external patrons, such as non-citizens, private companies, and non-federal partners, who require access to certain public-facing ICE ServiceNow applications, such as the Office of Enforcement and Removal Operations (ERO) Bed Request System (BRS). BRS is used to create and approve bed reservations at detention facilities. ICE is implementing a Customer Identity and Access Management system (CIAM) using an Identity as a Service (IDaaS) vendor system to provide identity and access management services for external users requiring access to ICE services/applications.

The vendor system is an on-demand identity and access management service that enables enterprises to accelerate the secure adoption of their web-based applications, both in the cloud and behind the firewall. The vendor delivers a complete solution addressing the needs of information technology (IT) operations, end users, and business leaders with no customization required. The service offers the following:

- Secure, strong authentication sign-on for end users, thus providing seamless access to the applications or online services they need;
- Comprehensive user management that is integrated with the ICE Active Directory,[78] including user provisioning and de-provisioning, enabling IT to accelerate adoption of online services or applications; and
- Authentication analytics on system usage, utilization, and cost that provide IT the insight needed to optimize their application investments and address their compliance needs.

CIAM will allow ICE to manage its external patrons from a centralized point and enable ICE to leverage other cloud-based applications. For instance, when an external patron goes to BRS hosted on ServiceNow, ServiceNow will redirect the user to the vendor system. Then, the user will log in (authenticate) using the vendor system.[79] ICE will receive logs from the vendor that do not contain any personal identifiable information (PII).

Privacy Risk: There is a risk that information will be included in the system about members of the public that is not necessary or relevant to accomplish the system's purpose.

Mitigation: This risk is mitigated. CIAM provides identity and access management services for external users requiring access to ICE services/applications. For example, when an external patron goes to the public facing ICE ERO BRS hosted on ServiceNow, ServiceNow will

[78] Active Directory is Microsoft's directory service that is used by computers running Microsoft Windows to identify machines, networks, and users (similar to an electronic rolodex).
[79] The vendor system will provide the user with a token and redirect the user to ServiceNow to present that token, at which point they will be able to access the system.

redirect the user to the vendor system. Then, the user will log into the vendor system using a username and password. ICE will not receive any credential information provided to the vendor by the member of the public in order to gain access to the application.

Relevant SORNs:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS),[80] which outlines how DHS collects information from employees to provide authorized individuals with access to DHS information technology resources;
- DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System,[81] which covers the collection and management of PII for the purpose of issuing credentials for access to DHS facilities and information systems; and
- DHS/ALL-037 E-Authentication Records System of Records,[82] which covers collection of information from members of the public who electronically authenticate their identities.

Categories of Information:

Information collected from members of the public include:

- Name;
- Email address;
- User Principal Name (UPN);[83] and
- Password (requires associated Multifactor Authentication).[84]

Information collected from ICE employees and contractors, and other federal government users:

- Name;
- Email address; and
- Electronic Data Interchange Personal Identifier (EDIPI).[85]

[80] *See* DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792 (Nov. 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[81] *See* DHS/ALL-026 Department of Homeland Security Personnel Identity Verification Management System, 74 FR 30301 (Jun. 25, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.
[82] *See* DHS/ALL-037 E-Authentication Records, 79 FR 46857 (Aug. 11, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[83] UPN is the name of a user in an email address format, for example: john.doe@domain.com. However, a UPN is not the same as an email address. Sometimes, a UPN can be identical to a user's email address, but this is not a general rule.
[84] This is the process where a process where a user is prompted during the sign-in process for an additional form of identification, such as entering a code.
[85] The EDIPI number is a unique number assigned to the Personal Identity Verification (PIV) card that uniquely identifies each user.

Password and Multifactor Authentication will be managed by the ICE Active Directory.

Records Retention Period

The records are retained in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS) 3.2 Information Systems Security Records, item 30 and 31. Records must be destroyed six years after password is altered or user account is terminated.

Appendix P: Enforcement Coordination Center (E2C2) Automated Deconfliction System (ADS) Export

Purpose and Use:

The ICE Office of Homeland Security Investigations (HSI) Export Enforcement Coordination Center (E2C2) Automated Deconfliction System (ADS) collects, disseminates, compiles, and responds to interagency counter proliferation deconfliction requests.[86] E2C2 is an HSI managed and funded interagency task force, established by Executive Order 13558, that is designed to coordinate and enhance criminal, administrative, and related export enforcement activities of protecting national security through greater export enforcement and intelligence exchange.[87] E2C2's most critical function is the deconfliction and case coordination process, which determines whether a partner agency has an open record/open case consisting of a partner's target in that partner agency's database.[88] ADS consists of a secure, but unclassified, easy-to-use, web based ServiceNow (ITSM) system that automates the E2C2 deconfliction process.

Authorized HSI Counterproliferation Investigations Program (CPI) agents, totaling up to 300 individuals, have access to ADS, with HSI maintaining ownership of ADS with administrative and access rights. In addition to internal ICE users, other government agencies or participating government E2C2 partners (hereinafter "partner agencies") have access to ADS.[89] The external (i.e., non-ICE) users access the ServiceNow "ADS application" via the URL, e2c2ads.ice.gov, which has been created to provide access to interagency partners with a need to know. Partner agency personnel use this URL to submit queries to determine if another agency is already working on the same case.

The following is an example of how ADS could be used for the deconfliction function and case coordination process in the scenario where an individual, who is acting in his capacity as a

[86] Event deconfliction is the process of determining whether more than one law enforcement partner has an open case on the same activity at the same time.
[87] In November 2010, as part of the Administration's Export Control Reform Initiative, President Obama issued Executive Order 13558 creating the Export Enforcement Coordination Center (E2C2). The Executive Order mandated that DHS would house, manage, and fund the E2C2 and DHS handed that responsibility to HSI. See Executive Order 13558 -- Export Coordination Enforcement Center, *available at* https://obamawhitehouse.archives.gov/the-press-office/2010/11/09/executive-order-13558-export-coordination-enforcement-center.
[88] The open record is recorded as a "yes or no" response from the ADS standpoint.
[89] These partner agencies include: Bureau of Industry and Security (BIS); Federal Bureau of Investigation (FBI); Alcohol Tobacco and Firearms (ATF); Defense Criminal Investigative Service (DCIS); Defense Counterintelligence and Security Agency (DCSA); Directorate of Defense Trade Controls (DDTC); Defense Intelligence Agency (DIA); Export Import Bank (EXIM); National Aeronautics and Space Administration (NASA); Office of Foreign Assets Control (OFAC); United States Postal Inspection Service (USPIS); Customs and Border Protection (CBP), Countering Weapons of Mass Destruction (CWMD), and Office of Intelligence and Analysis (I&A) (DHS). The partner number total is fluid because E2C2 may not be able to identify appropriate successor points of contact as presidential administrations transition.

Company A executive, is suspected of shipping firearm parts and other illegal weapons without a license to a foreign country. The below-referenced process steps will be undertaken, using "Company A and the individual" as the deconfliction query data.

1. An E2C2 partner agency (e.g., FBI) will initiate a request to ascertain whether any partner agencies have an open case on the individual. The partner agency will submit a deconfliction request (or inquiry) through ADS to the E2C2.
2. ADS will distribute the deconfliction request to all participating E2C2 partner agencies' deconfliction points of contacts (POCs).
3. All POCs will receive the individual/Company A deconfliction request and manually[90] enter the query data into their respective case management systems.[91] The agency's case management system does not ingest data entered in ADS, and ADS has no direct connection to any partner agency's system. The purpose of inputting data into the case management system is solely to find out whether an investigate on is already underway with an open case on the target (i.e., obtain a positive or negative match).
4. Each partner agency will manually obtain information from their own case management systems respectively, including whether there is an open case on the individual/Company A, or any relevant intelligence report exists.
5. The deconfliction information obtained from the partner agencies' case management systems will be manually entered into the Deconfliction response section within ADS. When a partner agency transmits the response, ADS receives the entered response:
    a. Match. If the partner agency's system indicates that an open case or relevant intelligence report exists on the individual/Company A—this is a positive match. As such, the partner agency POC will manually enter the case agent or intelligence analyst name, contact information, and annotate that a positive match/find exists into ADS for the requestor to follow-up and further deconflict.
    b. No Match. If the partner agency's system indicates that an open case or relevant intelligence report does not exist, the agency POC will manually enter information into ADS stating that the agency has no open case.
6. The E2C2 partner responses (match/no match) will be sent to the E2C2 deconfliction program manager (an ICE employee) via ADS. Positive (i.e., "match") responses will be consolidated into a singular prepared response.
7. Using ADS, the E2C2 program manager then transmits the response to the requesting

[90] This manual data action reflects that ADS has no direct interconnection to the receiving agency's relevant case management system(s).
[91] In the case of ICE, this would be the Investigative Case Management system (ICM).

partner agency by (i) transmitting any positive matches and (ii) sharing additional information provided by the partner (e.g., name of the existing case agent or intelligence analyst who "owns" the open case or intelligence report). Additionally, the program manager will make the high-level match/no match results (with any additional, detailed information omitted) available through ADS to all participating E2C2 partners which have a "need to know" of the results.

All ADS deconfliction information is stored in a secure HSI database to support deconfliction searches, analysis, and potential information sharing.[92] ADS includes a robust analytical, tracking and reporting capability, and a planned predictive analytics application.[93] Network hosting and data storage is currently within an existing internal ICE network that can only be accessed by the E2C2 team for full search capabilities and accessed by partners on a "need to know" ad hoc basis.[94]

Relevant SORNs:

E2C2 ADS has SORN coverage under the DHS/ICE-018 Analytical Records SORN,[95] which provides notice of personnel searching, aggregating, and visualizing large volumes of information to enforce criminal, civil, and administrative laws under ICE's jurisdiction.

Categories of Information:

Information collected from individuals include:

- Name;
- Social Security number (SSN);
- Date of birth (DOB);
- Employee identification number (EID);
- Address;
- Phone number;
- Email address;

[92] All data is stored in ServiceNow's Fed Ramp IL4 certified cloud infrastructure. ADS data is stored behind the DHS firewall and the data is encrypted while at rest and in transmission.
[93] This refers to an advanced analytics artificial intelligence to be implemented in a later phase two. At the time of this PIA, technical details and methodologies regarding information security, data storage, network hosting, etc., are being fine-tuned but will comply with all applicable DHS IT, information assurance, and security requirements.
[94] Case details can only be seen by the Requestor (who requested the case) or by the Responding partner when a partner has responded to a deconfliction case request.
[95] *See* DHS/ICE-018 Analytical Records, 86 FR 15246 (Mar. 22, 2021), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Miscellaneous identifiers (such as A-Number, Visa number, Passport number, Driver's License number, etc.); and
- Financial information (such as bank account, credit card, or other financial account number).

Information collected on companies could include:

- Company name;
- Employer identification number (EIN);
- Data universal numbering system (DUNS) number;
- Incorporation date;
- Address;
- Phone numbers;
- Website/Internet Protocol (IP) address;
- Company email;
- Miscellaneous identifiers;
- Company officers;
- Foreign or domestic company (drop down option); and
- Additional information (any other relevant information that could support the investigation or deconfliction process).

Information collected on DHS, or "other federal" employees/contractors could include:

- Requester Information:
  - Name;
  - Agency/location;
  - Email address
  - Participant agency (joint case only).
- E2C2 Agency Partner Responses:
  - POC name;
  - Phone number;
  - Email address;

- Secure Terminal Equipment (STE); and
- Comments.

Records Retention Period

The records are retained in accordance with National Archives and Records Administration (NARA) Operation Reports, Determinations, and Deconfliction Records Schedule, DAA-0567-2016-0004. Data relevant to an HSI investigation is retained in accordance with the approved Investigative Case File Records Schedule, N1-36-86-1-161.3 for 20 years after the case closure.

Privacy Impact Assessment

Privacy Risk: There is a risk that information in the system will be accessed by unauthorized individuals.

Mitigation: This risk is mitigated. The requesting agent and E2C2 partner agencies (which have relevant information on the entity or individual in question) conduct operational deconfliction at the lowest possible level.[96] Within ICE, only authorized HSI CPI agents will have access to ADS, with HSI maintaining ownership of ADS with administrative and access rights. The external (i.e., non-ICE) users will access the ServiceNow "ADS application" via the URL, e2c2ads.ice.gov, which has been created to provide access to interagency partners with a need to deconflict. Additionally, there is a registration process that includes the signing of the rules of behavior by every requested user. Users cannot query information in ADS, but only enter information for deconfliction purposes. Select users have roles designated by their agencies to search within their own databases for positive or negative findings and respond to the requestor, via ADS.

[96] Lowest possible level refers to need to know but also to lower risk in general; the less information that is disseminated, the lower the chance that information would be compromised. A future version of ADS may include a cross domain capability to support classified deconflictions.

Appendix Q: Bed Request System (BRS) 2.0

Purpose and Use:

The Bed Request System (BRS) 2.0 is used by U.S. Immigration and Customs Enforcement (ICE) field officers (i.e., ICE detention center field officers and ICE Medical Approvers) and Office of Enforcement and Removal Operations (ERO) deportation officers to create bed space reservations at ICE and non-ICE detention facilities. The Bed Request System is a customized application residing on the ICE ServiceNow Platform environment as part of the Enforcement and Removal Operations Title 8 (T-8) Aliens Nationality Program. BRS 2.0 uses ServiceNow to manage the workflow for requesting, reviewing and decisioning bedspace requests.

Users of BRS 2.0 create bed requests for any noncitizen by Subject Identification (ID) number, sourced from the Enforcement Integrated Database (EID).[97] This provides ERO the ability to reserve bedspace prior to taking custody of the noncitizens.

BRS 2.0 ingests new data workflows to make use of newly available non-personally identifiable information facility capacity and availability data, and external access does not require the use of a third-party collaboration tool. This allows BRS 2.0 users more flexibility in requesting bedspace for noncitizens no matter where they are in the enforcement lifecycle.

Once a bed space request has been created, the Bed Request System streamlines these processes by continuously tracking each bed space request, decision, transfer, and booking information to provide near-real time bed space availability. Additionally, the Bed Request System compiles information about the subject from Enforcement and Removal Operations systems, such as the Risk Classification Assessment (RCA) and ENFORCE Detention Module for review. The Bed Request System allows ICE field officers to request beds and manage the available bed space inventory. The platform provides ICE field officers with a centralized portal to manage available beds within an Area of Responsibility (AOR), and request booking detainees against those beds.

Information collected through Bed Request System is available to ICE field officers and Enforcement and Removal Operations deportation officers.

Relevant SORNs:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS),[98] which outlines how DHS collects information from employees in order to provide authorized individuals with access to DHS information technology resources.

---

[97] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[98] *See* DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER),[99] which discusses information collected to support the detention and removal of individuals unlawfully entering or present in the United States.

Categories of Information:

Information maintained on subjects is collected at the time of the bed request from the Enforcement Integrated Database. This is created as a record on the Custody Information table in the Bed Request System. The information maintained includes:

Non-Citizen:

- A-Number;
- Age;
- Alert - Known Suspect Terrorist (KST);
- Alerts – Information that is added to the main page of the subject information file on the ENFORCE Detention Module (this is similar to a comments section that is easily viewable. It can be anything that the officer wants to communicate at the very beginning of the record that that he/she feels is important. Alerts can include prosecutions, and criminal information;
- Apprehension date;
- Bed intended occupation date;
- Case category – this is a category of the case that is usually a 2-digit alpha character field (i.e.: 8I);
- Case Category Description – This gives a more detailed description (i.e.: [8I] Inadmissible - ICE Fugitive - Expedited Removal);
- Country of birth (COB);
- Country of citizenship (COC); and
- Crimes – multiple records that can be attached to a custody information record that describes the crimes (description, classification, disposition, National Crime Information Center (NCIC) code charge date, conviction date).

Risk Assessment Classification:

[99] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, 81 FR 72080 (October 19, 2016) and subsequent updates, *available at* https://www.dhs.gov/system-records-notices-sorns.

- Criminal records – this is a collection of all the crime records in one field;
- Special vulnerabilities;
- Open wants or warrants;
- Supervision history;
- Security threat group (STG) status;
- Date of birth;
- Date of entry;
- Detainee currently in hold room (Yes or No);
- Detention classification – this is high, medium/high, medium, medium/low or low;
- Federal Bureau of Investigations (FBI) number;
- Final order date;
- Final order removal;
- Fingerprint Identification Number (FIN) number;
- Name (first, middle, last);
- Gang affiliation – this is a true/false field;
- Gang involvements – this is a text field to describe the gang information;
- Gender;
- Health condition observed at book in;
- Health observation date;
- Juvenile status;
- Medical comments;
- Medication at book in;
- Processing disposition – this is a disposition (i.e.: warrant of arrest/notice to appear) of what type of processing event the encounter is;
- Reason preventing removal; and
- Subject Identification (ID) number.

Information collected and maintained about ICE field officers, ICE medical approvers, and

ICE detention center approving officials includes:

- First and last name;
- Email address; and
- IRMNet ID.

Information collected and maintained about non-ICE detention facility and detention operations coordination center approving officials includes:

- First and last name;
- Email address; and
- Name of the facility they are going to be approving for.

Records Retention Period

The Bed Request System record retention is 75 years in accordance with records maintained in the Enforcement Integrated Database, which falls under Records Control Schedule DAA-0563-2013-0006.20. This schedule maintains records regarding the identification, investigation, apprehension, and/or removal of noncitizens unlawfully entering or residing in the United States. Under this schedule, records are retained for 75 years from the end of the calendar year in which the data is gathered. This ensures that the records are kept for at least the lifetime of the individuals to whom they pertain because they document the arrest, detention, and possible removal of individuals from the United States.

The Bed Request System development team will create a script to delete/purge records older than 75 years. Prior to purging/deletion, the Records Disposal Form 8-002 must be filled out requesting to destroy the records and be signed and approved by the Records Officer.

Privacy Impact Assessment

Privacy Risk: There is a risk of unauthorized access to sensitive personal data (of noncitizens) due to potential vulnerabilities in the system or misuse by internal users which can lead to privacy breaches, identify theft, or misuse of personal information.

Mitigation: This risk is mitigated. Robust access controls and authentication mechanisms are implemented to ensure only authorized personnel (i.e., ICE field officers, ICE detention center field officers, ICE medical approvers, and Enforcement and Removal Operations deportation officers) are authorized. Additionally, audit access logs are reviewed regularly on user activities to detect and respond to unauthorized access attempts.

Privacy Risk: There is a risk that the Bed Request System lacks the appropriate Section 1367 privacy safeguards required to prevent the inadvertent disclosure of sensitive information and ensure compliance with legal requirements.

Mitigation: This risk is partially mitigated. The Office of the Chief Information Officer and Enforcement and Removal Operations personnel will ensure that Section 1367 privacy safeguards are implemented to ensure compliance with statutory and DHS policy requirements. These privacy safeguards may be implemented at the system or application level. Safeguards include, but are not limited to, testing protocols, which shall include requirements (e.g., use case) to test functionality of these safeguards before deployment and continuously, such as after application or system updates/modifications or releases.

Privacy Risk: There is a risk that inaccurate or incomplete data maintained within the Bed Request System can lead to wrongful detention or the misallocation of beds, impacting the rights and liberties of noncitizens.

Mitigation: This risk is mitigated. Processes are established in the Enforcement Integrated Database ENFORCE Detention Module and Bed Request System for regular data quality reviews and audits to ensure the accuracy and completeness of the information stored. Training is provided to ICE field officers and Enforcement and Removal Operations deportation offices on the importance of data accuracy and the potential impacts of errors. Additionally, the Bed Request System user interface is configured to minimize the likelihood of data entry errors and allows for easy correction of inaccuracies.