



# Privacy Impact Assessment

for the

## USCIS Enterprise Collaboration Network

**DHS Reference No. DHS/USCIS/PIA-083**

**July 6, 2020**



**Homeland  
Security**



## Abstract

The U.S. Department of Homeland Security (DHS), U.S. Citizenship and Immigration (USCIS) uses SharePoint-as-a-Service (SharePoint), commonly referred to throughout the agency as the Enterprise Collaboration Network (ECN), a web browser-based collaboration and document management platform from Microsoft. 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 is conducting this Privacy Impact Assessment (PIA) to assess the privacy risks to the personally identifiable information (PII) collected, used, maintained, and disseminated on the USCIS ECN.

## Introduction

USCIS oversees lawful immigration to the United States. USCIS provides accurate and useful information to its customers, grants immigration and citizenship benefits, promotes an awareness and understanding of citizenship, and ensures the integrity of the immigration system. With over 19,000 government employees and contractors located at over 200 offices domestically and internationally, USCIS must be able to effectively manage information and workflows, including the receipt, creation, distribution, tracking, and archiving of tasks, assignments, inquiries, and other correspondence or data. The USCIS ECN provides a collaborative environment for USCIS personnel located in various offices and multiple geographic locations, to engage and act as partners working toward a common mission.

USCIS historically relied on the shared drive, personal drives, and emails to meet its mission needs. While these tools offer a number of advantages, there are significant pitfalls to effectively and efficiently managing and sharing documents. Generally, the use of these tools causes duplicate and redundant documents, inaccessibility to information, lack of document governance and control, and hinders cross-collaboration. To streamline information sharing, document management, communication, and collaboration across USCIS domestic and international offices, USCIS implemented the USCIS ECN. USCIS ECN is built using SharePoint, which is a document management and collaboration tool developed by Microsoft.

SharePoint is a commercial off-the-shelf (COTS) cloud-based application that provides a platform on which to build custom applications and features a suite of collaboration, document management, and communication tools, as well as a high degree of integration with other Microsoft Office products. SharePoint automates the matter tracking process, eliminating or reducing the need to manually track emails and manage paper-based documents and forms, and promotes a more efficient means of sharing, storing, searching, and reporting on agency



information. Used as a matter tracking tool, the SharePoint platform enables secure data entry, standardizes the display of information, and supports data management and analysis by USCIS personnel.

## **USCIS ECN Functions and Capabilities**

ECN is a cloud-based platform that improves USCIS' effectiveness by streamlining the management of and access to data. Although USCIS primarily uses ECN as a document repository, SharePoint offers additional capabilities and enhanced functionality. The following provides a general description of USCIS' use of ECN:

- **Forms management:** Users can create customized forms within ECN so that the information gathered in the form can be stored in a list or library for organization and analysis of data. These forms can access and display data from multiple sources to aid in the collaboration and organization of information.
- **Records management:** ECN provides a method for systems to automatically archive or expire content based on criteria set forth by the site administrator. For example, a system could delete items from a list if the items are labeled as "Status = Closed" and the items are greater than three years old. Similarly, ECN can move items to a separate archive list when they are better suited for long term retention.
- **Reporting capabilities:** A suite of reporting tools offers reporting and business intelligence solutions while eliminating the need for writing custom code. These tools can be used on specific SharePoint systems so that users can run regular or ad hoc reports that suit their business needs. For example, reporting through SharePoint can be used to manage employee workloads, manage budgets, align resources with operational needs, or perform other trend-based or statistical reporting.
- **Survey capabilities:** SharePoint allows individuals to create surveys and polls and contains recruitment features, such as the ability to email a link to prospective survey participants. Surveys are an efficient and cost-effective way to collect information and experiences from a large number of participants. Surveys are particularly useful for collecting and processing quantifiable data because they generally contain closed-ended questions that allow USCIS to more easily compare responses.
- **Auditing capabilities:** SharePoint automatically stores information on the identity of system users and logs the actions users take while navigating throughout the environment. Tools such as version history can be used on SharePoint pages, lists, or libraries to determine whether any changes were made, which user made the changes, or when the user made the changes.
- **Microsoft Office integration:** SharePoint ties in closely with Microsoft Office products in



an effort to bring some of the native capabilities of certain Microsoft Office products into SharePoint sites and pages. For example, Excel provides the ability to present data from an Excel spreadsheet on a SharePoint page or leverage Excel data in a SharePoint list for configuring the data. This functionality can also help to present charts and graphs from Excel in SharePoint which are automatically updated based on data changes that are made in real time.

## **USCIS Users and Structure**

USCIS is divided into Directorates and Program Offices.<sup>1</sup> Each Directorate and Program Office maintains its own ECN site for their data collection, use, and dissemination, as well as possible sub-sites for specific mission needs. Sites and sub-sites are managed by a site administrator who is responsible for overseeing his or her respective ECN sites, including confirming that any additional site facilitators are regularly maintaining, updating, and monitoring both content and user access to their Directorate or Program Office site.

Access control of sites and specific content areas such as ECN lists and libraries is achieved using SharePoint group security and the SharePoint targeted audience feature. This enables access control over any content on a need-to-know basis. Users must be members of a group assigned to the site. All libraries have unique permissions, and access to libraries is through a smaller subset of groups allowed on the parent website.

USCIS is conducting this PIA to provide transparency on the agency's use of ECN as a document management tool, address its capabilities, and identify the broad categories of information that may be maintained, the sources from which information is collected or derived, and the safeguards implemented to mitigate privacy risks. In addition, this PIA uses the Fair Information Practice Principles (FIPPs) to evaluate ECN's privacy risks. The body of this PIA will provide a high-level overview of USCIS' overall use of ECN, while the appendices to this PIA describe the specific USCIS Directorate and Program Office ECN purpose and uses, types of data maintained, access controls, categories of individuals, sources of information, records retention, and System of Records Notice (SORN) coverage for each individual USCIS Directorate and Program Office. USCIS plans to update the appendices as new site or uses are deployed or as changes to current sites take place.

## **Governance**

USCIS Directorate or Program Offices are permitted to collect, use, store, and share both PII and Sensitive PII (SPII) on ECN sites. However, prior to using any SPII on an ECN site, Directorate and Program Offices are required to (1) provide a record of the activity and its privacy requirements, (2) demonstrate compliance with privacy laws and regulations, and (3)

---

<sup>1</sup> For more information, see <https://www.uscis.gov/about-us/directorates-and-program-offices>.



document the inclusion of privacy considerations. This is generally done through the Privacy Threshold Analysis (PTA) process, and each PTA is required to include the following details:

- The purpose for which the Directorate or Program Office is using ECN and how it benefits USCIS business processes;
- The types of documents/information stored in the document library;
- Itemized categories of information that are collected, used, stored, and shared;
- Derivation of information (e.g., source systems, social media, external agency);
- Uses of information;
- Access rights and limitations; and
- Site administrator oversight responsibilities.

USCIS tracks and maintains an internal inventory of all collaboration sites that store S/PII and ensures that visual cues are included on each site to denote which sites are authorized to maintain SPII and which are not.

In addition to the PTA process, Directorates and Program Office site facilitators are responsible for completing SharePoint training. Prior to using any USCIS system, individuals are responsible for signing the USCIS Rules of Behavior, which indicates the employee has read, understands, and acknowledges the rules of behavior while engaging with USCIS systems and will comply with the guidelines. Employees cannot access restricted ECN sites without first completing the rules of behavior. Once the site facilitator reviews the request and obtains supervisory verification that the employee has a valid need-to-know, the individual is then granted access to the requested site.

### **Categories of Information**

USCIS ECN supports a variety of business functions in broad mission areas that may include:

- Adjudications;
- Administrative and Mission Support;
- Community Relations;
- Legislative Affairs;
- Fraud Detection and National Security;
- Production Planning and Reporting;
- Quality Management and Assurance; and



- Records Management.

Any USCIS ECN site may include a variety of information about USCIS or DHS personnel, contractors, and members of the public. This PIA covers different types PII, including employee and contractor human resource and contact information, as well as SPII, such as Social Security numbers (SSN), Alien Registration Numbers (A-Number), immigration information, criminal history information, medical information, and financial data. USCIS ECN is not authorized to collect, store, or maintain classified information. The specific information collected and maintained depends on the nature and business process of the particular activity, project, or program that the ECN is being used to support. The appendices to this PIA describe the collection, use, and maintenance of PII by different USCIS Directorates and Program Offices.

All sites approved to maintain PII and SPII will be identified through a Warning Banner. This banner provides visual notification of SPII storage approval in a red banner at the top of the page. This applies to each page that contains SPII and not just the site.

## **Sources**

Information contained within ECN is obtained from various sources. Similar to the variances in categories of information, sources of information depend on the nature and business process of the particular activity, project, or program for which the site is used. Information may be collected directly from the individual or third parties, or derived from other sources (e.g., other paper-based or electronic systems). Other sources of information include other USCIS Directorates and Program Offices; DHS Headquarters and Components; state, local, and foreign government agencies; Congress; the White House; nongovernmental organizations; and members of the public. Please refer to Directorate and Program Office appendices of this PIA for specific sources of information.

## **Retention and Removal of Content**

Records retention and disposition in ECN varies by the type of record collected. All current records retention schedules requirements are being maintained, as required by the National Archives and Records Administration (NARA). ECN provides a method for systems to automatically archive or expire content based on criteria set forth by the business owner. Files are also purged by the site owner and site facilitators as they age, in keeping with existing required retention schedules, as well as when no longer needed. Please refer to Directorate and Program Office appendices of this PIA for specific retention periods.



## Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974<sup>2</sup> articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.<sup>3</sup>

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.<sup>4</sup> The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208<sup>5</sup> and the Homeland Security Act of 2002, Section 222.<sup>6</sup> Given the particular technology and the scope and nature of its use, USCIS conducted this PIA, within the construct of the FIPPs, to address the privacy risks associated with USCIS ECN.

### 1. Principle of Transparency

*Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.*

The type of information maintained on USCIS ECN varies by the particular business need established by each Directorate or Program Office. In most cases, USCIS ECN is used to collect, maintain, and disseminate information in support of existing programs and processes. ECN sites serve various purposes including adjudicative, human resource, or financial management purposes and may include information about both USCIS employees and members of the public. Many of the uses of existing programs and processes are covered under previously published privacy compliance documentation that can be found at [www.dhs.gov/privacy](http://www.dhs.gov/privacy). Additional notice about USCIS' use of ECN is provided to the public through this PIA. The underlying SORNs for Program Offices and Directorates provide further notice.

---

<sup>2</sup> 5 U.S.C. § 552a.

<sup>3</sup> 6 U.S.C. § 142(a)(2).

<sup>4</sup> See Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," available at <https://www.dhs.gov/privacy-policy-guidance>.

<sup>5</sup> 44 U.S.C. § 3501 note.

<sup>6</sup> 6 U.S.C. § 142.



There is no significant privacy risk associated with notice. While individuals may not know that their information is being maintained in USCIS ECN, the information collected is already being used as part of existing programs and processes. USCIS ECN allows for the ability to collaborate and manage the business process more efficiently. Specific notice of USCIS ECN is provided through the publication of this PIA.

## 2. Principle of Individual Participation

*Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

The USCIS ECN does not collect information directly from the public. The Directorate or Program Office collecting the information may provide the individual with the opportunity to either consent, decline to provide information, or opt out through other established means and processes. In certain circumstances, a Directorate or Program Office may create a form on ECN to collect information directly from USCIS employees and contractors. This information is generally collected only for Human Resources purposes.

An individual may gain access to his or her USCIS records by filing a Privacy Act or Freedom of Information (FOIA) request. Only U.S. citizens, lawful permanent residents, and individuals covered by the Judicial Redress Act of 2015 (JRA) may file a Privacy Act request.<sup>7</sup> Any person, regardless of immigration status, may file a FOIA request. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS record, he or she may mail the request to the following address:

National Records Center  
FOIA/Privacy Act Program  
P. O. Box 648010  
Lee's Summit, MO 64064-8010

Additional information about Privacy Act/FOIA requests for USCIS records is available at <https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia>.

There is no privacy risk associated with individual participation. Individuals may access or amend their information by filing a Privacy Act/FOIA request.

---

<sup>7</sup> The Judicial Redress Act of 2015, 5 U.S.C. § 552a note, extends certain rights of judicial redress under the Privacy Act to citizens of certain foreign countries or regional economic organizations; more information is available at <https://www.justice.gov/opcl/judicial-redress-act-2015>.



### 3. Principle of Purpose Specification

*Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

USCIS uses ECN to track, manage, review, and report on matters related to its mission and statutory requirements. The specific purpose of an ECN site and the use of the information maintained within depends on the nature of the Directorate or Program Office and the business process for which the site is established. During the PTA process, Program Offices and Directorates are required to specify their particular uses of ECN sites for the USCIS Office of Privacy to verify that the uses are consistent with the relevant PIAs and SORNs. Additional coverage beyond this PIA may be determined. PIA and SORN coverage for the collection and use of the information is validated by the DHS Privacy Office through the adjudication of a PTA.

**Privacy Risk:** There is a risk that information collected, maintained, and used on a USCIS ECN site may be used for purposes beyond supporting the USCIS mission.

**Mitigation:** This risk is mitigated. USCIS Office of Privacy requires the completion and submission of a PTA prior to collecting, using, and storing any SPII on ECN. During the PTA process, the site is evaluated to ensure the purpose of the site is compatible with the USCIS mission.

USCIS Office of Privacy has also established a partnership with the USCIS Office of Information Technology (OIT) ECN Support Team, who is responsible for enforcing the overall SharePoint governance. The OIT ECN Support Team developed a governance plan that outlines the policies and procedures used to ensure that the USCIS SharePoint environments provide a consistently robust, stable working environment for its entire end user population. Both the OIT ECN Support Team and the USCIS Office of Privacy Compliance Branch have global access to the ECN sites. If the ECN Support Team identifies that a site or subsite is out of compliance (e.g., contains SPII but does not contain the banner) the ECN Support Team will notify the site facilitator of the violation and shut the ECN page down until the site becomes compliant (e.g., applies the banner and completes the appropriate privacy compliance documentation). The ECN Support Team will also notify the Office of Privacy, who will access the site and determine whether a PTA exists. If a PTA does not exist, the USCIS Office of Privacy will work with the Directorate or Program Office to complete the documentation.

Furthermore, proper safeguards, including need-to-know and access restrictions, are implemented in coordination with the site administrator to deter the unauthorized use and dissemination of information beyond its official purpose.



## 4. Principle of Data Minimization

*Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

USCIS ECN provides a secure platform for more sophisticated access controls to the data contained within the systems. USCIS ECN includes access controls specific to each Directorate and Program Office site, depending on the business process for which the system is created and the sensitivity of the information stored within it. These controls are placed on the system as a whole, as well as specific files and items contained in the system so that only users with a need-to-know have access to the data. Alternative methods, such as email or shared drive-based solutions or other more rudimentary database management systems, do not typically provide such controls.

For example, USCIS Fraud Detection National Security Directorate (FDNS) uses ECN to manage internal policy and operational documents, content, and reports.<sup>8</sup> In the course of the FDNS mission, FDNS is responsible for handling large amounts of PII while processing immigration inquiries, investigative referrals, law enforcement requests, background checks, and case determinations. Due to the sensitive nature of information that FDNS handles, the FDNS site facilitator in coordination with the site owners is responsible for ensuring that only the minimum information necessary is collected, used, and stored on the FDNS ECN sites. The types of information collected, stored, and used are documented in the PTA.

Retention of data in the USCIS ECN environment is consistent with the approved retention schedule for the original data collection. ECN is an extension of the systems already identified in a SORN, and therefore the retention schedules applicable to the SORN apply to particular IT system holding the data, in this case a particular ECN site. In the case of FDNS, it was determined that a 15-year retention period was adequate to provide FDNS with access to information that is critical to an investigation of fraud, criminal activity, egregious public safety, and national security concerns. Users will follow the established data retention guidelines that govern existing processes.

---

<sup>8</sup>See DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate, *available at* <https://www.dhs.gov/uscis-pias-and-sorns>.



## 5. Principle of Use Limitation

*Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

USCIS uses ECN to further support the USCIS immigration benefits mission. The specific purpose of each Directorate and Program Office site is defined prior to the creation of the site based on each unique business need and purpose. USCIS site administrators and facilitators are responsible for determining the site requirements and user base and, once the site is created, ensuring that it is used only for approved purposes. USCIS ECN enables site administrators and facilitators to use built-in tools to provide more granular access controls than what was previously available via email and shared drives. In addition, the use of ECN limits the proliferation of data. ECN allows for data consolidation and eliminates or reduces the need for USCIS Directorates and Program Offices to retain both paper and electronic copies of documents or multiple electronic copies in more rudimentary database management systems.

Direct access to ECN is not available to external entities, and data stored in the systems is not directly accessible by users or computer systems outside of the USCIS network. Any external sharing of information contained within a USCIS ECN site is made pursuant to the Privacy Act (5 U.S.C. Section 552a(b)).

## 6. Principle of Data Quality and Integrity

*Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

Information that is collected and stored on USCIS ECN is generally not systematically checked for accuracy and timeliness. The USCIS employee or contractor entering the information into the ECN site is initially responsible for the accuracy of information. In general, the site administrator or users have the responsibility of reviewing information maintained on the ECN site to ensure the uses are consistent and complies with mission-related initiatives. Directorates and Program Offices may take appropriate actions to ensure the information is accurate, relevant, timely, and complete, within the context of each use of the ECN site.

**Privacy Risk:** There is a risk that USCIS ECN may contain inaccurate information that is used as part of the adjudication process.

**Mitigation:** USCIS works to mitigate this risk in several ways. USCIS does not rely on information found on USCIS ECN to make a determination as to whether or not an individual is eligible for an immigration request. USCIS ECN is used as a collaboration tool that is used in support of the adjudicative process. USCIS takes into account the totality of an immigration requestor's information prior to granting or denying an immigration request. This includes



information provided by the immigration requestor and information found in DHS and other government databases. USCIS adjudicative personnel relies on the information found in the authoritative source system in order to grant or deny an immigration request.

## 7. Principle of Security

*Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

USCIS ECN is available for USCIS personnel except under limited circumstances. USCIS may extend limited access rights to certain DHS users for a particular use as outlined in the Appendices. Users must have access to the USCIS network to gain access to ECN. Only authorized users with a valid need-to-know who are required to perform the stated purpose of the specific site will be granted rights to access and post data on the site. Users are trained on how to use ECNs access controls, on a group or user-level, to systems, document libraries, and specific documents and items.

USCIS personnel can gain access to a USCIS PII-restricted ECN site only after a site administrator approves a particular user's access. The site administrator allows members of USCIS organizational entities to gain a higher level of permissions to ECN upon successful completion of an exam and adherence to posted guidelines and rules of conduct. Site facilitators and administrators have additional permissions that allow them to make data and user-based modifications to a specific site they have been granted permission to manage. The USCIS OIT ECN team keeps records of all site administrator nominations as well as where these individuals have increased levels of permissions within the environment. The specific Directorate and Program Office access controls are described in further detail in the appendices to this PIA.

In the event of a data incident—including misuse of data, unauthorized access to a SharePoint application, unauthorized posting of PII, and inappropriate disclosure of PII from a site—the incident will be reported and handled as a Privacy incident.

## 8. Principle of Accountability and Auditing

*Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

USCIS ECN automatically stores information on the identity of system users and logs the actions users take while navigating through the environment. Tools, such as version history, provide visibility into where, when, and by whom changes are made in ECN pages, lists, and libraries. If more in depth tracing is necessary, the USCIS ECN teams can reference the detailed audit log files to determine when and who performed the specific actions in question within



ECN.

Furthermore, all USCIS employees and contractors are required to take annual Privacy Awareness training, to reinforce the Privacy principles and remind staff of their responsibilities as data stewards for the public.

## **Responsible Officials**

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

## **Approval Signature**

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

---

Dena Kozanas  
Chief Privacy Officer  
U.S. Department of Homeland Security  
(202) 343-1747



## ECN APPENDICES

### Appendix A – National Records Center

#### Program/System:

USCIS, Immigration Records and Identity Services (IRIS), National Records Center (NRC)

#### Purpose and Use:

The NRC provides stakeholders with access to requested immigration records and information. The NRC oversees the storage, management, and integrity of 74 million immigration files and 18 million receipt files while supporting the largest Freedom of Information Act (FOIA) program in the federal government. The NRC provides support to USCIS, U.S. Customs Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and other government agencies to assist with requests for immigration files.

The NRC leverages the ECN site as a business tool for document and project management, and reporting dashboards. Some pages enable users to perform functions such as approve documents, complete and submit forms, post announcements, and add calendar events. The NRC uses the ECN site to streamline the information sharing internally across branches and externally to other USCIS service centers. The NRC ECN site provides effective communication among NRC branches and service centers allowing for a singular copy of the information and access on a need-to-know basis. The NRC's goal is to allow for knowledge management and sharing in a most useful and accessible format.

The NRC consists of five Branches:

1. Immigration Records Contract Management Section (IRCMS)(RMOB)
2. Management Branch (MBR)
3. Freedom of Information Act (FOIA)
4. Information Management Liaison Section (IMLS)
5. Program Management Operations (PMO)

Each Branch has a page on the NRC ECN site dedicated to information sharing specific to their branch. Each Branch is responsible for maintaining the information placed on their ECN page and ensuring the information is accurate and does not contain PII, unless specifically authorized.

#### Immigration Records Contract Management Section (IRCMS)

The IRCMS is responsible for providing contract oversight for the records operations contractor. The contract includes oversight at the NRC and the Harrisonburg File Storage Facility (HBG). The IRCMS uses the ECN site to facilitate the sharing of data between the two facilities and the other NRC divisions. The IRCMS also uses the ECN site for team discussions



and “Lunch and Learn” presentations.

### *Data Elements and Individuals Impacted*

- The IRCMS ECN site collects the following information about federal employees and contractors: name, work phone number, USCIS email address, and user ID.

### *SORN(s)*

- OPM/GOVT-1 General Personnel Records, which covers general Federal employee records.
- DHS/ALL-003 Department of Homeland Security General Training Records, which covers training records for both Federal employees and contractors.
- DHS/ALL-021 Department of Homeland Security Contractors and Consultants, which covers contractor information.

### Management Branch (MBR)

The MBR is responsible for personnel functions, facilities management, and logistics. The MBR uses the ECN site to collaborate with NRC Executive staff regarding the number of MBR requests. These requests consist of IRIS tracking issues, Executive Section Tasking, and NRC Branches. The MBR uses its ECN page to streamline information sharing internally across all branches. The MBR page also contains links to OPM website resources to assist employees with access to personnel information and benefits.

There are two pages within MBR’s ECN section that collect PII. The MBR is responsible for parking at the NRC facilities, and the Vehicle Module is used to track and streamline the analysis of changes in personnel vehicle parking. The other page is the Visitor Request Form, which is accessible by all USCIS employees. Employees use this page for visitor entry approval into the NRC. The PII input by USCIS employees is only accessible to MBR staff. PII is secured and has the required header information clearly marking the site and describing the type of information allowed on it.

### *Data Elements and Individuals Impacted*

- The MBR ECN site collects the following information about the public: visitor name, company/affiliation, vehicle model, license plate number, year, color, phone number, visitor status (escorted/unescorted), and the visitor adjudication outcome.
- The MBR ECN site also collects the following information about federal employees: name, title, type of request, desk location, desk phone number and extension, USCIS email address, supervisor’s name, entrance on duty date, grade,



photograph, license plate number, make, model, year, color, home address, home telephone number, emergency contact name, and phone number.

- In addition, the MBR ECN site collects the following information about contractors: name, title, USCIS email address, supervisor's name, photograph, license plate number, make, model, year, and color.

#### *SORN(s)*

- DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, which covers records associated with DHS facility and perimeter access control, as well as visitor security and management.

#### Freedom of Information Act (FOIA) Branch

The mission of the FOIA Branch is to provide public access to agency records in accordance with FOIA and the Privacy Act of 1974. The FOIA Branch uses the ECN site to collaborate with Headquarters staff regarding the number of FOIA requests. Using the NRC ECN site allows staff to not only meet the short deadlines, but also to track the Director's performance goals for the NRC. The FOIA ECN page is separated into different pages for each operational unit within the FOIA branch: (1) FOIA Processing; (2) Significant Interest Group (SIG); and (3) Quality Assurance and Customer Service (QA/CS).

#### *FOIA Processing*

The FOIA Processing Unit processes all A-File related FOIA requests. The use of the ECN assists in processing FOIA and Privacy Act requests by providing exemption explanations, final action letter templates, examples of the information withheld, samples of documents with redactions, and flowcharts/diagrams. Under the FOIA Reference Links on the ECN there are useful resources such as the Processing Guide, the FOIA/Privacy Act Assistant's Guide, and other FOIA/Privacy Act training materials.

#### *Data Elements and Individuals Impacted*

- PII is not stored on the FOIA Processing Unit's section of the FOIA Branch's ECN page. Other resources on the FOIA ECN page include hoteling cubicle reservations, calendars, and announcements.

#### *SORN(s)*

- No PII is stored on this section of the page and so no SORN is required.

#### *Significant Interest Group (SIG)*

SIG processes all non-A-File FOIA requests, such as procedural manuals, employment selections, training manuals, and contracts. SIG has a PII-approved page under the FOIA ECN



page. All SIG cases are updated using a spreadsheet log called the Component Backlog Report. Access to this page is controlled by the SIG ECN administrator and the page contains the appropriate banners and notices.

### *Data Elements and Individuals Impacted*

- The SIG ECN site collects the following information about the public: name, date of birth, address, country of birth, Alien number, receipt numbers, temporary file numbers, immigrant status, application/petition type, parents names, Social Security number (or other number originated by a government that specifically identifies an individual), photographic Identifiers (e.g., photograph image, x-rays, and video tapes), driver's license, biometric identifiers (e.g., fingerprint and voiceprint), mother's maiden name, vehicle identifiers (e.g., license plates), phone numbers (e.g., phone, fax, and cell), certificates (e.g., birth, death, and marriage), legal documents or notes (e.g., divorce decree, criminal records, or other), email address, education records, financial records.
- The SIG ECN site collects the following information about federal employees and contractors: name, work phone number, USCIS email address, and user ID.

### *SORN(s)*

- DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, which covers records about Freedom of Information Act and Privacy Act requests and appeals submitted to the Department.

### *Quality Assurance and Customer Service (QA/CS)*

The QA/CS Unit is responsible for doing trend analysis for FOIA processing functions. They also develop and deliver training to FOIA personnel related to their position functions. The QA/CS Unit maintains PII on its ECN page. This page will store three databases that contain PII: (1) FOIA QA Case Auditing Database; (2) Case Create QA Auditing Database, and (3) FOIA Support Team Database.

The QA/CS Unit maintains a FOIA QA Case Auditing database and a Case Create QA Auditing database to keep track of processed cases that are audited for gathering statistical data for trend analysis reports that are provided to management. The QA/CS Unit also maintains the FOIA Support Team database to track FOIA staffing to identify training needs related to staffing for files. These databases are access controlled on a "need-to-know" by the site administrator based on the section supervisor's request. The page displays the appropriate PII banners. Other reference materials currently stored on the QA/CS ECN page are court decisions, policy manuals, links to USCIS systems, and FOIA bulletins.



### *Data Elements and Individuals Impacted*

- The QA/CS ECN site collects the following information about federal employees and contractors: name, work phone number, USCIS email address, and user ID.

### *SORN(s)*

- DHS/ALL-001 Department of Homeland Security (DHS) Freedom of Information Act (FOIA) and Privacy Act (PA) Record System, supports the collection and use of information for FOIA management purposes.

### Information Management Liaison Section (IMLS) Branch

The IMLS Branch provides 24/7 access to information from A-Files located at the NRC and the Kansas City Federal Records Center (FRC) to USCIS, CBP, ICE, and other government agencies. The IMLS Branch uses their NRC ECN page for information sharing among IMFS staff members. The IMLS Branch uses the ECN site to post work schedules, links to manuals and guides, training resources, and a document library with information that assists employees to process cases.

Links to manuals and guides include Central Index System Quick Guide, Enforcement and Removal Module (EARM), Systematic Alien Verification Entitlement ECN site, Enterprise Document Management System (EDMS), EZ Ticket (IT Service Desk Help Tickets), and Faxcom (Microsoft Windows based facsimile application). The training resources, such as “New Hire Training,” “IMLS Overview,” “IMLS Policy,” “Weekly Tidbits,” and “How to Create an A-File” help IMLS Branch staff perform their work duties. The Document Library contains a variety of reference information that employees need when processing cases, such as the IMLS Branch employee directory, electronic Classes of Admission chart, and a For Official Use Only coversheet. It also contains important standard operating procedures related to national security, handling classified files, and Deferred Action for Childhood Arrivals.

### *Data Elements and Individuals Impacted*

- The IMLS ECN site collects the following information about federal employees and contractors: name, work phone number, USCIS email address, and user ID.

### *SORN(s)*

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, which supports the sharing of A-File content.

### Program Management Operations (PMO) Branch

The PMO Branch assists in building the NRC acquisition, program management, and strategic planning capabilities. The PMO Branch focuses on costs, schedules, and performance



for project management within the NRC. The PMO Branch uses the ECN site to share NRC space analysis project files, project tracking data, and budgetary data among PMO Branch staff members.

The PMO Branch maintains PII on its ECN page. The PMO ECN site collects the following information about federal employees and contractors: name, work phone number, USCIS email address, and user ID.

### **System Access:**

Access to PII restricted pages within the NRC ECN site is limited to NRC personnel. The site administrator controls the permissions given to access the NRC ECN. Individuals requiring access to a page containing PII must request access through the site administrator. The site administrator reviews the request, obtains supervisory verification that the employee has a valid need-to-know, and only then is the employee granted access to that particular page.

### **Sources of Information:**

Information maintained on the NRC's ECN site comes from redacted A-File materials and documents, manual audit logs, Microsoft Access databases, FOIA Information Processing System (FIPS), Freedom of Information Act Immigration Records System (FIRST), eSTAT, Microsoft Excel workbooks, Microsoft Word documents, and Infopath forms.

### **Records Retention Period:**

The NRC reviews the NRC ECN site on a monthly basis to ensure that documents that follow the general records schedule of "delete when no longer needed" are disposed of within three years. However, this will not be the case for all documents, such as policies and procedures documents, training guides or documents that are for on-going projects, which may not change every three years. Site owners and site facilitators are responsible for archiving and removing the data from ECN. In accordance with the applicable record retention schedules (GRS 1.3, 2.2, 4.2, and 5.6), the NRC will continuously audit all content in its site collection to ensure only the most current information is stored and will archive any old files.



## Appendix B – Office of Security and Integrity

### Program/System:

Office of Security and Integrity ECN Site

### Purpose and Use:

#### Background:

In March 2007, U.S. Citizenship and Immigration Services (USCIS) Director Emilio Gonzalez announced the creation of the Office of Security and Integrity (OSI) to enhance existing USCIS functions that focus on management integrity, individual integrity, and security of USCIS employees and facilities. OSI is divided into four distinct divisions: the OSI Front Office, the Field Security Division, the Mission Integrity Division, and the Personnel Security Division.

*OSI Front Office* provides: (1) overall fulfillment of all USCIS mission requirements for security and integrity and for the strategic leadership and management of OSI; (2) leadership of the overall ongoing management and operations of OSI; (3) a cohesive and unified single point of contact for coordination and control of all issues, guidance, training, and communications going into and coming out of the OSI; and (4) all of the administrative, financial, contracting, and human capital services needed to run the OSI.

*Field Security Division (FSD)* provides physical and field security expertise and support to USCIS personnel and facilities nationwide to include HQ. The work of the FSD is central to achieving a core mission of USCIS by promoting the security and integrity of USCIS operations, organization, and resources. The FSD is responsible for the active and passive measures designed to prevent unauthorized access to personnel, equipment, facilities, assets, and documents and to mitigate the disruption of the USCIS mission.

*Mission Integrity Division (MID)* provides security products and the development and integration services for fulfilling the mandatory mission-level security, occupational safety and health, continuity, and emergency management requirements for the USCIS enterprise. The Chief of the Division serves as the Designated Agency Safety and Health Official (DASHO) as well as the Agency Continuity Manager.

*Personnel Security Division* ensures all federal and contractor personnel have the appropriate background investigations, to include investigations for suitability, fitness, security clearances, and periodic reinvestigations.

#### Enterprise Collaborative Network (ECN)

OSI uses the Enterprise Collaborative Network (ECN) as a tool to improve collaboration and communication with internal and external DHS stakeholders. ECN has become an integral



and mission critical part of OSI daily operations to manage documents and information using SharePoint lists, libraries, surveys, and team calendars. OSI has also automated several business processes to improve efficiency and transparency in the Office.

The OSI Web Management (OWM) is the site owner for the entire OSI ECN site collection. Selected Divisions have assigned site facilitators which have completed the required USCIS ECN Contributor and Facilitator training. These site facilitators are responsible for the design as well as the content of their respective sites; and work closely with the OWM administrators to ensure that data and information is properly stored and is accessible only by authorized users. OSI OWM requires all OSI Division site facilitators to appropriately identify and certify that they have S/PII data stored on their sites. S/PII stored must be directly relevant and needed to meet mission requirements. Privacy and security practices are being followed to monitor the ECN and ensure the appropriate handling and maintenance of S/PII. The OSI OWM site owner and all OSI site facilitators are required to complete the PII training and conduct monthly audits on ECN sites and permission groups to ensure the information being shared conforms to the approved uses.

OSI has a critical need to store S/PII data on ECN sites to facilitate and improve daily operations. The OSI ECN Site is broken into the following sub sites:

### OSI Front Office

OSI site has created a list to comply with DHS/USCIS emergency or Continuity of Operations Planning (COOP) requirements housing HQ OSI employees' contact information and emergency contact information. All personal information is inputted or edited directly by the employee. Employees cannot view the information of other employees, but may only access their own information. The list is located on the ECN in a secure environment. Full access to the list is only given to key management personal and accessed only during an emergency and/or COOP event when accountability of all personnel is necessary (i.e., a disaster or other life-threatening event occurs).

#### *Data Elements and Individuals Impacted*

- The OSI Front Office site collects contact information about HQ OSI employees, including employee name, office phone number, cell phone number, employee home address, and employee personal phone number.
- The site also collects the name and phone number for an employee emergency contact.

#### *SORN(s)*

- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, which covers the collection and use of contact information.



## Federal Emergency Response Officials (FERO)

The purpose of the site is to support the designation/revocation process for appointment of Federal Emergency Response Officials (FERO). The FERO process is carried out as part of agency compliance with federal continuity directives (i.e., FCD1, FCD2). The online form which is maintained by MID's Emergency Management and Safety Branch, is based on DHS Form 11000-27 (Federal Emergency Response Official Designation Request). The information is not shared outside the office. The function of the FERO process is to coordinate approval and then notify the USCIS Identity Management Unit (IMU) to add or remove the FERO designation label to the employee's PIV card.

### *Data Elements and Individuals Impacted*

- Personal identifiers, such as date of birth and home address, are required on the DHS FERO form. The Identity Management Unit will use the personal identifiers in the Information Security Management System (ISMS)<sup>9</sup> to identify the correct applicant to process the designation.

### *SORN(s)*

- DHS/ALL-014 Department of Homeland Security Personnel Contact Information, which covers the collection and storage of emergency contact information, as well as federal employee information for federal emergency response purposes.

## Local Security Officer (LSO) Program

Field Security Division (FSD) manages the Local Security Officer (LSO) program for USCIS. Volunteers are selected to serve as LSOs to help the Field Security Managers provide security support to their respective offices. To help manage the program, FSD uses the site to keep track of information, including the names of USCIS employees and contractors appointed as LSOs, the date the LSO was appointed, and the date the LSO received training. The information is entered in ECN by the FSD regional Program Support Analysts and the HQ Senior Security Analyst who oversees the LSO program. Access to the ECN page is restricted to FSD staff and the OSI site owners. Documents are posted on ECN until they are replaced by an updated version or are no longer applicable. The Site Administrator is responsible for creating and managing the ECN page and making sure that permissions are restricted to authorized personnel only.

---

<sup>9</sup> ISMS is a web-based case management tool designed to support the life cycle of DHS personnel security, administrative security, and classified visit management programs. For more information, please see DHS/ALL/PIA-038 Integrated Security Management System (ISMS), available at <https://www.dhs.gov/privacy-documents-department-wide-programs>.



### *Data Elements and Individuals Impacted*

- The FSO Program site collects the names of USCIS employees and contractors appointed as LSOs.

### *SORN(s)*

- DHS/ALL-014 Department of Homeland Security Personnel Contact Information permits the collection and storage of emergency contact information, as well as federal employee information for federal emergency response purposes.

### Facility Access Request (FAR)

The Field Security Division (FSD) manages the Facility Access Request (FAR) List for the USCIS National Capital Region (NCR). When a contractor (e.g., plumber, electrician, movers, painters, laborer or any other maintenance repair personnel) is scheduled to come to work at a facility, facilities personnel or building management submits a request with the contractor's information to the OSI NCR Security Office.

### *Data Elements and Individuals Impacted*

- The FAR ECN Site collects the following information from the requestor: Visitor date and time of visit, Requestor's name, Requestor's phone number, Visitor's full name, Visitor's date of birth, Visitor's full SSN, Visitor's company, Date NCIC check was conducted, Approval status, Comments.

### *SORN(s)*

- DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management to collect and maintain records associated with DHS facility and perimeter access control, as well as visitor security and management.

### Monthly Insider Threat Docket Report

MID's Enterprise Risk Management Branch (ERMB) creates the monthly Insider Threat Docket Report to inform the USCIS Office of Communication and senior leadership of the status of serious criminal cases involving current and former USCIS employees, as well as selected high-profile non-employee cases impacting the USCIS mission. The order of the cases is based on the timing of upcoming event and the nexus between the offense and the USCIS mission.

The Insider Threat Docket Report is the official report of USCIS employee misconduct, and the misconduct of other employees within DHS. The report is necessary to preserve the chain of record cases that could ultimately assist in creating new policies, and to enhance training



at USCIS thus ensuring the integrity of the agency's mission is not being compromised. All information within this report comes from publicly-available court documents and covers insider threat cases for awareness to USCIS stakeholders.

ERMB downloads case information on serious criminal cases involving current and former USCIS employees and contractors, as well as selected high-profile non-employee cases affecting the USCIS mission.

### *Data Elements and Individuals Impacted*

- The following types of information are collected from current and former USCIS employees as well as individuals involved in non-employee cases that impact the USCIS mission: Alias, Associated Cases, Attorney, Case File Location, Case Summary, Deadlines/Hearings, Docket Report, Filers, History/Documents, Party (defendant, plaintiff, etc.), Related Transactions, Status, View a Document.

### *SORN(s)*

- DHS/ALL-014 Department of Homeland Security Personnel Contact Information permits the collection and storage of emergency contact information, as well as federal employee information for federal emergency response purposes
- DHS/ALL-020 DHS Internal Affairs permits the collection and storage of DHS and USCIS personnel who are involved in cases of employee misconduct.
- DHS/ALL-038 Insider Threat Program System of Records, which covers the management of insider threat inquiries, and identify and track potential insider threats to DHS.

### **System Access:**

OSI ECN users may include USCIS employees and in rare instances employees from other DHS components. All OSI ECN sites have three primary permission groups: Owners, Members, and Visitors. The Owners Group has 'full control' over specific ECN sites and sub-sites. Site Owners are responsible for the design, security, and maintenance of their ECN team sites, including permissions, site creation, web part creation and customization, and user training. The Members Group has 'contribute' access with permission to view, add, update, and delete select content within that site. The Visitors Group has 'read' access to the site, with permission to view/read select content within that site. This group allows for cross site visibility with restricted permissions. OSI ECN parent sites are visible to all OSI employees. Sub-sites with designated site facilitators can be restricted to certain members. Depending on the sensitivity of some information, permissions are set at the document level and only those with a need-to-know can access it. OSI maintains strict security controls over sensitive information per direction from



USCIS. OSI ensures that all information on its ECN sites is protected and in compliance with USCIS ECN governing policies and procedures.

**Sources of Information:**

Information contained in the OSI ECN sites is provided by USCIS Employees, federal employees, members of the public, and public websites.

**Records Retention Period:**

OSI frequently reviews the OSI ECN site to ensure documents follow the general records schedule of “delete when no longer needed,” and are disposed of within three years. However, this will not be the case for all documents, such as policies and procedures documents, training guides or documents that are for on-going projects, which may not change every three years. Site owners and site facilitators are responsible for archiving and removing the data from ECN. In accordance with the OSI Records Retention Schedule of 15 years, OSI will continuously audit all content in its site collection to ensure only the most current information is stored and will archive any old files.



## Appendix C – Fraud Detection and National Security Directorate

### Program/System:

Fraud Detection and National Security Directorate ECN Site

### Purpose and Use:

#### Background:

The Fraud Detection and National Security Directorate (FDNS) is a directorate within the U.S. Citizenship and Immigration Services (USCIS), an agency within the U.S. Department of Homeland Security (DHS). FDNS leads USCIS' efforts to safeguard the integrity of the nation's lawful immigration system by spearheading agency efforts to combat fraud, detect national security and public safety threats, and maximize law enforcement and Intelligence Community (IC) partnerships. FDNS consists of the following offices and divisions: Front Office, Reports & Analysis Branch (RAB), Facilities & Asset Management, Fraud Division, Immigration Vetting Division (IVD), Intelligence Division, Social Media Division, National Security & Public Safety Division (NSPSD), Systems Integration Division (SID), Mission Support Division, and Training and Knowledge Management Division.

#### Enterprise Collaboration Network (ECN)

FDNS uses the Enterprise Collaboration Network (ECN) as a tool to improve collaboration and communication with internal and external USCIS stakeholders. ECN has become an integral and mission critical part of FDNS's daily operations to manage documents and information using SharePoint lists, libraries, surveys, and team calendars. FDNS has also automated several business processes to improve efficiency and transparency within the directorate.

The FDNS ECN Site is broken into several pages and collaborative workspaces. The FDNS parent site collection includes administrative tracking and personnel lists. Each FDNS division and organizational office maintains its own collection of pages and collaborative workspaces within the ECN site collection, which may include both administrative records and operational records.

#### Administrative and Personnel Records

The FDNS ECN site collection maintains records used for mission support and personnel management, including personnel lists and calendars, hiring/onboarding actions, employee dashboards, employee recognition and awards, telework agreements and work schedules, hiring actions, detail or rotational assignment documents, organizational lists, and related documents. FDNS also uses the ECN to comply with DHS/USCIS emergency or Continuity of Operations



Planning (COOP) requirements. The ECN site is also used to facilitate sensitive property tracking, equipment tracking requests and asset management guidance, and related documents.

### Data Elements and Individuals Impacted

- The FDNS ECN site maintains information about FDNS employees, including but not limited to: name, position, photo, office phone number, work cell phone number, work email address, personal email address, home address, and personal phone number(s), awards, etc.;
- The site contains emergency contact person(s) for the employee and their contact email address(es) and phone number(s); and
- The site also contains PII on members of the public applying to job vacancies, including: name, address, title, grade and salary, employment history, performance awards, military records, and education transcripts.

### SORN(s):

- OPM-GOVT-1 General Personnel Records<sup>10</sup> covers the use and storage of FDNS personnel PII for administrative purposes;
- OPM-GOVT-5 Recruiting, Examining, and Placement Records<sup>11</sup> covers the use and storage of applicants and selectees for a FDNS vacancy;
- DHS/ALL-010 Department of Homeland Security Asset Management Records<sup>12</sup> covers the use and storage of FDNS employee assets; and
- DHS/ALL-014 Department of Homeland Security Personnel Contact Information System of Records<sup>13</sup> covers the collection, use, and storage of FDNS emergency contacts.

### Executive Secretariat Task Tracking

The FDNS Executive Secretariat Dashboard (ED) is a tool used to manage Executive Secretariat taskings. ED has built in functionality to automatically assign tasks to designated FDNS divisions for response or action. ED is used to coordinate internal document reviews and facilitate collaboration. ED is also used to track responses to Freedom of Information Act (FOIA) requests and may include internal taskers related to personnel actions; however, sensitive

---

<sup>10</sup> See OPM/GOVT-1 General Personnel Records, 77 FR 73694, (December 11, 2012), available at <https://www.dhs.gov/system-records-notices-sorns>.

<sup>11</sup> See OPM/GOVT-5 Recruiting, Examining, and Placement Records, 79 FR 16834, (March 26, 2014), available at <https://www.dhs.gov/system-records-notices-sorns>.

<sup>12</sup> See DHS/ALL-010 Asset Management Records System of Records, 80 FR 58280, (September 28, 2015), available at <https://www.dhs.gov/system-records-notices-sorns>.

<sup>13</sup> See DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 FR 11780, (March 16, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.



personnel documents or those containing PII are not attached to the record in ED. ED is used primarily for tracking purposes. FDNS uses permissioned links to ensure that only those with a need-to-know see sensitive personnel information in the ED tracker.

### Data Elements and Individuals Impacted

- ED collects names, email addresses, and telephone numbers of federal employees and contractors; and
- ED also collects names of members of the public when that information is included in a FOIA request.

### SORN(s):

- DHS/ALL-016 Correspondence Records<sup>14</sup> covers the collection and maintenance of correspondence records submitted by the general public, DHS personnel, and others; and
- DHS/ALL-002 DHS Mailing and Other Lists System<sup>15</sup> covers the use, collection, and storage of contact information included in the Executive Secretariat taskings.

### Division and Organizational Office Sites

FDNS and its divisions also use the ECN to house internal, collaborative workspaces and project trackers. FDNS maintains documents that include PII or sensitive PII on the following:

- Project workspaces, to include workspaces for specific projects managed by each division; these workspaces include sensitive PII on U.S. Citizens and non-U.S. Citizens and may include information relating to administrative investigations, background, identity or security checks, external vetting, large scale fraud cases, site visit programs, social media assessments<sup>16</sup>, and coordination during national security events, or other special projects;
- FDNS file review site for tracking Government Performance and Results Act (GPRA) measures;
- Reports and analysis, such as fraud trends, studies, requests for statistics, field reporting, and critical incident response reporting;

---

<sup>14</sup> See DHS/ALL-016 Correspondence Records, 83 FR 48645 (September 26, 2018), available at <https://www.dhs.gov/system-records-notices-sorns>.

<sup>15</sup> 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>.

<sup>16</sup> The collection and use of social media information is compliant with DHS Instruction 110-001, Privacy Policy for the Operational Use of Social Media and is detailed in a separate PIA. See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE FRAUD DETECTION AND NATIONAL SECURITY DIRECTORATE, DHS/USCIS/PIA-013-01(a) (2019), available at <https://www.dhs.gov/uscis-pias-and-sorns>.



- Intelligence reporting, intelligence workflow management, and information used in support of managing internal and external requests for information (RFIs); and
- Training materials, including “real world” examples used for training purposes that contain PII such as digital copies of some Alien File (A-file) documents or printouts from systems used to perform background checks.

### Data Elements and Individuals Impacted

FDNS ECN sites maintain information on individuals associated with immigration requests that have been reviewed by FDNS. This may include, but is not limited to, any of the following data elements on non-U.S. persons and sometimes U.S. persons: name, date of birth (DOB), place of birth, country of citizenship/nationality, immigration status, Passport number, Alien Number (A-Number), receipt number, mailing addresses, telephone numbers, email addresses, names of immediate family members, names of associates, marriage records, civil or criminal history information, military and educational records, travel information, biometric identifiers, other unique identifying numbers, and other information from the A-File or immigration request form or from other sources of information dependent upon the situation.

### SORN(s):

- DHS/USCIS-006 Fraud Detection and National Security Records (FDNS)<sup>17</sup> permits the collection and maintenance of PII associated with immigration requests in the FDNS – Data System and other IT systems developed specifically for FDNS, including the collaborative workspaces within the FDNS ECN site collection.

### **System Access:**

Only USCIS personnel assigned to unique SharePoint permission groups have access to the FDNS ECN site collection and may not have access to the entire site, based on need-to-know. The FDNS Training and Knowledge Management team serves as the lead contributors for any directorate-wide needs on the FDNS ECN site collection which includes initial design and initial management of access requirements.

To address specific requirements within each division’s ECN site, each division is responsible for assigning a site facilitator who has completed the required USCIS ECN contributor and facilitator training. The site facilitators work closely with the FDNS Training and Knowledge Management team on the initial design and content of their respective sites and provide technical support as needed. The site facilitators are also required to ensure that data and information is properly stored and is accessible only to authorized users on their respective sites.

---

<sup>17</sup> See DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012), available at <https://www.dhs.gov/system-records-notice-sorns>.



All FDNS ECN sites have three primary permission groups: Owners, Members, and Visitors.

1. Owners have ‘full control’ over specific ECN sites and sub-sites. They are responsible for the design, security, and maintenance of their ECN team sites, including permissions, site creation, web part creation and customization, and user training;
2. Members have ‘contribute’ access with permission to view, add, update, and delete select content within that site; and
3. Visitors have ‘read’ access to the site, with permission to view/read select content within that site. They can provide cross site visibility with restricted permissions.

FDNS ECN parent sites are visible to all FDNS employees who have been added to the FDNS members permission group. Sub-sites with designated site facilitators can be restricted to certain members. Depending on the sensitivity of some information, permissions are set at the document level and only those with a need-to-know can access it. FDNS maintains strict security controls over sensitive information with direction from USCIS. FDNS ensures that all information on its ECN sites is protected and in compliance with USCIS ECN governing policies and procedures. USCIS ECN Support performs routine auditing to confirm permissions are being appropriately managed.

### **Sources of Information:**

Much of the data collected in the FDNS ECN site is obtained from the immigration benefit applications and forms submitted to USCIS by individuals or their authorized representatives or preparers. Information is also collected from systems against which that data is screened during the screening process. Information may be derived from multiple sources, including DHS and USCIS systems, external systems, A-files, interviews and site visits.

Information on FDNS personnel is directly collected from personnel, personnel records, or from DHS’s Global Address Listing (GAL).

### **Records Retention Period:**

Retention periods will vary, depending on the content of the records. In general, documents stored on FDNS ECN sites are retained until no longer needed for business purposes and have a shelf life of three years before being archived to a shared drive. However, this will not be the case for all documents, such as policies and procedures documents, training guides or documents for ongoing projects, which may not change every three years. Site owners and site facilitators must be familiar with retention requirements specific to their respective datasets and are responsible for archiving and removing the data from ECN. In accordance with the appropriate General Records Schedules and the FDNS Records Retention Schedule of 15 years,



FDNS will continuously examine content in its site collection to ensure only the most current information is stored and will archive any old files.