



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 personnel¹ 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 Sites² 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 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-sorn>.

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-sorn>.

⁵ See DHS/ALL-033 Reasonable Accommodations Records System, 76 FR 41274 (July 13, 2011), available at <https://www.dhs.gov/system-records-notices-sorn>.

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-sorn>.

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 authentication¹⁶ 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 System²²
- OPM/GOVT-1 General Personnel Records²³

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 aliens 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 inquiries/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 System²⁶
- DHS/ALL-033 Reasonable Accommodations Records System²⁷
- OPM/GOVT-1 General Personnel Records²⁸

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 submitted, a

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>.



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 aliens 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
- 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 aliens 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, Alien Registration 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 alien 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 alien 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 aliens 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 an alien. The following data is ingested from 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 alien 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 Programming 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
- DHS/ICE-013 Alien Health Records System⁴²

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 forms, treatment records, mental health records, prescription drug records, dental history

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.



(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.