Privacy Impact Assessment
for the

USCIS ServiceNow: Service Desk

DHS/USCIS/PIA-070

August 31, 2017

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS), Office of Information Technology (OIT) offers technical support to USCIS employees, contractors, and non-USCIS personnel who have access to USCIS systems for official business. USCIS ServiceNow serves as the incident management system for service requests. USCIS is conducting this Privacy Impact Assessment (PIA) to evaluate the privacy risks and mitigations associated with the collection, use, and maintenance of personally identifiable information (PII) provided by individuals seeking USCIS Service Desk support.

Overview

U.S. Citizenship and Immigration Services (USCIS) Office of Information Technology (OIT) is responsible for the incident management functions for the agency. The goal of incident management is to restore normal service operations as quickly as possible following service disruptions to minimize the impact on business operations. The USCIS Service Desk serves as the single point of contact for logging, assigning, tracking, reporting, and resolving service requests for USCIS employees and contractors (herein after known as USCIS personnel), and other individuals who have access to USCIS information systems (non-USCIS personnel)[1]

USCIS ServiceNow does not support Service Desk tickets for public users seeking IT support for public-facing systems. USCIS offers other service support avenues for individuals experiencing issues with USCIS public-facing systems. USCIS ServiceNow serves as the technical solution to support the service incident management process. USCIS ServiceNow is an internal system that allows USCIS personnel the ability to create and report Service Desk tickets. It also allows USCIS IT Support Technicians to log tickets, classify tickets according to impact and urgency, assign to appropriate groups, escalate, and manage tickets through to resolution.

USCIS offers three avenues to submit a service request. USCIS personnel may initiate a Service Desk ticket through the self-service portal, called myIT, or by contacting the Service Desk by phone or email. All self-created Service Desk tickets are instantaneously processed and may be immediately accessed by the USCIS personnel who submitted the initial service request. Non-USCIS personnel cannot make requests on the portal. Non-USCIS personnel must call the Help Desk to report and resolve issues. All users seeking IT support or access to USCIS-owned systems are able to call the USCIS Service Desk to report a service incident.

Depending on the user submitting a Service Desk ticket, USCIS collects different information about the IT system, software, or technology-related information, the individual, and, in certain

[1] Non-USCIS persons from other Government agencies, state, local and federal law enforcement entities, as well as trade related organizations requiring access to USCIS-owned IT systems. Some common examples are employees from the Department of State, the Department of Labor, and the office of CIS Ombudsman.

circumstances, USCIS customers (i.e., applicants and petitioners). The following information is collected to create a Service Desk ticket:

- Employee Name
- Agency or business entity name;
- Email addresses
- Employee Login IDs
- Business, mobile, or home telephone number (for teleworkers)
- Business location
- Description of service request
- Name of IT system user is attempting to access (if applicable)
- Device name or number (if applicable)
- Ticket number for existing support requests

USCIS personnel are able to upload attachments into myIT, the self-service portal of ServiceNow. The uploaded documents may be used in support of remediation efforts related to the reported service request. In certain circumstances these documents may contain limited information about USCIS public customers. For example, a USCIS user may need to have a proof of immigration benefit pulled or reprinted in the event of a system or human error. In this case, the user would create a Service Desk ticket and provide a limited amount of customer information (e.g., USCIS Online Account Number, Social Security number, Alien Number) with the ticket to assist the IT Support Technician with locating the case in the relevant USCIS system. This information is only used for reference and is not transferred to or manipulated by any other USCIS systems. IT Support Technicians are not able to query ServiceNow to retrieve an attachment by a unique or personal identifier.

Once the information is appropriately entered in USCIS ServiceNow, a system-generated ticket with a unique ticket number is created and the ticket is classified based on priority. Once the Service Desk ticket is created, it is assigned to the appropriate USCIS IT Support Technician to handle as appropriate.

USCIS IT Support personnel use USCIS ServiceNow to track and manage incoming and existing Service Desk tickets. USCIS ServiceNow also offers a collaboration feature. The collaboration feature provides a chat interface optimized to enhance communication with the USCIS IT Support Technician and USCIS personnel that submitted the request. USCIS personnel are able to chat with IT Support Technicians through the Self-Service portal. Chat is a central feature for USCIS IT Support Technician to reach USCIS personnel.

Outside of USCIS ServiceNow, IT Support Technicians investigate and diagnose reported issues. During the investigation and diagnostic processes, IT Support Technicians may use USCIS ServiceNow to add work notes, which are appended to the Service Desk Ticket, as an issue is being evaluated. Work notes and other updates can be conveyed to the concerned parties through email notifications to facilitate communication.

After the reported issue is resolved, the IT Support Technician marks the Service Desk ticket as resolved and no further action is performed on the ticket. USCIS ServiceNow sends the user a summary and brief customer satisfaction survey. This survey is voluntary and helps OIT improve operations. No PII is collected; however, the survey is linked to the user's Service Desk ticket number.

Closed incidents are filtered out of view, but will remain in ServiceNow for reference and reporting purposes. Closed incidents can be reopened if the user or IT Support Technician reports that the service request was not sufficiently resolved.

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?

The specific legal authority for this collection of information is 5 U.S.C. § 301 "Departmental Regulations", 8 U.S.C § 1101, 1103, 1104, 1201, 1255, 1305, 1360 "Aliens and Nationality"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?

The DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) SORN covers the collection of a discreet set of personally identifiable information in order to allow IT Support to access, or to interact with, DHS information technology resources, and allow DHS to track the use of DHS IT resources.[2]

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

The USCIS ServiceNow System Security Plan was completed on April 26, 2016. The USCIS ServiceNow Authority to Operation (ATO) is pending the publication of this PIA and will enter into the Ongoing Authorization program, upon completion of this PIA. Ongoing Authorization requires USCIS ServiceNow to be reviewed on a monthly basis and to maintain its security posture.

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

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

The records in USCIS ServiceNow are covered by NARA General Records Schedule 5.8 Administrative Help Desk Records.

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.

USCIS ServiceNow is not subject to the PRA because federal employees and contractors are exempt from the PRA while engaged in official business.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

Create Service Tickets

USCIS uses ServiceNow to create and manage service tickets. To create a service ticket, USCIS ServiceNow collects the following information from the users who have made a service request:

- Full Name
- Agency Name
- Email Address(es)
- Login IDs
- Business, mobile, or home telephone number (for teleworkers)
- Business location
- Name of IT system attempting to access (if applicable)
- Device name or number (if applicable)
- Incident-related attachments [which may contain SSNs, A-Numbers, USCIS Online Account Number, Receipt numbers, home addresses, and business addresses from

other USCIS case management systems (i.e., Computer Linked Application Information Management System (CLAIMS 3) and USCIS Electronic Information System (USCIS ELIS))] (if applicable)

This information is collected to confirm the identity of the requestor and determine where he or she is located. Through Google's Application Program Interface (API), USCIS ServiceNow collects longitude, latitude, and time zone information for USCIS offices. Once a service ticket is created, a unique system-generated serial tracking number is assigned to the service request ticket.

Manage Service Tickets

USCIS IT Support Technicians use USCIS ServiceNow to track and process service request tickets. USCIS IT Support Technicians are able to update the status of the service request ticket by entering work notes and other updates. This information is also available for access by the user in myIT, the self-service portal. Non-USCIS personnel do not have access to their service tickets. USCIS personnel are also able to directly communicate with IT Support Technicians through a chat feature available in myIT.

Employee Survey Results

USCIS ServiceNow maintains survey results, which are linked to the requestor's service request ticket number. No PII is collected.

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

USCIS ServiceNow collects information directly from USCIS personnel and non-USCIS personnel. Only USCIS personnel using myIT, the self-service portal, can upload attachments. The uploaded attachments, which are used to aid in the remediation of incidents or problems, may contain PII or SPII about USCIS employees and the public (i.e., benefit requestors, beneficiaries, etc.). The uploaded information is used only for reference purposes and is not transferred, accessed, or manipulated by any other system. Attachments may contain SSNs, A-Numbers, USCIS Online Account Numbers, Receipt numbers, home addresses, and business addresses from other USCIS case management systems (i.e., CLAIMS 3 and USCIS ELIS).

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

Through Google's Application Program Interface (API), USCIS ServiceNow collects longitude, latitude, and time zone information for USCIS offices. USCIS office addresses, which are already available to the public, is the only information provided to Google from USCIS ServiceNow. USCIS ServiceNow does not provide user information, links between locations and users, or any

information about the location itself outside of the physical address. USCIS ServiceNow provides Google an address, and Google returns the longitude and latitude for the provided address. Once USCIS ServiceNow receives the longitude and latitude of that address, it resubmits those coordinates to Google who then provides the time zone information for those coordinates. Accurate time zone information is a benefit to USCIS as it aids in determining an office's business hours. IT Support Technicians can use the time zone information to determine the best time for contact based on the time zone of an office.

2.4 Discuss how accuracy of the data is ensured.

Data is collected directly from all users who make a request. Data collected from email and telephone requests are manually entered into USCIS ServiceNow by IT Support Technicians. For individuals who call into the USCIS Service Desk, the USCIS IT Support Technician asks a series of questions to confirm the caller's identity, according to the Service Desk Standard Operating Procedures (SOP), to assist with the inquiry, and prevent the unauthorized disclosure of information. USCIS ServiceNow automates the Service Desk accuracy by mapping a USCIS user's full name to the associated USCIS Active Directory account to ensure technical support reached the assigned technician and the appropriate individual seeking support. An electronic identity is created and assigned to a single individual in the USCIS Active Directory, with the purpose of identifying and authenticating that user specifically. Non-USCIS personnel cannot be checked in the Active Directory.

Information is checked for accuracy through self-verification by either the user or USCIS IT Support Technician entering information to process a service request. USCIS ensures data accuracy in USCIS ServiceNow through program coding to mitigate or prevent inconsistencies in data. The data fields in the input screen are configured to limit the possibility of entering malformed data (e.g., the system rejects 000/000/0000 phone numbers). USCIS personnel or USCIS IT Support Technicians can review and edit information prior to and after their submission. Additionally, authorized USCIS IT Support Technicians can correct and edit inaccuracies brought to their attention at any stage of the process.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that SPII is uploaded unnecessarily by users to create a service ticket.

Mitigation: This risk is partially mitigated. In order to create a service request ticket, limited business and contact information about USCIS personnel or non-USCIS personnel are obtained directly from the requestor. Only the minimum amount of information is gathered in order to identify an individual and distinguish him or her from other users with similar attributes (e.g., same first and

last name). Only USCIS personnel have access to myIT to upload files that may be relevant to users' requests for service and support. Due to technical limitations, there are no restrictions placed on the types of files uploaded, or the content they may contain. As such, it may be possible for USCIS personnel to upload files that contain sensitive PII and may include SSNs, A-Numbers, Receipt numbers, USCIS Online Account Numbers, home addresses, host names and dynamic IP addresses. This risk is partially mitigated because SPII that may be uploaded in an attachment, is not retrievable by unique identifier.

Privacy Risk: There is a risk that service requests received by phone are inaccurately entered into USCIS ServiceNow.

Mitigation: This risk is mitigated by through administrative and technical controls. USCIS IT Support Technicians ask a series of questions to confirm the caller's identity, according to the Service Desk SOP, to assist with the inquiry, and prevent the unauthorized disclosure of information. USCIS ServiceNow automates the Service Desk accuracy by mapping a USCIS user's full name to the associated USCIS Active Directory account to ensure technical support reached the assigned technician and the appropriate individual seeking support. An electronic identity is created and assigned to a single individual in the USCIS Active Directory, with the purpose of identifying and authenticating that user specifically. Non-USCIS personnel cannot be checked in the Active Directory.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

USCIS uses the data collected by USCIS ServiceNow to provide technical support and other service-oriented activities to support all USCIS systems and applications. USCIS technical support teams use a user's information, as defined in Section 2.0, to provide support for USCIS IT systems, assets, and properties. Service orientated activities include the following:

- Managing service requests tickets;
- Assigning work orders;
- Managing IT assets;
- Retrieving incident information;
- Troubleshooting;
- Depicting outage information across the enterprise;

- Identifying and locating service requests residing in other applications/systems for coordination activities; and
- Emailing correspondence and customer feedback surveys.

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.

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

No. Access to USCIS ServiceNow, including myIT, is limited to USCIS personnel. Non-USCIS personnel must telephonically report a service request to the USCIS Service Desk.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that unauthorized users may access records in USCIS ServiceNow.

Mitigation: This risk is mitigated. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards such as restricting access to authorized personnel who have a need-to-know. USCIS ServiceNow is a web-based application that is only available through the USCIS network. Access to USCIS ServiceNow is granted to only a limited number of users through DHS. Users must authenticate their credentials to gain access to the system.

Prior to gaining access to the system, USCIS ServiceNow displays a warning banner on the login screen to advise all users about proper and improper use of the data, that the system may be monitored to detect improper use, and the consequences of such use of the data. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. This acts as a deterrent to unauthorized activity.

Privacy Risk: There is a risk that USCIS ServiceNow could be used for purposes outside the scope of IT support.

Mitigation: The risk is mitigated through role-based access rules governing technical support personnel usage. USCIS personnel are able to access myIT to create a service ticket and are only able to view their own service requests along with the status. General users cannot view service requests submitted by other users. IT Support Technicians are able to view information submitted by general users that contain both PII and SPII as part of their duties in reviewing and responding to service

request tickets. Users are informed of their roles and responsibilities in regards to protecting PII. Users have been trained to provide only the minimum amount of PII necessary to complete a service request.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

The public receives general notice through the publication of this PIA and the DHS/ALL-004 GITAARS SORN. USCIS provides a Privacy Act Statement prior to the collection of any information on myIT as required by Section (e)(3) of the Privacy Act. The Privacy Act Statement notifies the individual about the authority to collect the information requested, purposes for collecting it, routine uses, and consequences of providing or declining to provide the information to USCIS. Applicants and petitioners who may have their information uploaded as an attachment do not receive notice that their information may be in ServiceNow beyond this PIA.

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

Individuals can choose to not provide information to address their IT matter, but doing so will prevent IT Support Technicians 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 privacy risk that individuals who call into the USCIS Help Desk are not provided with sufficient notice.

Mitigation: This risk is partially mitigated with USCIS publishing this PIA. The USCIS Help Desk is responsible for providing IT support to all users. In order to report a service request, these individuals may call into the USCIS Help Desk and provide basic business contact information to the IT Support Technician to address their issue. While callers are not provided direct notice by the USCIS Help Desk, callers understand that their contact information is used to assist with and process their service request. Callers understand that the IT Support Technician will not be able to assist them with the service request without this information.

Privacy Risk: There is risk that members of the public do not know their information is being stored in USCIS ServiceNow.

Mitigation: This risk is partially mitigated with USCIS publishing this PIA. The USCIS

overall mission is to adjudicate applications, petitions, and other benefit requests. USCIS uses a variety of systems in support of its mission. These systems may experience technical errors that result in production problems and outages that directly impact applicants, petitioners and benefit requestors. USCIS personnel are required to report such system issues to the USCIS Service Desk. In certain situations, USCIS personnel may need to recover records pertaining to these individuals. In these situations, USCIS personnel may include attachments containing personal identifiers of applicants, petitioners, and benefit requestors to retrieve the information in the respective USCIS system. Without this information, USCIS IT Support Technicians may be unable to resolve the assist and resolve the service request.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

The records in USCIS ServiceNow are covered by the NARA-approved General Records Schedule (GRS) 5.8 Administrative Help Desk Records, which permits agencies to maintain records for one year unless there is a business need. USCIS plans to destroy service request tickets, including the attachments containing S/PII, three years after the ticket is resolved, or when no longer needed for business use (i.e., ongoing investigations), whichever is appropriate. USCIS maintains historical service request tickets to analyze recurring problems and analyze trends.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that USCIS is maintaining attachments containing SPII for longer than needed to resolve the help desk ticket.

Mitigation: This risk is partially mitigated. USCIS determined there is a business justification to retain historical service tickets for up to three years as the information may be needed for reporting, training, trend analysis, IT Service continuity, and reviewing service level agreements. Access to these records are restricted to high level administrator roles. USCIS will standardize the process of deletion across ticket and file types to ensure the removal of SPII by mandating a uniform retention period of three years. In very limited circumstances, USCIS may

maintain records beyond the three year retention period for ongoing investigations and other legitimate business reasons.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

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. USCIS does not share USCIS 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.

USCIS does not share USCIS ServiceNow information with external entities

6.3 Does the project place limitations on re-dissemination?

USCIS does not share USCIS ServiceNow information with external entities.

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

USCIS does not share USCIS ServiceNow information with external entities.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no privacy impact related to external information sharing because USCIS ServiceNow information is not shared with external entities.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

USCIS personnel and non-USCIS users who telephonically report a service request receive USCIS ServiceNow-generated email detailing the issue and status of the request. Only USCIS

personnel who submit a request through myIT may view their records. Additionally, individuals may seek access to his or her USCIS records by filing a Privacy Act or Freedom of Information (FOIA) request. Only U.S. citizens and lawful permanent residents may file a Privacy Act request. Any person, regardless of immigration status, may file a FOIA request. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, he or she may mail the request to the following address:

National Records Center

Freedom of Information Act (FOIA)/Privacy Act Program

P. O. Box 648010

Lee's Summit, MO 64064-8010

Further information about Privacy Act and FOIA requests for USCIS records is available at http://www.uscis.gov.

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

USCIS personnel have an opportunity to correct their information by IT technical support or contact the USCIS Service Desk or log into myIT to correct inaccurate information. They may also submit a Privacy Act request as described in Section 7.1.

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

This PIA explains how an individual may correct his or her information once obtained by USCIS ServiceNow. In addition, USCIS provides notice to individuals via the applicable SORNs in Section 1.2.

7.4 Privacy Impact Analysis: Related to Redress

USCIS will always provide access and amendment of ServiceNow records. USCIS notifies individuals of the procedures for correcting their information in this PIA, Privacy Act Statement, and through the USCIS internal website (USCIS personnel only).

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

USCIS ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability. DHS security specifications require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

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

All USCIS personnel are required to complete annual privacy and security awareness training. The Culture of Privacy Awareness training addresses appropriate privacy concerns, including Privacy Act obligations. The Computer Security Awareness training examines appropriate technical, physical, personnel, and administrative controls to safeguard information. Additionally, the USCIS IT Support Technicians are required to take the following role based training: Change Management Training and USCIS ServiceNow Foundations Online Learning Course.

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

USCIS ServiceNow user accounts are managed through Identity, Credential and Access Management (ICAM). Users authenticate through ICAM to gain access to USCIS ServiceNow. ICAM deploys user role-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each operational role is mapped to the set of system authorizations required to support the intended duties of the role. The mapping of roles to associated authorizations enhances adherence to the principle of least privilege. Authorized users are broken into specific classes with specific access rights. This need-to-know is determined by the respective responsibilities of the user. Only necessary user identities are created and access rights assigned to USCIS ServiceNow. These are enforced through DHS and USCIS access request forms and access control procedures outlined in standard operating procedures.

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?

USCIS does not share information maintained in USCIS ServiceNow with organizations within or outside of DHS. However, should this change, USCIS has a formal review and approval process in place that requires approval of any new sharing agreement.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security