Privacy Impact Assessment
for the

DHS Correspondence and Inquiries Tracking Tools

DHS/ALL/PIA-007(a)

November 13, 2019

Contact Point
Huong Mai
Manager, Applications Branch
Office of the Chief Information Officer
Department of Homeland Security
(202) 447-0384

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) operates correspondence tracking tools to assist the Department in tracking and responding to inquiries from the public and reviewing official documents from DHS Components, other government agencies, Congress, the public, and the private sector. DHS receives and processes tens of thousands of pieces of correspondence ranging from letters to official rulings, policy statements, testimony, and legislative materials on an annual basis. DHS previously issued the DHS/ALL/PIA-007 Enterprise Correspondence Tracking (ECT) system privacy impact assessment (PIA) that solely covered the Department's use of the ECT system to track such correspondence. DHS is expanding the scope of that previously published PIA to account for the additional correspondence tracking systems and tools used throughout the Department to track and manage incoming and outgoing inquiries and documents. Accordingly, DHS is renaming this PIA "DHS Correspondence and Inquiries Tracking Tools."

Overview

DHS generates and processes a large volume of correspondence ranging from official rulings, policy, guidance, memoranda, legal materials, testimony, and letters on an annual basis. Due to the high amount of correspondence, some of which are uniquely challenging, DHS and its Components created systems and tools to track the documents received from the public, DHS offices and Components, external government agencies, Congress, and the private-sector, to efficiently handle the intake of correspondence, which require analysis, storage, categorization, and coordinated responses from DHS personnel assigned to review the correspondence on behalf of the Department, Component, or office. This system, previously referred to as DHS/ALL/PIA-007 Enterprise Correspondence Tracking (ECT),[1] is now comprised of several DHS, Component, and office information systems and tools and is renamed DHS/ALL/PIA-007(a) DHS Correspondence and Inquiries Tracking Tools to reflect its expanded scope. These Departmental (DHS) and Component systems (collectively referred to herein as DHS Correspondence and Inquiries Tracking Tools) run on existing platforms (e.g., SharePoint, Salesforce) to effectively track and respond to correspondence. Employees use these systems and tools to manage and share incoming and outgoing information including, but not limited to:

- Briefing material for senior leaders;
- Clearance and maintenance of official documents (e.g., operational guidance, standard operating procedures, memoranda, policies, legal positions, and materials);
- Documenting and responding to mail sent to DHS by the public;

[1] *See* DHS/ALL/PIA-007 Enterprise Correspondence Tracking (ECT), *available at* www.dhs.gov/privacy.

- Maintaining internal coordination within DHS; and
- Enabling the appropriate handling, records management, and customer service actions generated by the correspondence.

This PIA will primarily focus on the correspondence tracking process and the privacy protections in place to safeguard these data, but does not cover correspondence related to Freedom of Information Act (FOIA) or Privacy Act inquiries. For a discussion on FOIA and Privacy Act correspondence, review the DHS FOIA and Privacy Act Records Program PIA and corresponding updates.[2] See the attached appendices to this PIA for a list and description of tools developed and used by Components to manage incoming and outgoing correspondence.

Correspondence Lifecycle

Receipt & Assignment

The correspondence lifecycle begins when the Department or Components receive postal mail, email, telephone, or fax from the public, other DHS Component or offices outside government agencies, Congress, or the private sector.[3] Typically, correspondence are received by either the Executive Secretariat[4] (at either the DHS Headquarters or at the Component level) or by a specific office within the Department or respective Component. If sent to Executive Secretariat, the correspondence is routed to those offices that are required to review and respond. However, there are some instances in which an individual or organization may have a direct relationship with a specific office and may send correspondence directly to the office (e.g., Congress may send documents directly to a legislative affairs office, or an attorney may send correspondence directly to a DHS counsel). When a Department, Component, office, or individual is tasked to review a correspondence or inquiry, DHS commonly refers to these as "taskers."

Depending on how the entity receives the correspondence, a designated employee is responsible for inputting the correspondence and other relevant information into a DHS Correspondence and Inquiries Tracking Tool, and assigning personnel to review and respond to the tasker. Correspondence that originates within DHS or a Component that has recipients outside the Department, which requires Agency clearance before dissemination, will also go through this process. In this scenario, an office within a Component will generally send the document to

[2] *See* DHS/ALL/PIA-028(b) DHS FOIA and Privacy Act Records Program Update, *available at* www.dhs.gov/privacy.
[3] If DHS receives correspondence through the mail, DHS will scan the correspondence and upload it into the respective tool for processing.
[4] Executive Secretariat provides all manner of direct support to the DHS Secretary and Deputy Secretary or component leadership, respectively, as well as related support to leadership and management across the Department and/or component. This support takes many forms, the most well-known being accurate and timely dissemination of information and written communications from throughout the Department and our homeland security partners to DHS senior-leadership.

Executive Secretariat, which is responsible for distributing the document to relevant offices within the Department or Component for review, comments, or concurrence.

Review & Analysis

As described above, a tasker may be assigned to the entire Department, a specific component, specific offices within a component, or certain Subject Matter Experts (SME) within an office. The Component(s), office(s), or individual recipient(s) of a tasker is required to review and respond to the tasker within a designated timeframe. Reviews may consist of substantive comments or edits, concurrence or non-concurrence, or an official response to an inquiry received by an entity. These responses are either uploaded directly into the DHS Correspondence and Inquiries Tracking Tool by the reviewing entity, or returned to the responder to consolidate all comments, edits, and questions.

Response

After a designated recipient reviews the tasker, he or she is required to upload or log an individual or office's response into the respective DHS Correspondence and Inquiries Tracking Tool. The designated administrator will compile all responses, if applicable, and send them back to Executive Secretariat, which will then compile its own agency's responses, if necessary, to be sent back to the requesting entity.

Information collected in DHS Correspondence and Inquiries Tracking Tools may include the name, mailing address, email, and phone number of the individual sending the correspondence, or who placed a telephone call to the Department, Component, or office that warrants an official response. On rare occasions, public submitters voluntarily provide sensitive personally identifiable information (SPII),[5] such as DHS case numbers, U.S. Citizenship and Immigration Services (USCIS) receipt numbers,[6] Alien Numbers (A-Numbers), Social Security numbers (SSN), or some other identifying information in their correspondence to DHS. DHS does not request the public to provide SPII. USCIS, for instance, warns the public on its website not to provide SPII:

[5] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this analysis, SPII and PII are treated the same. Biometrics information is PII.
[6] The receipt number is a unique 13-character identifier that USCIS provides for each application or petition it receives. The agency uses it to identify and track its cases.

"Please do not include the following:

- Sensitive Personally Identifiable Information (SPII): Emails may not necessarily be secure. Therefore, we suggest that you do not email sensitive PII (such as your Social Security number) to us.

If SPII is submitted with correspondence DHS may retain the correspondence without redacting the original copy if it is necessary and relevant to reaching a decision (e.g., benefit applications). DHS and its Components will take reasonable precautions necessary to protect SPII it maintains.[7] However, any SPII determined to be not necessary will be redacted prior to be being entered into a correspondence and inquiries tracking tool. For instance, as noted in Appendix B, the Cybersecurity and Infrastructure Security Agency's (CISA), formerly known as National Protection and Programs Directorate's (NPPD), Office of Privacy works with its Executive Secretariat to either minimize the PII when possible, or provides instructions to password protect the files and then sends the password via a separate email.

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?

Pursuant to 5 U.S.C. § 301, DHS is authorized to implement departmental regulations that manage DHS's day-to-day operations. These operations include regulating employees, managing agency business, and controlling agency papers and property. The collection of documents within the DHS Correspondence and Inquiries Tracking Tools is authorized by 5 U.S.C. §301 (general agency powers for recordkeeping).

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

The following SORNs provide coverage for the DHS Correspondence and Inquiries Tracking Tools:

- DHS Mailing and Other Lists System[8] covers the contact information included in the correspondence and inquiries;
- DHS Correspondence Records[9] covers the collection, maintenance, and use of correspondence and inquiries;

[7] See Appendix.
[8] DHS/ALL-002 Mailing Lists and Other Lists Systems, 73 FR 71659 (Nov. 25, 2008).
[9] DHS/ALL-016 Correspondence Records, 83 FR 48645 (Sept. 26, 2018).

- General Information Technology Access Account Records System (GITAARS)[10] covers employee access to the systems and tools used to manage correspondence;
- DHS General Legal Records[11] provides coverage for DHS attorneys assisting in providing legal advice to DHS personnel on a wide variety of legal issues and collecting the information of any individual in litigation with the Department; and
- Various Component SORNs. In response to a specific correspondence, a component may access PII to retrieve information in the component's records. For example, USCIS may use a submitter's contact information to retrieve an individual's case in the Alien File, Index, and National File Tracking System.[12] USCIS will use this information to respond to the received correspondence.

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

DHS Components manage the system security and compliance of their respective DHS Correspondence and Inquiries Tracking Tools. These information technology systems are detailed in the attached appendices.

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

The National Archives and Records Administration (NARA) General Records Schedule (GRS) 4.1, item 010 covers taskers received by DHS Components, other government agencies, and Congress. Taskers and reminder emails are required to be destroyed immediately, or when no longer needed for reference, or according to a predetermined time period or business rule (e.g., implementing the auto-delete feature of electronic mail systems). Each DHS Component may create its own retention schedule, in consultation with NARA, for correspondence received (e.g., general inquiries, questions, letters, threats), as noted in the attached appendices.

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.

Unsolicited correspondence does not require a PRA approval. However, if it is a request for a benefit or other action, DHS will tie it to an existing approved collection or seek PRA approval.

[10] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).
[11] DHS/ALL-017 DHS General Legal Records, 76 FR 72428 (Nov. 23, 2011).
[12] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System, 82 FR 43556 (Oct. 18, 2017).

Section 2.0 Characterization of the Information

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

The information maintained in each tracking system maintained by the Department or a Component covered by this PIA varies, based on the collection requirements for each DHS office and Component. Please see the attached appendices for information collected by each system. However, generally, DHS Correspondence and Inquiries Tracking Tools may collect the following information:

- Prefix;
- First Name;
- Middle Name;
- Last Name;
- Suffix;
- Title;
- Organization;
- Home Phone;
- Business Phone;
- Mobile Phone;
- Fax;
- Email;
- Uniform Resource Locator (URL);
- Mailing, Work, or Home Address;
- Component specific unique identifiers (e.g., case number, A-Number);[13] and
- Unsolicited Sensitive information sent by the requestor.

In limited circumstances, DHS may send internal correspondence from one office to another (e.g., attorney to attorney) that may include case specific PII.

[13] See Appendix for a full list of data elements collected, including component specific identifying numbers.

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

The sources of information may include the following:

- The original sender of correspondence;
- DHS Headquarters;
- Internal DHS Components;
- The White House and the Executive Office of the President;
- The Office of the Vice President;
- Other federal agencies;
- Congressional offices;
- State and local governments;
- Foreign officials or governments;
- U.S. and foreign corporations;
- Non-government organizations; and
- The general public.

DHS employees may enter information into the DHS Correspondence and Inquiries Tracking Tools by:

- Scanning original documents into the respective DHS Correspondence and Inquiries Tracking Tool;
- Uploading the electronic version of the correspondence into the DHS Correspondence and Inquiries Tracking Tools;
- Manually keying the information received into the DHS Correspondence and Inquiries Tracking Tool; and
- Copying information received electronically and pasting it into the appropriate fields in an electronic form.

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.

2.4 Discuss how accuracy of the data is ensured.

DHS assumes the information received in the original correspondence is true and accurate for the purposes of processing correspondence, unless follow-up documentation or correspondence indicate otherwise. Should an inaccuracy be discovered during the tasker process, the Executive Secretariat or a designated individual will follow up with the submitter (using the contact information provided) to verify any inaccuracies.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk DHS collects more information than necessary to process the correspondence.

Mitigation: DHS only collects the amount of information necessary to act upon the request, correspondence, or other possible action item received by DHS. Although each correspondence is very likely to only include basic contact information such as the name, address, and phone number, some submitters voluntarily provide SPII, such as an SSN or A-Number. Dependent upon the circumstance, the SPII may or may not be placed into DHS Correspondence and Inquiries Tracking Tools, or SPII will be redacted from a scanned copy of the correspondence. Each component has its own process for handling SPII as described in the attached appendices.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

DHS uses the information to facilitate efficient, accurate, and timely handling of incoming correspondence, from other government agencies, Congress, the public, and the private sector. DHS uses Correspondence and Inquiries Tracking Tools to maintain a record of the contacts, enable follow-up correspondence from the Department, or to forward the correspondence to the appropriate Component or officer for action. DHS Correspondence and Inquiries Tracking Tools use PII to track incoming correspondence, assist DHS in analyzing requests, storing the large volume of correspondence, and categorizing and responding to individuals and entities. The collection of PII also facilitates DHS's ability to forward correspondence, by uniquely identifying the record.

The information in the DHS Correspondence and Inquiries Tracking Tools also enable Executive Secretariat offices to maintain the record copy of correspondence for senior leadership within a Component, as well as the DHS Secretary, Deputy Secretary, and the Chief of Staff.

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?

The information contained within DHS Correspondence and Inquiries Tracking Tools may be shared with any of the Executive Secretariats at DHS or with DHS Components. Each DHS component may share incoming and outgoing information contained within DHS Correspondence and Inquiries Tracking Tools for:

- Briefing material for senior leaders;
- Maintenance of official documents;
- Documenting and responding to mail from the public;
- Maintaining internal coordination within DHS; and
- Enabling the appropriate handling, records management, and customer service actions generated by the correspondence.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that users will have access to more PII and SPII than is necessary to respond to certain correspondence, due to differences in component source systems.

Mitigation: This risk is partially mitigated. Each component is required to redact unnecessary and irrelevant SPII and PII, prior to placing it into its own correspondence and inquiries tool, so this unnecessary information is not held by the Component and possibly shared with the Department, other components, or external entities.

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.

Notice is provided through this PIA and associated SORNs. However, since information in the DHS Correspondence and Inquiries Tracking Tools are unsolicited and generally not

provided on a government issued form containing a Privacy Act statement, notice is limited. Nonetheless, the Department and Components may caution the public on its websites not to provide SPII in their correspondence. For instance, on the USCIS website, under the "Contact Us" link, the public is asked not to provide certain information when contacting a service center:

"When contacting a service center. . . . Please do not include the following:

- Sensitive Personally Identifiable Information (SPII): Emails may not necessarily be secure. Therefore, we suggest that you do not email sensitive PII (such as your Social Security number) to us.
- Supporting documentation for your case: You must submit all documentation for your case according to the form instructions."[14]

General notices about information collected in order to respond to an inquiry is provided in the following SORNs:

- DHS *Mailing and Other Lists System*;[15]
- DHS *Correspondence Records*;[16]
- DHS *GITAARS*;[17]
- DHS *General Legal Records*;[18] and
- DHS Component SORNs.

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

The correspondence in DHS Correspondence and Inquiries Tracking Tools are voluntary submissions by the public to DHS or its Components, therefore, the submissions are inherently consensual.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk the sender may not be aware of how DHS and its Components will use and share their correspondence.

[14] https://www.uscis.gov/about-us/contact-us.
[15] DHS/ALL-002 Mailing Lists and Other Lists Systems, 73 FR 71659 (Nov. 25, 2008).
[16] DHS/ALL-016 Correspondence Records, 83 FR 48645 (Sept. 26, 2018).
[17] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).
[18] DHS/ALL-017 DHS General Legal Records, 76 FR 72428 (Nov. 23, 2011).

Mitigation: This risk is partially mitigated. Notice is provided through this PIA, associated SORNs, and on some websites. The information is sent to DHS voluntarily, without solicitation, and there is minimal privacy risk if an individual or entity is not aware of the notices provided.

Section 5.0 Data Retention by the project

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

The NARA GRS 4.1, item 010 covers taskers received by DHS Components, external government agencies, and Congress. Taskers and reminder emails are required to be destroyed immediately, or when no longer needed for reference, or according to a predetermined time period or business rule (e.g., implementing the auto-delete feature of electronic mail systems). Each DHS Component is responsible for creating its own retention schedules for correspondence received, including general inquiries, questions, letters, threats, etc., as noted in the attached appendices.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that DHS Components may be retaining certain correspondence longer than is necessary.

Mitigation: This risk is partially mitigated. The Executive Secretariat for each Component regularly reviews the correspondence to determine their statuses as a temporary or permanent record, and whether further retention, based on the records retention schedule GRS 4.1, item 010, is warranted. Each DHS Component is responsible for creating its own retention schedule for correspondence received (e.g., general inquiries, questions, letters, threats) as noted in the attached appendices.

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.

DHS does not grant external organizations access to the DHS Correspondence and Inquiries Tracking Tools. However, DHS may share documents maintained in the tools to respond to an external organization's request for information.

For instance, DHS may share correspondence with law enforcement personnel as required by law or request a legal opinion from an attorney at the Department of Justice. If DHS shares information with an outside entity, such as Congress or another federal agency, it is done by email,

fax, or hand-delivery, and not done using the correspondence and inquiries tracking tool. When shared externally, only the minimum amount of PII is provided, as authorized by the Executive Secretariat or required by statute. If DHS receives an inquiry from a member of Congress, the reply may include PII depending upon the topic of the correspondence, whether the underlying individual has provided consent for release of his/her information, and applicable Component regulations or policies. Please refer to the attached appendices for a description on how components share information from their tracking tool externally.

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

DHS and its Components may only share information externally in compliance with the routine uses identified in the SORNs listed in Section 1.2.

6.3 Does the project place limitations on re-dissemination?

If an external agency determines re-dissemination is needed (e.g., for law enforcement purposes), that agency should notify the appropriate DHS Component before any re-dissemination occurs.

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

DHS records the disclosure within the appropriate DHS Correspondence and Inquiries Tracking Tool or email audit trail. This audit trail maintains a record of the DHS individual or DHS office sending the correspondence, additional documents (if any), were transmitted, and the destination of the transmission. Additionally, the audit trail discloses actions, such as unauthorized access, modification, and destruction of data. Further information is provided below in Section 8.0 Auditing and Accountability.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is risk that external entities may receive more information than necessary.

Mitigation: This risk is partially mitigated. Any correspondence transmitted by DHS is documented in an audit trail. This audit trail maintains a record of the DHS individual sending the correspondence, additional documents transmitted, if any, and the destination of the transmission. For instance, if there is any unauthorized use of information contained in the DHS Correspondence and Inquiries Tracking Tools, the audit trail will capture and reveal actions such as unauthorized access, modification, and destruction of data.

In the event DHS or a Component determines a correspondence should be reviewed by an external agency, the correspondence will be shared, as appropriate, and in accordance with an approved routine use from the applicable SORN(s).

Section 7.0 Redress

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

U.S. citizens or Lawful Permanent Residents may gain access to their own information by submitting a Privacy Act request. All individuals may submit a Freedom of Information Act (FOIA) request in writing to:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
245 Murray Drive, S.W.
STOP-0655 Washington, D.C. 20528.

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under contacts.

Individuals may request access to records about themselves by following the procedures outlined in the SORNs identified in Section 1.2. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interest.

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

If individuals obtain access to information pursuant to the procedures outlined in the SORNs identified in Section 1.2, they may seek correction of any information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the SORNs identified in Section 1.2.

Should an inaccuracy be discovered, DHS may contact the originating submitter to obtain corrected information. Information can manually be updated in DHS Correspondence and Inquiries Tracking Tools to make administrative changes (e.g., spelling of names, prefixes, suffixes). Additionally, some of the DHS Correspondence and Inquiries Tracking Tools have data integrity checks built into the system where the address is verified with the U.S. Postal Service.

Requests for corrections can be submitted to the DHS Correspondence Department, U.S. Department of Homeland Security, Washington, DC 20528.

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

Individuals are notified of the procedures for correcting their information through the SORNs identified in Section 1.2, this PIA, as well as DHS and Component FOIA and Privacy Act webpages, available at www.dhs.gov.

All or some of the requested information may be exempt from access under the Privacy Act or FOIA (for those individuals who are not U.S. citizens or lawful permanent residents and whose records are not covered by the Judicial Redress Act) or in order to prevent harm to law enforcement investigation or interests. For those records protected by the Privacy Act and the Judicial Redress Act, the exemptions would be the same as those claimed in the underlying source system. Providing individual access to such records may inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

7.4 Privacy Impact Analysis: Related to Redress

There is no additional privacy risk associated with redress in relation to the DHS Correspondence and Inquiries Tracking Tools PIA. DHS provides individuals with access and correction to their records when contacting DHS or when requested through a FOIA or Privacy Act 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?

DHS Correspondence and Inquiries Tracking Tools use database-level auditing to capture information associated with any viewing, creating, updating, or deleting of records, and the user that performed the activity. The application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. The audit trail discloses actions such as unauthorized access, modification, and destruction of data. DHS Correspondence and Inquiries Tracking Tools information is also safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the stored

information. Additionally, information is securely shared via encrypted system connections or encrypted email.

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

DHS employees and contractors are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. Privacy training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). The Computer Security Awareness Training examines appropriate technical, physical, and administrative control measures.

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

DHS uses 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 providing a user with the minimum amount of privilege necessary. Authorized users are broken into specific classes with specific access rights. This need-to-know is determined by the respective responsibilities of the employee. These are enforced through DHS access request forms and 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?

DHS has a formal review and approval process in place for new information sharing agreements. Any new use of information, or new access requests for the system, must go through the DHS change control process and must be approved by the proper authorities of this process, such as the DHS Privacy Office, Chief of Information Security Officer, and Office of General Counsel.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There is a risk that there will be a lack of oversight and accountability.

Mitigation: This risk is largely mitigated through the robust auditing, security, training, and user access controls described above. For instance, if there is any unauthorized use of

information contained in the DHS Correspondence and Inquiries Tracking Tools, the audit trail will capture and reveal actions, such as unauthorized access, modification, and destruction of data.

Responsible Officials

Christina Bobb
Executive Secretary
Department of Homeland Security

Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A: Component Correspondence and Inquiries Tracking Tools

DHS Headquarters Level and Executive Secretary Correspondence Systems

Intranet Quorum (IQ)

The IQ system is a browser-based workflow system that DHS uses to respond to inquiries from the public and other government and private-sector agencies. IQ is designed to manage correspondence tracking with pre-defined routing inside workflow templates. Each DHS organization may use IQ and share incoming and outgoing information contained within the system to: (a) Provide briefing material to senior leaders; (b) Maintain official documents; (c) Document and respond to citizen mail sent to DHS; (d) Maintain internal coordination within DHS; (e) Enable the appropriate handling, records management, and customer service actions generated by the correspondence; and (f) Track staff workflow and case management functions.

The scope of the information collected in IQ is limited to the amount of data necessary to act upon the request, correspondence, or other possible action item received by DHS. If information is provided that is not relevant, it is either not collected (e.g., information taken by phone is not written down) or it is grayed out to users (if in electronic form). These practices differ because many submissions arrive at DHS in unsolicited correspondence. If information is extraneous it is either grayed out within IQ data fields or not entered at all.

Individuals Impacted:

Individuals who submit inquiries, complaints, comments, or other correspondence to DHS; individuals who are the subject of the correspondence; and any DHS employee or contractor assigned to respond on behalf of DHS.

Data Elements:

DHS may collect and use the contact information of submitters or responders, such as:

- Name;
- Organization;
- Phone/fax numbers; and
- Email.

The system will also track certain demographic identifiers of the submitter, such as:

- Country of origin;
- Date of birth;

- Gender.

Additionally, IQ will retain Social Security number (SSN) or A-Number if necessary to respond to the request made in the correspondence; and any attachments that may include PII.

Sources of Information:

Records are obtained from all sources of incoming correspondence and responses by DHS, including members of the public, non-governmental organizations, business, and governmental entities such as Congress.

Information Sharing:

IQ information is shared among all DHS components and offices. It does not connect or share information with external agencies or organizations.

System Access:

The DHS Executive Secretary is the final authority on who may have access to IQ, and what their roles and responsibilities are. Access to IQ is limited and not generally available to the DHS population.

Applicable System of Records Notice(s):

- DHS/ALL-002 DHS Mailing and Other Lists System, which covers the contact information included in the correspondence and inquiries;
- DHS/ALL-016 Correspondence Records, which covers the collection, maintenance, and use of correspondence and inquiries;
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), which covers employee access to the system;
- DHS/ALL-017 DHS General Legal Records, which provides coverage for DHS attorneys assisting in providing legal advice to DHS personnel on a wide variety of legal issues and collecting the information of any individual in litigation with the Department; and
- Various Component SORNs (In response to a specific correspondence, a component may access PII to retrieve information in the Component's records. For example, USCIS may use a submitter's contact information to retrieve an individual's case in DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System. USCIS will use this information to respond to the received correspondence.)

Retention Period:

Under NARA schedule N1-563-07-001, IQ records are considered temporary. DHS will cut off files at the end of the fiscal year in which the record was created in the system. All records will be destroyed 10 years after the cut off.

Office of the General Counsel (OGC) Regulatory Affairs Management System (RAMS)

RAMS is a regulatory action tracking system, workflow management tool, and reporting solution that was designed to facilitate the review and clearance of regulations throughout DHS. The OGC Regulatory Affairs Law Division (RLD) is the administrator of the system, and user access is assigned to DHS headquarters/component/sub-agency groups and various OGC subject matter experts.

The RAMS software suite integrates three separate systems: Microsoft Dynamics CRM 2016 (to automate and track the workflow), Microsoft SharePoint 2010 (to store documents for reviewers and for future reference), and SQL Server Reporting Services (SSRS) (to generate status reports and other metrics). Together, these systems are an integrated tool for automating and tracking a regulatory action's progress through the DHS regulatory clearance process and generating metrics on the progress of those regulatory actions. RAMS automates workflows, improves information capture and retrieval, and provides visibility and metrics for DHS regulatory actions. RAMS has robust tracking, collaboration, and reporting functionalities.

Individuals Impacted:

- DHS employees who are assigned to a RAMS CRM license and perform a broad range of tasks throughout the regulatory clearing process. Depending on his or her role in RAMS, a user might upload data and documents into the system, coordinate review of documents in RAMS SharePoint, or submit documents to OGC.
- DHS employees who only use RAMS SharePoint for the review and analysis of RAMS documents.
- Employees in the Office of Management and Budget (OMB) who submit Interagency Regulatory Actions to DHS for review. RAMS collects the employee names and office contact information of the submitters.

Data Elements:

Information collected in RAMS includes the user names (CRM Users only) and office contact information of DHS and Interagency employees.

- First Name;

- Last Name;
- Title;
- Organization;
- Business Phone; and
- Email.

Sources of Information:

Sources of information include DHS headquarter groups, DHS components; and other federal agencies. Most documents from external federal agencies are submitted to RAMS by the Office of Management and Budget.

Information Sharing:

RAMS information is shared among DHS components and offices. The system does not connect or share information with external agencies or organizations.

System Access:

OGC RLD is the administrator of the system. One hundred RAMS CRM licenses are available to be assigned to DHS employees. These employees also have access to RAMS SharePoint. Additional DHS employees may be given permission to access RAMS SharePoint if there is a business need to access regulatory documents in the RAMS SharePoint environment.

Applicable System of Records Notice(s):

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);
- DHS/ALL-016 Correspondence Records System of Records; and
- DHS/ALL-17 General Legal Records.

Retention Period:

Records are retained in accordance with GRS 4.1, item 010.

Executive Secretary (ExecSec) Correspondence Analysts Task Tracker[19]

CATT is a Microsoft Dynamics 365-based task management system for the management and assignment of tasks and correspondence between ExecSec and other DHS Components/departments.

[19] Other DHS Components use separate iterations of CATT in the same manner.

CATT primarily uses DHS Customer Relationship Management (CRM) as a Service (CRMaaS) which is based on Microsoft Dynamics 365. It also uses SharePoint as a Service (SPTaaS) for document management.

CATT integrates with DHS email and via mailbox monitoring can automatically pull emails into the system for automated task creation. It uses custom fields, business rules, and workflows to create dynamic forms and processes for task management. Documents are uploaded to SharePoint and inherit metadata fields from information stored in Dynamics.

Individuals Impacted:

Federal employees and members of the public.

Data Elements:

Information collected from federal employees and members of the public includes:

- Email address;
- First and last name;
- Job title;
- Mailing address;
- Organization mailing address;
- Organization Role;
- Organization Site;
- Phone number;
- Username; and
- Title (e.g., Mr., Mrs., Ms.).

Sources of Information:

Records are obtained from all sources of incoming correspondence and responses by DHS, including members of the public, non-governmental organizations, business, and governmental entities such as congress.

Systems Access:

Access to CRMaaS and SPTaaS is restricted to IP addresses approved by DHS, ensuring that they are only accessible to badged DHS employees while on a DHS network. No part of CATT can be accessed outside the DHS domain or by a member of the public.

Information Sharing:

CATT may connect to SharePoint as a Service for document management and retention, as well as the DHS Active Directory is used to look-up information about DHS employees and contractors. It also integrates into DHS Email as a Service for mailbox monitoring.

Applicable Systems of Records Notice(s):

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS); and
- DHS/ALL-016 Correspondence Records.

Retention Period:

The NARA General Records Schedule (GRS) 5.2, item 010, covers taskers and documents contained within the Task Tracker and can be destroyed once business use ceases.

CBP Correspondence and Inquiries Tracking Tools

CBP Tracking 2.0

CBP Tracking 2.0 is a multi-tier, web-based case management system that all CBP Headquarters (HQ) offices use to track document and data requests through case completion. The correspondence includes: Congressional responses; official rulings; policy statements; and records requests, inquiries, complaints, and testimony received from the public, other government agencies, and the private sector. The system uses a customizable Commercial-off-the-Shelf (COTS) product which facilitates real-time reporting, document searching, and status tracking. CBP Tracking 2.0 is used by the CBP Office of the Executive Secretariat (OES) to process information and correspondence requests received at HQ. In addition, the Management Inspections Division (MID) within the Office of Accountability uses CBP Tracking 2.0 to maintain an electronic data repository and reporting capabilities for all audit and inspection data.

Individuals Impacted:

CBP Tracking captures data on members of the public, which is obtained from correspondence received and sent in response to queries, and the actual documents are scanned and saved in the form of PDF or Word files in the respective system folders.

Data Elements:

Personally Identifiable Information in CBP Tracking 2.0 includes:

- Originator/Requestor name and contact information;
- Constituent/Subject name and any identifying information required (may include sensitive personally identifiable information, including: date of birth, SSN, A-Number);
- Incoming Documents, (which may include SPII); and
- Relevant notes and status information, (which may include SPII and law enforcement information).

CBP Tracking also contains CBP employee information, including name and contact information, but does generally not contain employee SPII unless the employee is the subject of a request.

Sources of Information:

CBP Tracking 2.0 is used to create a new record or "folder" for every piece of correspondence received by CBP. The correspondence is grouped into: OES Correspondence, Questions for the Record, Internal Correspondence, and Congressional Reports. The MID module contains information related to audits, inspections, and recommendations.

The actual correspondence is uploaded as Word or PDF files attached to the respective folders. The data captured in folders and the attached correspondence files can be retrieved via free text searches based on key field names.

Information Sharing:

CBP Tracking 2.0 does not share information outside of CBP.

System Access:

Currently, OES uses Case Tracker 2.0 to process information and correspondence requests and share that material with CBP Correspondence staff, Questions for the Record staff, DHS Tasking/Briefing staff, CBP Congressional Reports staff, and the CBP Office of the Commissioner. The MID module is accessible only to designated staff with a need to access the information. Records are kept physically intact, identifiable, and retrievable to allow access by authorized users.

Applicable System of Records Notice(s):

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System;
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS); and
- DHS/ALL-016 Correspondence Records.

Retention Period:

Documents in CBP Tracking 2.0 are considered temporary, and can be destroyed or deleted when no longer needed for business purposes in line with GRS 4.1, item 010.

FEMA Correspondence and Inquiries Tracking Tools

FEMA Action Concurrence Tracker (ACT)

ACT is a FEMA-wide enterprise tool to track FEMA's internal review and concurrence of official agency correspondence. Upon FEMA's receipt of correspondence (e.g., congressional inquiries, Department taskers) the action officer for the responsible program office will enter the subject and/or nature of the correspondence; name and contact information of FEMA personnel required to review or take action related to supporting response; and relevant dates. The correspondent's name, job title, phone number, address, and email address may also be added to the task.

ACT allows users to add attachments to generated tasks. These attachments are stored in a dedicated SharePoint online library. ACT creates a link to the SharePoint library within the task. The SharePoint library permissions are set to "contribute" for all ACT users; however, navigation to the library is only published within each ACT tasker effectively limiting access to each attachment to the individuals assigned to the task.

Individuals Impacted:

Individuals who submit inquiries, complaints, comments, or other correspondence to FEMA, individuals who are the subject of the correspondence, and any FEMA employee or contractor assigned to respond on behalf of FEMA.

Data Elements:

FEMA may collect and use contact information from members of the public, such as:

- Name;
- Job title;
- Mailing address;
- Phone number;
- Email address; and
- Any attachments sent with the correspondence that may contain PII or SPII.

FEMA may also collect and use the following information from FEMA Employees and contractors accessing ACT:

- Name;
- Email address (individual or group inbox); and
- Organization.

Sources of Information:

Records are obtained from all sources of incoming correspondence and responses by FEMA including members of the public, non-governmental organizations, business, and governmental entities such as Congress.

Information Sharing:

ACT does not connect, receive, or share PII with any external agencies or components. Any sharing of information required to respond to correspondence is conducted outside the system.

System Access:

Only FEMA Action Officers and system administrators have complete access to the system. FEMA employees can be assigned to respond to certain correspondence, and will be granted access to information only related to that task. ACT does not allow any access to individuals or organizations outside FEMA.

Applicable System of Records Notice(s):

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS); and
- DHS/ALL-016 Correspondence Records.

Retention Period:

Documents in ACT are considered temporary, and can be destroyed or deleted when no longer needed for business purposes in line with GRS 4.1 item 010.

ICE Correspondence and Inquiries Tracking Tools

Immigration and Customs Enforcement Correspondence and Task Tracking (I-CATT)

The U.S. Immigration and Customs Enforcement (ICE) Office of the Executive Secretariat (OES) is responsible for providing professional, timely, and accurate responses to all public, governmental, and congressional correspondence addressed to the agency. ICE Correspondence and Task Tracking (I-CATT) is the central repository and tracking system for agency requests for information; executive correspondence; criminal, civil, and administrative law enforcement and non-law enforcement-related inquiries; and certain internal matters and memoranda (i.e., taskings). ICE OES uses I-CATT to facilitate efficient, accurate, and timely handling of taskings and maintain a record of internal coordination on taskings. Though I-CATT does not directly collect Sensitive PII, in order to facilitate correspondence tracking, it may incidentally host Sensitive PII provided in documents received from submitters or from other ICE offices and uploaded into the system repository. The nature of the Sensitive PII varies depending on the type of tasking.

Individuals Impacted:

DHS federal employees and contractors; other state, local, and federal employees; and members of the public.

Data Elements:

The information collected in I-CATT includes ICE user names and office contact information (e.g., email, phone, title) of federal employees and contractors that have access to I-CATT and are responsible for responding to taskings.

Other information hosted in I-CATT will vary depending on the tasking and may include:

- First and last names of members of the public;
- Names and titles of local, state, federal employees, foreign officials and entities;
- Names of organizations;
- Home, business, and mobile telephone numbers;
- Fax numbers;
- Email addresses;
- Uniform Resource Locator (URL);
- Mailing, work, or home addresses;
- Country of origin;
- Dates of birth;

- Gender;
- SSN;
- USCIS Receipt Number;
- A-Number;
- Social media handle;
- Biometric information; and
- The specific content of any tasking.

This list is not exhaustive and will vary based on the tasking. Incidental collection related to an individual tasking will be collected that may contain the above information or other information no reflected in the above list.

Sources of Information:

Sources of information include, DHS Headquarters and internal DHS components, Congressional offices, the White House, and other federal agencies; state and local governments and foreign officials and governments; non-government organizations; and the general public.

Information Sharing:

ICE may share documents contained within the tools in response to an external organization's request for information. This allows the efficient transfer of documents to individuals outside of the tracking tool for tasking's, or to provide information to those that require it, but do not have access to the tool. Information may be shared with other state, local, and foreign officials and agencies, Members of Congress, the White House, and other members of the public. Should ICE externally share correspondence, only the minimum amount of information necessary is shared, depending upon the reason for sharing this information as authorized by the Executive Secretary or required by statue.

System Access:

ICE does not grant external organizations access to I-CATT. Only ICE employees and contractors responsible for responding to taskings will have access to I-CATT.

Applicable System of Records Notice(s):

- DHS/ALL-016 Correspondence Records

Retention Period:

The NARA General Records Schedule (GRS) 5.2, item 010, covers taskers and documents

contained within I-CATT and can be destroyed once business use ceases.[20]

Immigration and Customs Enforcement Correspondence (ICE) Office of Human Capital Task Tracker (Task Tracker)

The U.S. Immigration and Customs Enforcement (ICE) Office of Human Capital (OHC) Task Tracker is the central repository and tracking system used by OHC to facilitate efficient, accurate and timely handling of taskings. OHC uses the Task Tracker to consolidate taskings generated from two systems, the ICE Correspondence and Task Tracking (I-CATT) and ServiceNow. The I-CATT system generates taskings related to requests for information; executive correspondence; employee relations; and certain internal program matters and memoranda. ServiceNow generates taskings related to employee inquiries. Though the Task Tracker does not directly collect Sensitive PII, in order to facilitate correspondence tracking, it may incidentally host Sensitive PII provided in documents submitted by requestors and uploaded into the system repository. The nature of the Sensitive PII varies depending on the type of tasking.

Individuals Impacted:

DHS federal employees and contractors; other state, local, and federal employees; and members of the public.

Data Elements:

The information collected in the Task Tracker includes ICE user names and office contact information (e.g., email, phone, title) of federal employees and contractors that have access to the Task Tracker and are responsible for responding to taskings.

Other information hosted in the Task Tracker will vary depending on the tasking and may include:

- First and last names of members of the public;
- Names and titles of local, state, federal employees;
- Foreign officials and entities;
- Names of organization;
- Home, business, and mobile telephone numbers;
- Fax numbers;
- Email addresses;

[20] See General Retention Schedule (GRS) 5.2, Item 010: Transitory Records, https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf.

- Uniform Resource Locator (URL);
- Mailing, work, or home addresses;
- Country of origin;
- Dates of birth;
- Gender;
- SSN;
- A-Numbers, USCIS Receipt Number, or other identifying number; and
- The specific content of any tasking.

Sources of Information:

Sources of information include: DHS Headquarters and internal DHS components; congressional offices; the White House; other federal agencies; state and local governments and foreign officials and governments; non-government organizations; and the general public.

Information Sharing:

ICE may share documents contained within the Task Tracker in response to an external organization's request for information. This allows the efficient transfer of documents to individuals outside of the tracking tool for taskings, or to provide information to those that require it, but do not have access to the tool. Information may be shared with other state, local, and foreign officials and agencies, Members of Congress, the White House, and other members of the public. Should ICE externally share correspondence, only the minimum amount of information necessary is shared, depending upon the reason for sharing this information as authorized by the Executive Secretary or required by and consistent with statute.

System Access:

ICE does not grant external organizations access to the Task Tracker. Only ICE employees and contractors responsible for responding to taskings will have access to the Task Tracker.

Applicable System of Records Notice(s):

- DHS/ALL-016 Correspondence Records.

Retention Period:

The NARA General Records Schedule (GRS) 5.2, item 010, covers taskers and documents contained within the Task Tracker and can be destroyed once business use ceases.[21]

[21] See General Retention Schedule (GRS) 5.2, Item 010: Transitory Records, https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf.

CISA Correspondence and Inquiries Tracking Tool

Executive Secretariat Task Tracker (ESTT)

ESTT is a customized tool designed in the Microsoft SharePoint platform to address the Cybersecurity and Infrastructure Security Agency (CISA) Executive Secretariat Task process. ESTT automates the ExecSec process efficiently while providing status, alerts, and communications for task fulfillment. ESTT tracks tasks throughout the life cycle and supports task actions such as creation, assignment, approvals, notifications, updates, cancellations, and closeouts using complex workflows and business logic.

ESTT also provides a detailed transactional history of each task's progress through multiple organizations leveraging a rich graphical user interface (GUI) composed of executive dashboards and forms. Dashboards in ESTT provide insight into task status with user managed filters and access to a repository for associated artifacts. Both tasks and artifacts are preserved in a searchable format. This solution provides a standard process for all of CISA and eliminates manual, time-consuming work to keep status of task work.

Individuals Impacted:

Members of the public, CISA employees and contractors, and employees of other federal agencies.

Data Elements:

PII included in correspondence entered into ESTT would be included in the system. This PII could include names and email addresses of those individuals; however, most information is organization and mission specific.

Traditionally, whenever any sensitive PII needs to be disseminated via ESTT, the CISA Office of Privacy works with CISA Executive Secretariat to either minimize the PII when possible, or provides instructions to password protect the files and then send the password via a separate email (so that the password isn't also displayed in ESTT). The CISA Office of Privacy has also conducted role-based training for Executive Secretariat staff in the past to ensure they knew how to handle PII associated with taskers.

Sources of Information:

Any documents or materials requested and/or submitted as required by official DHS tasks could be included in ESTT. Some examples may include briefing materials for senior leaders, documents or reports requiring official clearance, materials requiring internal coordination within CISA, and correspondence submitted to CISA.

Information Sharing:

ESTT Does not share information outside of CISA.

System Access:

ESTT imposes security constraints on task materials via role-based access rules and organizational structure. Certain controls are built into ESTT to prevent unauthorized access to information. Permissions are associated with the group and applied to each site within ESTT. The site permissions are highly restrictive to maintain access integrity. Access to tasks and documents is granted based on item level permissions. Each organization's sub-site will be accessible by members of that organization, but individual tasks and associated artifacts can only be viewed by those within leadership groups, management authority such as ExecSec Managers or Task Managers, and those Subject Matter Experts with assigned responsibility for execution.

Applicable System of Records Notice(s):

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System; and
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).

Retention Period:

Records are retained in accordance with GRS 4.1, item 010.

USCIS Correspondence and Inquiries Tracking Tools

USCIS Executive Secretariat Clearance Action Tracking System (CATS)

The USCIS Office of the Executive Secretariat (EXSO) handles the coordination and agency response to controlled correspondence tasking's from Congress, the Department, other DHS Components, and internal USCIS clearance of policy and operational guidance. To assist in this effort, EXSO developed a Salesforce tracking system, Clearance Action Tracking System (CATS). EXSO creates an official tasking and delivers it to all appropriate USCIS Program Office and Directorates with instructions to draft a response. The appropriate Program Offices and/or Directorates review the official tasking, and upload their response into CATS. After final review by the Office of Chief Counsel, the USCIS Front Office reviews and approves the agency response. EXSO then processes the approved document back to the originating office.

Individuals Impacted:

Federal employees and members of the public

Data Elements:

Information retained from federal employees includes:

- Name;
- Agency/office; and
- Contact information (email, phone, title).

Information collected from the general public includes:

- Names;
- Mailing addresses; and
- Email addresses.

CATS is configured to only collect contact information in order to respond to the correspondence or tasking. If incoming correspondence contains SPII such as Social Security number or A-Number, EXSO does not enter the SPII into CATS. This sensitive information is not used to respond to correspondence by EXSO.

Sources of Information:

The sources of the information are the original incoming correspondence sent by a submitter, and any related correspondence received back from assigned responder. The sources may include the following:

- DHS Headquarters;

- Internal DHS Components;
- The White House;
- The Office of the Vice President;
- Other federal agencies;
- Members of Congress;
- State and local governments;
- Foreign officials or governments;
- U.S. and foreign corporations;
- Non-government organizations; and
- The general public.

Information Sharing:

EXSO typically only shares a response with the original correspondent. In the event EXSO determines a correspondence should be reviewed by an external agency, the correspondence will be shared, as appropriate. If the correspondence contains PII it will be shared in accordance with an approved routine use from the applicable SORN(s).

System Access:

A limited number of individuals within EXSO have access to CATS to send official tasking to offices within the agency. Within USCIS Program Offices and Directorates, only a limited number of individuals have access to CATS to upload and respond to the official tasking on behalf of their office. EXSO frequently updates the USCIS Task Coordinator List to ensure the appropriate individuals within the office receive the taskings.

Applicable System of Records Notice(s):

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System;
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records.

Retention Period:

Records are retained in accordance with GRS 4.1, item 010.

Office of Chief Counsel - Portfolio Management Tool (OCC-PMT)

The USCIS Office of Chief Counsel is responsible for providing legal immigration advice to USCIS Program Offices and Directorates (e.g., Field Operations Directorate (FOD), Service Center Operations (SCOPS), and the Administrative Appeals Office (AAO)) as well as non-immigration issues (typically to USCIS managers and supervisors). OCC also provides legal advice on national security issues as well as issues related to any litigation involving USCIS. In providing legal advice to offices and individuals, OCC Divisions draft written responses (e.g., memorandums, position papers, justifications, proposals) in response to questions posed by other USCIS offices, individuals, and projects. Additionally, OCC gathers documents and drafts materials in response to litigation involving USCIS.

In order to manage attorney cases and workload, OCC developed the OCC-Portfolio Management Tool (OCC-PMT), a Salesforce tool. OCC Attorneys are located across the country and use OCC PMT as the primary location for tracking case work and referencing and sharing information about the case among assigned attorneys. The tool contains the lifecycle of OCC's workload, including the receipt of the case or question posed to OCC by USCIS Program Offices and Directorates, case information received from external entities (e.g., customers, interagency partners, other USCIS agencies), legal review tasks, attorney actions taken, and OCC's response. OCC uses OCC-PMT to track and organize all attorney work products.[22]

As part of the OCC caseload, attorneys may upload and store complete Alien Files (A-Files) into OCC-PMT to assist in providing accurate legal advice to clients and Department of Justice attorneys. Attorneys use the A-File alongside other documentation relevant to litigation that is not included in the A-File (litigation reports, court pleadings, privilege logs for example) as a matter of course. Having all relevant documentation in one system allows the attorneys to review the case/issue in its entirety and provide a response without having to access important pieces of information fragmented across multiple systems hindering coordination.

Individuals Impacted:

Federal employees and members of the public

Data Elements:

Information collected from federal employees includes:

- Employee name;

[22] Work products include materials such as briefs for cases before the USCIS Administrative Appeals Office (AAO) or Department of Justice Board of Immigration Appeals (BIA), draft memos, emails by attorneys developing legal positions for the agency, draft comments on policies from program offices, draft training materials, directives, and legal advice created by OCC. Other information on the site includes USCIS attorney contact information, biographies, and division descriptions.

- Title;
- Email;
- Phone number; and
- Office name and location.

Information collected from the general public may vary, as all forms of PII may be relevant in particular cases. Most often the PII includes:

- Names;
- Dates of birth;
- A-Numbers;
- Relatives' names;
- Addresses;
- Criminal history; and
- Marital history.

Less frequently, a case involving fraudulent use of credit cards could contain driver's license, credit card, or bank account information. As described above, OCC may also upload full A-Files to OCC-PMT. The type of PII included in an A-File may vary depending on the individual's immigration experience.

Sources of Information:

Members of the public and federal employees who are involved in an immigration or non-immigration matter requiring legal review or advice.

Information Sharing:

Should OCC determine external sharing is necessary, OCC will only share correspondence and litigation in accordance with an approved routine use from the applicable SORN(s). Furthermore, although the system itself may contain a large amount of SPII, when providing a response to an office or individual, OCC will only provide the response or position, which typically does not include PII. However, OCCs response may include some court cases and court rulings to provide context into OCC's position.

System Access:

Only OCC employees will have full access to OCC-PMT. OCC is comprised of approximately 250 attorneys and another 30 support staff, over 20 of which are paralegal support. All OCC staff will have access to OCC-PMT. In sensitive cases such as labor and employment,

only attorneys from a particular division will have access to those cases. Not all client documents are specific to a particular case; a substantial portion of OCC's work is on policy issues and regulations, not on particular cases. Some areas of OCC-PMT will have more restrictive permissions such that only subject matter experts working on a particular issue will have access to that library or list—for example, only labor relations attorneys with a need to know would have access to materials posted for collaboration by labor relations attorneys.

Applicable System of Records Notice(s):

- DHS/ALL-017 Department of Homeland Security General Legal Records; and
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records.

Retention Period:

Records are stored for the duration of the preparation of a case as well as through any related litigation which could be from 6 months to 5+ years. Records are deleted from OCC-PMT within 6 months after the final decision has been issued and the OCC case is closed, i.e., after a decision becomes final and is not appealed.

National Benefits Center Processing Workflow Repository (NPWR) - Electronic Mail Management Application (EMMA)

EMMA is a web-based incoming correspondence tracking system that supports case management of cases in which USCIS has correspondence with the applicant. Each incoming piece of correspondence is logged and associated with the benefit requestor's receipt number.[23] It also allows referring cases to Background Check Unit officers for resolution of the correspondence. EMMA provides an application to track incoming correspondence, including the dates received, addressee, A-Number, receipt number, name, form, type of correspondence, delivery tracking number, date of who/where the correspondence was delivered, as well as the person processing the correspondence.

Individuals Impacted:

Members of the public.

Data Elements:

Information collected from the general public can include:

[23] The receipt number is a unique 13-character identifier that USCIS provides for each application or petition it receives. The agency uses it to identify and track its cases. The receipt number consists of three letters—for example, EAC, WAC, LIN, SRC, NBC, MSC, YSC, AAO, or IOE-and 10 numbers.

- Name;
- Receipt number;
- A-Number;
- Mail tracking number associated with correspondence; and
- Responsible party code to which the correspondence was sent.[24]

Sources of Information:

The applicant sends the incoming correspondence to a USCIS Office.

Information Sharing:

EMMA does not share information.

System Access:

Only approved USCIS Service Center Operations (SCOPS) employees with a valid official need-to-know and supervisory approval have access to EMMA. Access rights and privileges are monitored regularly, and individuals' access is revoked once it is identified they do not need the information to perform their official duties.

Applicable System of Records Notice(s):

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records.

Retention Period:

Records are retained in accordance with GRS 4.1, item 010.

OPQ Report Request Process

The Office of Performance and Quality (OPQ) Performance Analysis & External Reporting Branch (PAER) provides quality analysis and reporting products to meet internal and external USCIS timelines in support of the Federal Open Government initiatives. PAERs values are Quality, Collaboration, and Customer Satisfaction. PAER provides accurate and timely responses to ad-hoc USCIS customer requests (e.g., how long it took to process I-539s; what are the most common H1B employers; FY 2016 workload by form type; if a Lawful Permanent Resident card found in a stolen card has a record in a USCIS system or if it is potentially fraudulent) and important recurring reports needed by customers to make timely and mission critical decisions.

[24] A responsible party code is a unique location code assigned to an individual or specific area within a USCIS Field Control Office. It helps locate the exact location of a file within a facility/office.

The OPQ PAER does not have a formal report request management system to track the receipt and response to these requests. OPQ PAER currently receives requests through various mediums, such as phone calls and emails to OPQ senior leadership, which then trickles down to the appropriate USCIS office and subject matter experts. By not having a central repository for requests, the reliability of receiving the request can be questionable and cause delay in meeting the requested deadline.

OPQ created a tracker and dashboard using a SQL server. To alleviate the current request process, PAER developed an OPQ Report Request Form as the primary means to accept customer requests. The request form will have a web-based front end to accept the customer requests feeds into the back-end internal OPQ tracking interface (to be used by OPQ staff only). The request form will eventually be accessible by DHS personnel (employees and contractors). However, for the first release, the form will only be accessible by USCIS employees and contractors and will be included on both USCIS Connect[25] and USCIS SharePoint (Employee Collaboration Network)[26] for employees to access. The customer interface asks pertinent questions relating to the request to help the OPQ personnel facilitate the completion of the request/creation of the requested report and generate the requested report. The intent of these questions is to reduce the amount of back and forth between OPQ and the requestor of contact to the requestor to obtain the desired information (i.e., how often do you want the report, what is the date range of the report, list the data types).

The new tool replaces a former SharePoint ECN tracker. It consists of a front-end tracking form (to be completed by DHS employees and contractors) and a backend dashboard and summary list of requests (to be accessible by only OPQ personnel (employees and contractors)). OPQ supervisors will also have access to a reporting dashboard to generate monthly summary reports needed to report to senior leadership.

This tool automates notifications (i.e., receipt of request, and status updates to the requestor) and automate the flow of managing requests.

Individuals Impacted:

Members of the public and DHS federal employees and contractors.

[25] USCIS Connect is an internal USCIS website for USCIS Program Offices and Directorates to obtain employee resources (e.g., form templates), learn about DHS, USCIS, and specific Program Offices and Directorates. PII is not permitted to be stored on USCIS Connect.

[26] The USCIS ECN is a secure space for USCIS employees to create, manage, and share documents using customizable tools and services to eliminate additional investments in duplicative collaborative technologies. The USCIS ECN supports secure agency-wide collaboration and communication by connecting separate USCIS Program Offices and Directorates located in various geographic areas through the use of a common platform. USCIS ECN contains PII.

Data Elements:

Information collected from federal employees includes:

- Name;
- Email address; and
- Office.

Information collected on the form from members of the public includes:

- Details of the request;
- Date range of the request;
- Fiscal year;
- Form type request is related to;
- Category (country of birth/citizenship, state);
- Data types (e.g., receipt, approvals, denials, pending, cycle time, notice to appear, request for evidence, other);
- Applicant filing type (initial, renewal, extension);
- Report format; and
- File type (e.g., .csv, excel, pdf).

In some cases, employees may submit requests containing SSNs or other specific identifying information so OPQ staff can use it as a personal identifier to locate specific information on an individual and to ensure that they are conducting research on the correct individual.

Sources of Information:

DHS federal employees and contractors.

Information Sharing:

No information is shared.

System Access:

The front-end tracking form is accessible via a shared link or a link found on USCIS Connect and ECN. The form is able to be completed by DHS employees and contractors. The backend dashboard and summary list of requests that is accessible only by OPQ employees and contractors.

Applicable System of Records Notice(s):

- DHS/ALL-016 Correspondence Records.

Retention Period:

Records are retained in accordance with GRS 4.1, item 010.

Documents, Correspondences and Inquiries Tracking LDAs

USCIS created and uses several Locally Developed Applications (LDA)[27] to support the tracking and response to incoming USCIS applications, inquires, status of lawsuits, and correspondences. USCIS offices receive correspondences that require analysis, storage, categorization and response from USCIS office or program. The inquiries can derive from written or electronic correspondences and phone calls, received from the public (applicants, applicant's attorneys or their representatives), community-based organizations, universities, DHS components, or other government or state agencies. USCIS personnel use Microsoft products such as Excel or Access to track all forms, inquiries, or correspondences it receives and respond to the documents in a timely manner.

The information is collected to facilitate efficient, accurate and timely handling of all incoming inquiries. The information is used to provide a record of the form, inquiry or correspondence received, USCIS employee assigned the inquiry, and status of the response to the inquiry.

USCIS offices may receive incoming correspondence via email or mail, fax or phone call from an applicant (or his/her representative), DHS component, or other government agency. Upon receipt, the USCIS employee or contractor manually enters information such as name, A-Number and/or receipt number, and contact information into the LDA. The supervisor then assigns the work to an employee. The incoming documents or response generated are not maintained by or in the LDA. The correspondence that is received and documents generated for a response are ingested in the A-File associated with the applicant. The LDA tracks inquiries, work assignment, and the progress of a response.

The LDA can generate reports such as number of inquiries received; pending workload; employee assigned the workload; type of inquiry; and the status of the inquiry. The reports are used to track the history of the inquiry, time in processing, and quality assurance of inquiry. The LDA reports can be used to identify peak periods in which phone calls are received. The LDA and reports are kept on the shared drive and access restricted to only those employees who have a need

[27] LDA is an application that stores, processes, or transmits USCIS data, but is not currently recognized as an official USCIS system, within the USCIS IT inventory, and has not been brought into Federal Information Security Management Act (FISMA) compliance to meet DHS IT security policies.

to know. The LDA and reports are accessible and used by supervisors for the applicable program area and information according to the applicable retention schedule for the underlying information.

Individuals Impacted:

Members of the public and DHS federal employees and contractors.

Data Elements:

The information the LDAs may collect from the public includes, but is not limited to:

- Name;
- Phone numbers;
- Fax number;
- Email address;
- Date of birth;
- A-Number;
- Alien name;
- Underlying application type;
- Receipt number, and
- Gender.

The information the LDAs may collect from DHS employees includes, but is not limited to:

- Name;
- Title;
- Organization;
- Email address;
- Fax numbers; and
- Phone numbers.

Sources of Information:

The inquiries can derive from written or electronic correspondences and phone calls, received from the public (applicants, applicants' attorneys or their representatives, community-based organizations, universities), DHS components, or other government or state agencies.

Information Sharing:

No information is shared.

System Access:

Only USCIS employees with a need-to-know in the specified USCIS locations within the chart below have access to the respective LDAs.

Applicable System of Records Notice(s):

- DHS/ALL-002 DHS Mailing and Other Lists System;
- DHS/ALL-016 Correspondence Records;
- DHA/ALL-004 General Information Technology Access Account Records System (GITAARS);
- DHS/ALL-017 DHS General Legal Records; and
- USCIS-specific SORNs to cover the response to a specific applicant's correspondence: DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, DHS/USCIS-005 Inter-Country Adoptions Security, DHS-USCIS-007 Benefits Information System, DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, DHS/USCIS–017 Refugee Case Processing and Security Screening Information System of Records.

Retention Period:

Records are retained in accordance with GRS 4.1, item 010.

USCIS Correspondence LDAs:

LDA Name	**USCIS Office**	**Description/Purpose**	**Data Elements**
Attorney Trak	BAL	Application used to track attorney inquiries.	Attorney Address, A-Number, and full name
Electronic Congressional Inquiry Tracker	NYC	Access database used to record customer service inquiry received through their customer service offices. The LDA is no longer used to process congressional inquiries. The data is purged once a year. A customer service inquiry is a request for information submitted	Applicant name, A-Number, type of inquiry, name of inquirer, and contact information or inquirer

		by someone outside the organization and needs a response. Usually a customer service team, office or some other sub-unit of a larger organization is assigned responsibility to review the request for information and determine how best to respond.	
MANUAL REJECT LOG (MRL)	CSC	Provides Division VII/contractors a process that tracks/accounts for petitions/applications that are rejected for any reason (i.e., wrong fee, no signature, missing pages). The CSC receives numerous inquiries from the public as to why they have not received a receipt notice, and this process enables them to respond immediately as opposed to waiting for the package to be returned in the mail.	No PII
CUTS (Congressional Unit Tracking System)	TSC	Microsoft database used to track Ombudsman and Customer Service Inquiries.	Receipt number, Congressional Office, Community Based Organization, and notes fields
Correspondence	NBC	It is used to track correspondence from the applicant.	A-Number, Receipt number, beneficiary/petitioner name, address, attorney name, attorney address
Correspondence LOC	NBC	The database is used for contract team improvement. It provides reporting on correspondence received from applicants. The database calculates a production count that is used to track how much inner filing clerks are doing.	A-Number, Receipt Number and User ID, beneficiary/petitioner name, address, attorney name, attorney address
NWIRP NO Fee Waiver Database	NBC	Record of correspondence received from applicants.	A-Number, Receipt Number, Applicant's Name, DOB, Address
RFE Track.mdb	NBC	Tracks RFE as they come into the building and are interfiled with primary application.	A-Number, Receipt Number

RFE.mdb	NBC	Tracks RFE letters returned from applicants.	A-Number, Receipt Number

Legislative Electronic Tracking System (LETS)

The USCIS Office of Legislative and Intergovernmental Affairs (OLIA) is responsible to providing Members of Congress and their staffs with timely, accurate, and comprehensive information about agency's operations, policies, and procedures. It also provides oral and written responses to congressional inquiries on individual casework and institutional/policy issues regarding immigration benefits processing. In order to perform this mission, OLIA relies on the Legislative Electronic Tracking System (LETS).

USCIS established LETS to support OLIA in its efforts to provide prompt responses to constituent concerns, proactive outreach on issues of interest, and ongoing educational activities for Members and their staff. LETS is a Microsoft (MS) Dynamics CRM web-based electronic system used for enhanced intake, tracking, and reporting of congressional inquiries. LETS is used to establish a consistent mechanism to report on trends and workload, identify duplicates (when constituent asks several Members for assistance as well as historical responses on the same inquiry), allow for transfer of an inquiry from one office to another, facilitate the exchange of information between regional/center leads, increase transparency and consistency, reduce response times, assist with cross jurisdictional inquiries, document responses more completely, meet USCIS privacy release policies, increase data security and integrity, provide consistent system support, and assist with quality reviews.

Individuals Impacted:

Federal employees and members of the public.

Data Elements:

LETS is configured to collect basic contact information about the congressional staff (such as Member of Congress or Committee). LETS collects the following information:

- Congressional staff name;
- Title;
- Phone; and
- Email address.

Additionally. LETS collects the name of the USCIS personnel who created the record, a unique system generated Inquiry number, Inquiry Type, Inquiry Issues and Sub-Issues, Contact

Method, a description of the nature of the inquiry, copies of the privacy release (third party consent form), and other supporting documents, such as such receipt notices from USCIS.

LETS also collects public information about constituents seeking assistance related to an immigration benefit filed or to be filed with USCIS, including:

- Name;
- A-Number;
- Date of birth;
- Receipt number, and
- Other case specific information may be collected.

OLA does not proactively track or record SSNs, but they may be provided by the congressional office. If an inquiry directly involves an individual, USCIS Congressional liaisons require the inquiry to be accompanied by a signed privacy release.

Sources of Information:

Information in LETS originates from incoming correspondences sent by a submitter, and any related correspondence received back from assigned responder. The sources may include, but are not limited to the following:

- Congressional offices and their staff;
- Constituents; and
- USCIS employees.

Information Sharing:

OLA typically only shares a response with congressional offices and constituents. In the event OLA determines a correspondence should be reviewed by an external agency, the correspondence will be shared, as appropriate. If the correspondence contains PII it will be shared in accordance with an approved routine use from the applicable SORN(s).

System Access:

The only individuals who have access to LETS are OLIA employees who have been approved users with a valid official need-to-know and supervisory approval. Access rights and privileges are monitored regularly, and individuals' access is revoked once it is identified they do not need the information to perform their official duties.

Applicable System of Records Notice(s):

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System; and
- DHS/ALL-016 Correspondence Records.

Retention Period:

Information processed in LETS to include documents are kept for a minimum of five years from the date of creation and comply with the Administrative Records Retention Schedule N1-85-91-01.

Salesforce Tracking Activities and Relationships System

The USCIS Office of Privacy serves as both advisor and oversight body for the agency's privacy-sensitive programs and IT systems. The Office of Privacy has primary authority for privacy policy and works to ensure that the use of technology sustains and does not erode privacy protections relating to the collection, use, dissemination, maintenance, and disposal of personal information.

The USCIS Office of Privacy's use of Salesforce Tracking Activities and Relationships System (STARS) was built using the Salesforce Government Cloud. The purpose of the Salesforce Government Cloud is to provide a trusted and secure service to the U.S. government, to quickly and securely deliver applications to meet customers' business needs. The Office of Privacy uses STARS to streamline the workflow of privacy incident management into a platform that provides a robust tracking, reporting, and collaboration platform. STARS allows the Incident Management team to securely store documentation pertaining to incidents and breaches, increase work productivity and automate the incident tracking process. Incidents received through the USCIS Incidents and Breaches Mailbox are captured through STARS using the Chatter functionality, which is a private[28] collaboration tool built into the STARS interface that allows USCIS employees to create private groups and to start and maintain secure communications with users who have a need-to-know and are needed to resolve an incident. STARS allows users to track the status of each incident, flag them for supervisory review, store training certificates and closing remarks, and to manage any other document(s) relevant to an incident. During the mitigation of incidents, STARS may collect personally identifiable information or sensitive personally identifiable information (PII/SPII) about USCIS personnel and members of the public.

[28] Private Chatter means any USCIS employee with access to STARS can find the group, but they **must** ask to join, and only the creator or administrator of the group can grant permission to the secure chat. Only once a user is a member, will they be able to see and send messages.

Individuals Impacted:

- Federal employees, contractors, and members of the public.

Data Elements:

Information about employees and contractors includes, but is not limited to:

- Contact information (name, phone number, email, address, title, and office); and
- Any other type of information that may be part of the evidence submitted to assist with incident mitigation to include human resource related information such as past similar incidents of concern and disciplinary actions.

Information about members of the public includes, but is not limited to:

- Name;
- Date of birth;
- Address;
- A-number;
- Passport number;
- Receipt number;
- Email address;
- Significant incident report number;
- Points of contact;
- Immigration status;
- Any other type of information that may be part of the evidence submitted to assist with incident mitigation. They may include, but not limited to, personally identifiable information, medical information, financial account number, and derogatory information.

While the Incident Management team does not collect or use social security numbers (SSNs), and the STARS application is not configured to collect or store SSNs, this type of personally identifiable information may sometimes be inadvertently included in the documents submitted as evidence for the mitigation of an incident.

Incident reports are retrieved from STARS using the system generated Salesforce service item number and/or Significant Incident Report (SIR) number, and occasionally via a word search.

Sources of Information:

Information in STARS application originates from incoming correspondences sent to the incident management mailbox, and any related correspondence received back from assigned

responder. The sources may include, but are not limited to the following:

- USCIS Command Center;
- USCIS personnel; and
- Members of the public.

Information Sharing:

The Office of Privacy will only share information as appropriate and in accordance with an approved routine use from the applicable system of record notices (SORNs).

System Access:

The only individuals who have access to the STARS application are USCIS personnel within the Office of Privacy who have a need-to-know for the performance of their official duties and with supervisory approval. Access rights and privileges are monitored regularly, and individuals' access is revoked once it is identified they do not need the information to perform their official duties. Some areas of STARS have more restrictive permissions such that only privacy team members working on a particular matter will only have access.

Applicable System of Records Notice(s):

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System;[29]
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);[30]
- DHS/ALL-016 Correspondence Records;[31] and
- Other applicable source system SORNs

Retention Period:

Privacy Incident Records are retained in accordance with the following General Records Schedules: 3.1: General Technology Management Records, 3.2: Information Systems Security Records, 4.2: Information Access and Protection Records, and 4.3: Input Records, Output Records,

[29] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659, November 25, 2008, *available at* https://www.dhs.gov/system-records-notices-sorns.
[30] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, November 27, 2012, *available at* https://www.dhs.gov/system-records-notices-sorns.
[31] *See DHS/ALL-016 Correspondence Records, 83 FR 48645 (September 26, 2018), available at* https://www.dhs.gov/system-records-notices-sorns.

and Electronic Copies as described in section 1.4 of the DHS and Component Network IT Security Operations and Privacy and IT Security Incident Response Privacy Impact Assessment (PIA).[32]

USCIS Board of Immigration Appeals (BIA) Recognition & Accreditation (R&A) Tracker ECN Site

DHS and the Department of Justice (DOJ) receive requests from accreditation/recognition individuals and organizations seeking to represent immigration benefit filers (providing legal assistance/advice, assisting with form completion, accompanying them to interviews, etc.).

Requests are made in the following manner:

1. Organizations seeking to become a recognized organization must submit the DOJ Form Executive Order for Immigration Review (EOIR)-31 to both the BIA and USCIS District Director.

2. Individuals seeking to become an accredited representative must submit a letter to both the BIA and USCIS District Director

The final determination is to recognize or accredit an organization/representative is made by the DOJ's BIA. However, the USCIS District Offices play an essential role in this process by providing a recommendation to the BIA on the individual or organization's suitability.

USCIS Field Operations Directorate tracks the recognition and accreditation requests using the BIA Recognition & Accreditation (R&A) Tracker ECN Site to ensure that a recommendation is provided by the District Director to the BIA within the required timeframe of 30 days.

Individuals Impacted:

Members of the public.

Data Elements:

Information collected from the public to be considered as a recognized organization includes:

- Name of the organization;
- Address of the organization;
- Email address of organization;
- Phone number of organization;
- Type of organization;

[32] See U.S. DEPARTMENT OF HOMELAND SECURITY FOR THE DHS AND COMPONENT NETWORK IT SECURITY OPERATIONS AND PRIVACY AND IT SECURITY INCIDENT RESPONSE, DHS/ALL/PIA-056 (2016) *available at* www.dhs.gov/privacy .

- Signature of authorized official of organization;
- Proof of service indicating that a copy was sent to (1) the local District Director for USCIS, and (2) the local Chief Counsel in charge for ICE; and
- Supplemental information collected include: Organization Charter; Constitution; Articles of Incorporation and/or By-laws; Fee Schedule; a detailed statement regarding the knowledge, information, and experience in immigration and nationality law and procedure available to the organization and a list of library and/or internet resources; Description of the specific immigration legal services the organization provides; Resumes and any immigration training certificates for staff members; Description and/or diagram of the organizational structure of the organization, which shows the supervision of staff members; Whether an accreditation request is being made concurrently, and if so, the name of the proposed representative.

Information collected from the public to be considered an accredited representative includes:

- Letter and Cover Letter;
- Category in which accreditation is being sought;
- Application with Certificate of Service/Proof of Service; and
- Indication that a copy was sent to: (1) the local District Director for USCIS, and (2) the local Chief Counsel in charge for ICE.

Information collected from the public and federal employees to be maintained in the R&A Tracker includes:

- Receiving District Office;
- Organization name;
- Organization city/state;
- Benefit type;
- Application for Recognition;
- Name of representative seeking accreditation;
- Date initially received by USCIS;
- Date received at Field Office;
- Date received at District Office;
- Date request for information sent to Fraud Detection and National Security, USCIS Counsel, and or the Field Office;
- Date of request for extension;

- BIA response to retention request;
- Date recommendation sent to BIA;
- Date the copy of the USCIS Recommendation sent to organization/individual;
- Date of BIA decision and disposition; and
- Comments.

Sources of Information:

Information collected in the tracker consists of a few points of information supplied by the organization or representative on the application form or letter. Additional information includes dates input by USCIS users of important milestones/actions taken on the request (date received, date sent to EOIR)

Information Sharing:

There is no direct connection to the ECN site. However, USCIS shares information with BIA through its recommendation on the individual or organization's suitability to be an accredited organization/representative.

System Access:

Access to the R&A Tracker ECN site is granted on an individual user basis. Each District provides the names of those on its R&A Review team who need access to the ECN to perform required duties.

Applicable System of Records Notice(s):

- DHS/USCIS-007 Benefits Information System.

Retention Period:

USCIS retains a copy of R&A requests for USCIS records according to the EOIR retention schedule, DAA-0582-2017-0001. R&A requests are retained by USCIS for 5 years.

SCOPSSCATA Shared Email Box

The USCIS Service Center Operations Directorate (SCOPS) manages and adjudicates applications and petitions from individuals seeking immigration benefits that do not require in-person processing or interview. SCOPS consist of a Headquarters office and the following five service centers: California Service Center, Nebraska Service Center, Potomac Service Center, Texas Service Center, and Vermont Service Center.

USCIS offers customers multiple avenues for customers to contact USCIS about case-specific questions. To enhance customer service inquires, SCOPS allows customers to email inquiries about a particular case if the customer previously created a Service Request online or called the USCIS Contact Center that was pending 30 days without a response.

All incoming customer inquiries are emailed to the USCIS SCOPSSCATA shared mailbox. HQ SCOPS operates the SCOPSSCATA shared mailbox and appropriately routes each customer email to the respective service center for processing. USCIS replies back to the individual with scripted language. USCIS does not provide customers with case-specific responses through the SCOPSSCATA box. USCIS also removes all sensitive personally identifiable information (SPII) when responding back to the customer.

Individuals Impacted:

Federal employees and members of the public.

Data Elements:

Information collected from federal employees includes:

- Name;
- Agency/office; and
- Contact information (email, phone, title).

Information collected about the general public includes:

- Names;
- Receipt number;
- Form number; and
- Type of immigration benefit being sought for the case about which the person is inquiring.

SCOPSSCATA also collects the USCIS Contact Center inquiry information, including:

- The date the customer contacted the National Customer Service Center (NCSC);
- The service request number that the customer was given;
- If available, the name of the NCSC customer service representative the customer spoke to; and
- A brief explanation if the customer called the NCSC and they informed the customer they were unable to complete a service request.

Customers are specifically advised not to include SPII, such as SSN, or supporting documentation for their case but some may do so. If a customer does include SPII, it is removed before sending the email on for a service center to respond.

Sources of Information:

The sources of the information are the original incoming correspondence sent by a submitter, and any related correspondence received back from the assigned service center. The sources may include the following:

- DHS Headquarters;
- Internal DHS Components;
- Other federal agencies; and
- The general public.

Information Sharing:

USCIS forwards emails to the corresponding Service Center or USCIS subject matter expert for response. USCIS occasionally responds to a request from a member of the public, or an employee of another agency. Responses to the inquiries are emailed back to the same email address from which the customer sent the inquiry.

System Access:

A limited number of individuals within SCOPS have access to the shared email box to forward incoming customer inquiries to the respective service center for processing. Only a limited number of individuals have access to the shared email box to respond to the customer directly if the inquiry does not meet requirements for SCOPS to process it.

Applicable System of Records Notice(s):

- DHS/ALL-016 Correspondence Records.

Retention Period:

Records are retained in accordance with GRS 4.1, item 010.

USCIS Office of Intake and Document Production (OIDP) – Lockbox Management Inquiry System under the System for Tracking Activities, Relationships, & Services (STARS) boundary

The purpose of the Salesforce Government Cloud is to provide a trusted and secure service to USCIS and its customers both internal to the government and external, and to quickly and securely deliver applications to meet USCIS's business needs. Internal and external stakeholders can create business applications by tailoring applications built by salesforce.com (Service Could, Sales Cloud, Chatter) or by building their own custom applications on the Salesforce Platform.

The USCIS Intake Operation Division (IOD) of the Office Intake and Document Production (OIDP) manages the lockbox operations provided by the Department of Treasury's Financial Agency, JP Morgan (Lockboxes).

The lockboxes are operated by Case Resolution Analysts, who are federal employees within the USCIS Office Intake and Document Production (OIDP). The lockboxes and USCIS are responsible for intake processing which entails the collection of the following: data entry of applications, petitions and requests, determining whether to accept or reject forms, depositing fees, sending receipt or reject notices, physically assembling cases in accordance with the business requirements, sending the files to the appropriate USCIS offices, and transmitting the electronic data to the appropriate USCIS offices.

When questions or issues related to the intake process arises, applicants or their representatives may send inquiries via email to lockboxsupport@uscis.dhs.gov. The team of Intake Operation Division (IOD) analysts perform the appropriate research and provide responses via e-mail using Microsoft Outlook per the established internal guidance.

The Office of Intake and Document Production (OIDP) is currently using the System for Tracking Activities, Relationships, & Services, (STARS) to track and respond to correspondences sent to the Lockbox e-mail address from applicants or their representatives regarding questions and/or status of applications submitted to the Lockboxes (IOD) uses the information provided by applicants or their representatives to verify the identity of the applicant and/or their representatives. Intake Operation Division (IOD) does not provide any PII in response to inquiries. Only the application intake status and/or the established internal guidance within the lockbox scope is provided. If an inquiry is regarding actions that occur post intake, the inquirer will be directed to contact the USCIS Contact Centers or a Service Center, as appropriate. The Lockbox Management Inquiry System is allowing the Intake Operation Division (IOD) team to automate the current processes, to boost work productivity, improve tracking, and facilitate effective group collaboration.

Using this new tool, correspondence received through the Lockbox Mailbox will be routed through the System for Tracking Activities, Relationships, & Services (STARS) Chatter functionality which allows analysts to easily assign inquiries or service items, create a space for group collaboration and supervisor review without having to email documents through Outlook. Within the Lockbox Management Inquiry System, the analyst may manually perform a Person Centric Query System (PCQS)[33] query using A-Number/ ELIS Account ID USCIS Receipt Number or a combination of First Name/Last Name/Date of birth to validate the identity of the applicant in question. The Person Centric Query System (PCQS) information available to the analyst is "read only." Once identified, the analyst may link the applicant to the Service Item within Lockbox Management Inquiry System. No additional information from Person Centric Query System (PCQS)[34] is stored within Lockbox Management Inquiry System.

[33] *See* DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR PERSON CENTRIC QUERY SYSTEM (DHS/USCIS/PIA-010), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[34] Person Centric Query System (PCQS) is used to validate the information received within the inquiry.

Individuals Impacted:

- DHS Employees/Contractors, Members of the public, U.S. Persons (U.S citizens or lawful permanent residents) and non-U.S. Persons., to include but not limited to representatives, interpreters, preparers, or any other individual who has submitted an inquiry.

Data Elements:

Personally Identifiable Information relating to an applicant that may be captured from emails/inquiries submitted by applicants or their representatives include, but is not limited to:

- Sender's name
- Applicants' names
- Date of birth
- Alien Number
- USCIS Electronic Information System (ELIS) Identification Number
- Social Security Number (SSN) (Note: this is not solicited, but may occasionally be provided by the individual)[35]
- Address
- USCIS Receipt Number
- Email address
- Phone number
- Financial information, account, and routing numbers – may be solicited on rare occasions.
- Photographic facial images such as a copy of a Legal Permanent Residence card, a Driver's License, or Passport.[36]

Information about USCIS employee or contractors – referred to here as users:

- Name
- Work e-mail address
- Activity log of the analyst's (customer service individual) action related to the inquiry.

Sources of Information:

- Information in the Lockbox Management Inquiry System originates from incoming correspondences via email to the lockboxsupport@uscis.dhs.gov.

Information Sharing:

[35] For additional information, please visit https://www.uscis.gov/about-us/contact-us
[36] For additional information, please visit https://www.uscis.gov/about-us/contact-us

The Office of Intake and Document Production (OIDP) – Lockbox Management Inquiry System will only be shared to respond to the incoming inquiry and in accordance with an approved routine use from the applicable SORN(s). Any PII information received in an inquiry will be removed from the response.

STARS only has "read only" access to the Person Centric Query System (PCQS) to identify and validate the applicant.

System Access:

Lockbox Management Inquiry System users only have read only access to the Person Centric Query System (PCQS) to identify the applicant. SSNs are not requested from applicants or their representatives through this process. However, if an individual provides his or her SSN unprompted within the free text form fields when submitting their message to the Lockbox, the Lockbox Management Inquiry System would not use the SSN to identify the individual in the Person Centric Query System.

The only individuals who have access to the Lockbox Management Inquiry System are Office of Intake and Document Production (OIDP) USCIS Federal employees within the Intake Operations Division (IOD) who have a need-to-know for the performance of their official duties and supervisory approval. Access rights and privileges are monitored regularly and individuals' access is revoked once it is identified they do not need the information to perform their official duties. Some areas of the Lockbox Management Inquiry System have more restrictive permissions such that only limited Intake Operations Division (IOD) team members, working on a particular matter, will have access to. Authorized individuals access the Lockbox Management Inquiry System via a network-level single-sign-on process using multi-factor authentication only.

Applicable System of Records Notice(s):

- Department of Homeland Security (DHS) Mailing and Other Lists System[37]
- General Information Technology Access Account Records System (GITAARS)[38]
- Department of Homeland Security Claims Records[39]
- Alien File, Index, and National File Tracking System[40]
- Benefits Information System[41]

[37] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659, November 25, 2008, *available at* https://www.dhs.gov/system-records-notices-sorns.
[38] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, November 27, 2012, *available at* https://www.dhs.gov/system-records-notices-sorns.
[39] *See* DHS/ALL-013 Department of Homeland Security Claims Records, 73 Fed. Reg. 63987 (October 28, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[40] *See* DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program System of Records, 85 Fed. Reg. 31798 (May 27, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[41] *See* DHS/USCIS-007 Benefits Information System, 81 Fed. Reg. 72069 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Correspondence Records[42]

Retention Period:

The records in System for Tracking Activities, Relationships, & Services (STARS) are currently retained indefinitely in absence of an approved records retention schedule. The System for Tracking Activities, Relationships, & Services (STARS) currently does not have an approved National Archives and Records Administration (NARA) records retention schedule. However, the records will be maintained as "permanent" until a schedule is created. The System for Tracking Activities, Relationships, & Services (STARS) team will coordinate with USCIS Local Records Information Managers (LRIM), DHS Records Management, and the National Archives and Records Administration to gain approval for a records retention schedule. Once the appropriate retention schedule is developed and finalized, the System for Tracking Activities, Relationships, & Services (STARS) team will ensure that the requirements are followed.

[42] *See DHS/ALL-016 Correspondence Records, 83 FR 48645* (September 26, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.