Privacy Impact Assessment
for the

Electronic Discovery Software System

December 10, 2010

Contact Point
Peter Vincent
Principal Legal Advisor
U.S. Immigration and Customs Enforcement
202-732-5000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Electronic Discovery Software System (EDSS) is owned by the Office of the Principal Legal Advisor (OPLA) within U.S. Immigration and Customs Enforcement (ICE), a component of the Department of Homeland Security (DHS). EDSS supports the collection and organization of paper and electronic documents for analysis, review, redaction, and production to meet litigation discovery requirements. ICE may also use the system to process agency records in response to Freedom of Information Act (FOIA) or Privacy Act (PA) requests. ICE conducted this Privacy Impact Assessment (PIA) because EDSS collects, analyzes, and stores personally identifiable information (PII).

Overview

ICE uses EDSS to support the collection, review, redaction, and production of agency records to comply with discovery requirements during litigation and to respond to FOIA/PA requests for ICE records. EDSS replaces the manual processes by which ICE attorneys gather, sort, review, and redact agency records that are potentially responsive to a discovery or FOIA/PA request; assess its relevance and/or responsiveness; and apply appropriate privileges (in litigation) or exemptions (under the FOIA/PA).

Like all government agencies, ICE increasingly stores information electronically. EDSS is necessary to address the complexity of collecting, reviewing, redacting, and producing agency records, including electronically stored information (ESI). In some cases, for example, ICE may have an obligation to produce ESI in the same format in which it is ordinarily compiled or maintained ("native format"), along with any associated "metadata," the hidden data in some electronic documents that may describe who created or edited a document. Although EDSS was developed primarily to address federal discovery requirements regarding ESI during litigation, in some cases ICE attorneys also may use the system to review paper documents that are scanned into electronic form.

EDSS has various capabilities that serve to streamline and automate the document reviews conducted by ICE attorneys. First, EDSS ingests and analyzes information in various data formats (e.g., Microsoft Word and Microsoft Excel), allowing document analysis in bulk within a single data file and using a single integrated viewer that does not require use of the original application that created the file. Second, EDSS allows ICE attorneys to view metadata within files stored in these varying file formats. Third, it identifies and eliminates duplicate documents from the review process. Fourth, the system automates the identification of protected information by searching for names, phrases, and terms (collectively, "keywords") that are input by the reviewing attorney. This allows the reviewing attorney to customize keywords for each set of documents or cases that may indicate the existence of privileged or protected information. The system uses that information to automatically flag files that contain those keywords for the attorney, who will review and determine if the files or information therein should be protected from disclosure. Finally, EDSS allows attorneys to electronically redact protected portions of documents in the system.

EDSS has additional features that speed up the process by which attorneys or other ICE employees designate or redact the same protected information from multiple records. For example, EDSS allows for the bulk redaction of a confidential informant's name, or identifies for the attorney all

occurrences of a keyword associated with a confidential law enforcement technique so that the attorney can decide whether it is appropriate to redact each instance of that keyword as it appears in multiple records.

Background

ICE acquired EDSS to facilitate the efficient compliance with federal requirements to preserve and produce ESI in civil and criminal litigation matters according to the Federal Rules of Civil and Criminal Procedure. In civil proceedings, ICE is typically defending an action brought against the agency for violations of federal tort law or on other grounds, and has obligations to preserve and produce relevant ESI and other records under the Federal Rules of Civil Procedure. As a criminal investigative agency, ICE may possess ESI and other records that are relevant to the proof of necessary elements of criminal offenses during a criminal trial, and may also be relevant, material, and necessary to a criminal defendant's legal defense. The U.S. Constitution and the Federal Rules of Criminal Procedure may require ICE to disclose such records and information fully during or before the criminal proceeding. Because of its technical capabilities in the efficient processing, review, and redaction of records, OPLA also expects to use EDSS during the processing and response of FOIA/PA requests for OPLA records, on an ad hoc basis.[1]

EDSS is expected to improve significantly the efficiency of OPLA's processing of records during discovery in litigation. OPLA's discovery productions typically require the preservation, collection, and analysis of tens of thousands of e-mails, word processing documents, PDF files, spreadsheets, presentations, database entries, and other documents in a variety of electronic file formats, as well as paper records. The current manual process of preserving, collecting, and analyzing those records is burdensome and inefficient. For example, under the current manual process it is difficult--and often practically impossible--for ICE attorneys to review documents for metadata; however, these metadata may be discoverable and may contain privileged information. In addition, many of the discoverable documents are duplicates, and because it is difficult to manually identify duplicates among voluminous records, ICE attorneys often waste valuable time reviewing multiple identical documents. The automation of this process using EDSS will dramatically reduce the time ICE attorneys spend on administrative tasks related to document management and improve the quality and efficiency of overall document review and production within OPLA.

[1] FOIA (5 U.S.C. § 552) permits any person to request access to federal agency records. FOIA also establishes a presumption that records in the possession of federal departments and agencies are accessible to the people, except to the extent the records are protected from disclosure by any of nine exemptions contained in the law, or by one of three special law enforcement record exclusions. The PA (5 U.S.C. § 552a) provides individuals the right to request access to records about them contained in an agency system of records. Individuals are entitled to these records unless the agency has claimed an exemption from the system of records based on sensitivities such as pending law enforcement activities. Requests received under the FOIA are also processed under the PA, and vice versa, to ensure that individuals who seek records about themselves receive the greatest access to which they are entitled by law. Agencies are obligated to search for, review, and produce non-exempt records or portions thereof in response to FOIA/PA requests.

Document Collection Process

In litigation, the document review and production process typically is initiated after litigation is filed against the agency or in a case in which the agency may have an interest (such as a criminal prosecution of a person the agency investigated). Once OPLA becomes aware of the need to preserve records, it issues a litigation hold notice describing the information and records that may be discoverable in the context of that litigation. The notice informs employees who may be custodians of such data that they are to preserve and/or produce it to OPLA for review.

In the FOIA/PA context, the process is initiated by the receipt of a FOIA/PA request by the agency's FOIA Office and the tasking of that request to OPLA as an office that is believed to have responsive records. OPLA may, on an ad hoc basis, use EDSS to gather, review, and mark exempt material in the records OPLA collected that are responsive to the FOIA/PA. Because the use of EDSS to facilitate the process of reviewing the documents does not differ greatly in FOIA/PA and litigation contexts, the remainder of this description will focus solely on the litigation context.

After the litigation hold issues, individual ICE employees and technical support personnel take action to preserve the evidence described by the litigation hold notice. In most cases, the litigation hold will state the names and any unique identifiers, such as the Alien Registration Number (A-Number), of persons related to the litigation. It may also include additional, distinctive terms that allow employees and technical support personnel to identify other relevant documents. Individual employees may be served with notices prohibiting the deletion or destruction of evidence, whether in paper or electronic form. They are not generally required to identify, harvest, and produce evidence until the case is in litigation and discovery commences.[2]

When discovery commences, ICE attorneys notify employees of their obligation to identify, harvest and produce evidence through pre-established points of contacts in the program offices. The role of technical support personnel varies, depending on the stage of the litigation and the media on which data are likely to be stored. These technical support personnel may be required to search all locations where responsive ESI might be stored including central agency databases, agency file servers (e.g., shared drives), and centrally stored agency electronic mail for records described in the litigation hold. In some cases, technical support personnel may initially set aside any back-up tapes and files containing relevant information and physically preserve them in their original form. In other cases, technical support personnel may have to search electronic storage systems for relevant agency records, which they then download to portable storage media or drives maintained on servers. In extreme cases, where an employee is likely to possess a significant amount of electronically stored information on an individual work station or storage medium, technical support personnel may make images or copies of the entire storage medium for evidence preservation purposes.

Once relevant information has been identified and litigation ensues, OCIO personnel or OPLA personnel will transfer the data to the secured shared drive. Once all relevant data has been transferred to the shared drive, the EDSS System Administrator(s) will use EDSS to upload the data from the shared drive onto a central EDSS repository.

[2] While OPLA usually does not begin the process of gathering records until litigation is actually filed, in some cases OPLA may gather such records when litigation is only reasonably likely.

If litigation does *not* ensue, the litigation hold is lifted when the statute of limitations expires, or when OPLA otherwise concludes that litigation is not reasonably likely. The records that were covered by the litigation hold, but never uploaded into EDSS, are then maintained or deleted in accordance with normal agency retention policy as set forth in applicable records disposition schedules.

Document Review Process

EDSS supports 400 different file formats that can be reviewed in a native viewer, avoiding the need to install the application used to create the document on the reviewing attorneys' computers. This also eliminates the necessity of converting documents into formats that can be viewed and redacted by attorneys using their current computer configurations, thereby reducing the risk that the documents will be altered which could violate federal evidentiary and discovery rules. The types of electronic documents that EDSS can collect and process varies but includes formats such as Tagged Image File Formats (TIFF), Portable Document Format (PDF) files, JPEG images, Microsoft PowerPoint documents, and Microsoft Word documents. The documents loaded into EDSS are exact duplicates of existing data that are already stored in other ICE paper or electronic recordkeeping systems. The records loaded into EDSS are maintained in their original form and not modified. EDSS does create new information that is associated with those records, but that data does not alter the integrity of the original records themselves. The EDSS created data consists of redactions,[3] tags, privilege log, search and filter report, and audit trail, which is automatically created and maintains an historical record of all actions taken by users in the case being reviewed. EDSS also assigns a unique key to the original unaltered file, which helps establish the chain of custody and proof that that the content of the produced file or document has not been altered from the original version.

Records are loaded into a new EDSS "case" that is created for a particular litigation matter. The ICE supervisory attorney for that litigation grants EDSS privileges to the ICE attorneys and paralegals assigned to that litigation, allowing them to access and review the documents. During the review process, ICE attorneys may narrow the scope of documents reviewed by executing searches and filtering data, often using search terms agreed between the parties in litigation. As part of this initial review, EDSS automatically identifies and removes duplicate documents from the collection of data in the EDSS repository.[4] The ICE attorneys and paralegals then review the subset of documents resulting from the search and filter and associate tags with specific documents to classify and categorize those documents. In addition, they redact protected or privileged information. For each document redacted, ICE attorneys may enter free-form text describing the reason for the redaction.

Using this information, EDSS generates a privilege log to document the redactions or withholding of records on the basis of privilege; the privilege log is typically shared with the U.S. Department of Justice (DOJ), with other parties in the litigation, and sometimes with the court. The privilege log lists the location and basis of each redaction or withholding, cross-referencing each redaction to a specific

[3] Redactions are not considered alterations of the documents in EDSS. They merely hide information that should not be produced to opposing parties.
[4] De-duplication is based on the use of hash values. All records are assigned a hash value based on a combination of the content of the file and the metadata associated with the record. EDSS maintains only one copy of records that have identical hash values.

page number within the production.[5] Executed search terms and filters by ICE attorneys become part of a search report that EDSS can generate. The search report is produced to opposing parties to demonstrate a defensible process for gathering the totality of relevant data as agreed upon between the parties, or ordered to be produced by the presiding judge. Once the attorneys and paralegals complete the initial document review process, other attorneys (including supervisory attorneys) may conduct a quality review assessment to verify the accuracy and appropriateness of redacted and unredacted information.

Once the review is complete, ICE attorneys place the reviewed records in a production folder in EDSS indicating that they are ready to be produced to the DOJ, and eventually, to the court and opposing counsel. System administrators place the reviewed records in the appropriate file format for production, which varies and depends on the agreement among the parties or an order of the court. Production file formats are typically image files, such as PDF and TIFF. While redactions made to the records in EDSS are temporary, i.e., the EDSS users can view the content underneath the redaction as may be needed, once those records are saved into a production format the redactions are permanent. A copy of the records in their original format with the temporary redactions still resides in the system, however, and redactions can be changed if the same records need to be produced again in cases where the parties' agreement or a court order may require the agency to produce previously redacted information from those records or if a change in the redaction is determined to be warranted. Files in any format included in the production file may contain PII data unless the data is redacted by ICE attorneys prior to production.

In a typical transaction, OPLA becomes aware of a risk of pending litigation and issues a litigation hold notice that describes the information and records that ICE employees need to preserve for discovery purposes. The litigation hold notice is forwarded to employees who may be custodians of discoverable information. Employees, assisted as needed by technical support personnel, identify the agency records that are described in the litigation hold notice. If litigation later ensues, OPLA or OCIO personnel copy and transfer the records in electronic format to a secure shared drive on the ICE network. The collection may include bulk scanning of paper documents into an electronic format, such as PDF or TIFF, and preferably in a machine-readable format. Once all of the data has been uploaded to the secure shared drive, the data is imported into a central EDSS repository by a system administrator. The data residing on the secured shared drive is deleted once it has been confirmed that the data has been successfully uploaded into the EDSS repository. Any hardcopy records received will be scanned and saved as PDF documents. The PDF documents will then be uploaded to the secure shared drive. Upon successful upload into EDSS, the PDF documents will be deleted from the secure shared drive; however, the hardcopy records will be maintained in their original form by the ICE attorney with the case file. Using EDSS, ICE attorneys and paralegals review these records to further cull the volume of potentially relevant documents that may need to be reviewed. Attorneys and paralegals use EDSS to search for, tag, and redact privileged or protected material and to generate a privilege log that describes the location of and basis for the redactions. When the review is complete, an EDSS system administrator generates a production file in EDSS that places the data into the appropriate format for production to the DOJ, other parties in the litigation, and in some cases the court. The production file is extracted from EDSS, encrypted, and written to an external portable storage device for transfer to the recipient.

[5] The page numbers, marked by a process known as Bates stamping, are also generated by EDSS.

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?

In civil cases, most electronic discovery requirements that govern the operation of EDSS are contained in Rules 16, 26, 34, and 37 of the Federal Rules of Civil Procedure and are enforceable by orders of the federal courts. In criminal cases, full and open discovery of agency records may also be compelled by the Fifth and Sixth Amendments to the U.S. Constitution and the Federal Rules of Criminal Procedure. In FOIA/PA matters, the disclosure requirements are mandated by the Freedom of Information Act (5 U.S.C. § 552) and the Privacy Act of 1974 (5 U.S.C. § 552a(d)).

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

In the context of litigation, the DHS General Legal Records SORN (DHS/ALL-017, October 23, 2008, 73 FR 63175) applies to EDSS data gathered in the context of litigation. The DHS FOIA and Privacy Act Record System SORN (DHS/ALL-001, October 28, 2009, 74 FR 55572) applies to EDSS data in the context of FOIA/PA.

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

The EDSS system is currently undergoing a Certification and Accreditation (C&A) process. The anticipated scheduled Authority to Operate (ATO) date for the system is December 15, 2010.

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

ICE is developing a records retention schedule for the records maintained in EDSS.

Section 2.0 Characterization of the Information

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

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

EDSS stores and processes agency records as necessary to satisfy litigation discovery requirements and to respond to FOIA/PA requests. Information in EDSS could consist of any ESI or other information in any ICE formal or informal recordkeeping system or any paper documents scanned into an electronic format for review. In some cases, if a discovery or FOIA/PA request asks ICE to

provide records in the possession of DHS or other DHS components, ICE personnel may process those records through EDSS.

Because EDSS is a document processing tool, the ESI and other records that may be stored and processed in EDSS could pertain to any matter in the scope of DHS or ICE's mission and may contain PII of any nature captured and stored in such records. For civil litigation that is reasonably likely or pending, any information that is potentially relevant to the matter may be collected and maintained in EDSS for discovery purposes. To the extent it is applied in the processing of FOIA/PA requests, EDSS may store and process any agency records that are potentially responsive to the request. For criminal matters, EDSS may be used to assist in pre-trial discovery of investigative materials related to the defendant's criminal investigation or prosecution. The actual information stored and processed in EDSS will always vary and depend on the nature of the particular litigation or FOIA/PA request.

The types of individuals on whom information could be collected in EDSS varies on a case-by-case basis, but may include anyone involved in litigation with DHS, persons who file FOIA/PA requests requesting ICE records, persons who correspond with DHS or ICE, employees and contractors of DHS and other federal agencies, aliens in removal proceedings, witnesses and other sources of information, attorneys and authorized representatives, subjects of investigations, criminal defendants, and others whose information is contained in the records collected during the course of an investigation, enforcement matter, or other matter of any kind handled by ICE or DHS.

Listed below are examples of general types of records that EDSS may store or process in a litigation or FOIA/PA context:

Electronic mail: messages among ICE employees, or among ICE employees and personnel of other federal agencies or outside entities, sometimes with other documents attached;

Presentations: documents such as PowerPoint presentations used for training purposes;

Spreadsheets: data collections, often including PII and sensitive law enforcement data, used to track the progress or investigations or focus investigative priorities;

Database entries: information collected or compiled from law enforcement or other agency databases;

Identification documents: passports, identification cards, driver's licenses, and documents with biometric information including but not limited to photographs and fingerprint cards;

Legal documents: criminal records, court documents such as Notices to Appear (NTAs), and I-213s (Record of Deportable Alien); and

Miscellaneous: letters, memoranda, drafts, and receipts.

Electronic documents stored in and processed by EDSS may also contain "metadata," the hidden data in some electronic documents that may describe who created or edited a document, and when. PII may be contained in metadata (e.g., the name of the author of a particular electronic file), which may itself be discoverable in litigation or responsive to a FOIA/PA request.

As described in the Overview, EDSS supports 400 different file formats that can be reviewed in a native viewer, such as TIFF, PDF files, JPEG images, Microsoft PowerPoint documents, and Microsoft Word documents. The specific PII collected in these records will vary based on the nature of the records themselves, the breadth of the request, and the nature of the request (criminal discovery, civil discovery, FOIA/PA). Generally, PII collected may include name, Social Security number, photograph, aliases, date of birth, citizenship and immigration status, nationality, immigration benefits, immigration history, admission information, customs import-export history, criminal arrest and conviction records, A-Number, phone numbers, addresses, identification document numbers, criminal associations, family relationships, employment, military service, education, and other background information.

During the document review process by ICE attorneys and paralegals, new data is generated in EDSS. A hash value is assigned to records in EDSS which is used to identify and remove duplicate documents with identical hash values. Documents are given page numbers, also known as the Bates stamp, and reviewers can add tags to individual records. Documents containing privileged or protected information are marked for redaction and tags are assigned to the redacted areas containing the legal justification for the redaction (e.g., attorney-client privilege, FOIA/PA exemption). EDSS uses this information to generate a privilege log, which contains the page number and basis for each redaction. (In the FOIA context this log is called the *Vaughn* index.) EDSS also generates a search and filter report, which contains a record of the searches and filters used by the attorneys and paralegals to reduce the size of the original records loaded into EDSS to only those that meet certain criteria, which is typically agreed upon by the parties in the case. EDSS also automatically creates and stores an audit trail that captures all actions by users in the case being reviewed. Finally, EDSS assigns a unique key to the original unaltered file, which helps establish the chain of custody and proof that that the content of the produced file or document has not been altered from the original version that was stored in the EDSS repository.

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

EDSS may store and process data from any ICE record keeping system. The nature of those records vary and may include law enforcement records, personnel and training records, financial records, etc. The source of such records will vary depending on the type of activity the record is created to support. For example, personnel records will typically collect information from the employee, the supervisor, and other offices within the agency such as payroll. Law enforcement records typically collect information from external sources such as witnesses, public records, business records, or other government recordkeeping systems, but may collect information from the individual that is the subject of an investigation in some circumstances. Any of these records may also contain metadata, which is typically generated by the source system. Because EDSS can contain any records that ICE receives, creates or maintains, it is not possible to list all of the possible sources of information for those records.

ICE attorneys and paralegals enter the search and filter terms, mark the records for redaction, add comments noting the reason for the redaction, and add tags to the documents. The system itself is the source of the following information: hash values, Bates stamp, privilege log, search and filter report, the audit trail, and the unique key assigned to the original file.

The records in EDSS are originally gathered by ICE personnel pursuant to direction from OPLA (or the FOIA Office in FOIA/PA cases) to produce material that may be relevant to pending litigation. Technical support personnel may also search and retrieve electronic data from all locations where responsive ESI might be stored including, central agency databases, agency file servers (e.g., shared drives), and centrally stored agency electronic mail. Once relevant records have been identified, OCIO personnel or OPLA personnel will transfer them to the secured shared drive. Once all relevant records have been transferred to the shared drive, the EDSS System Administrator(s) will use EDSS to upload them from the shared drive onto a central EDSS repository.

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

EDSS could contain commercial or publicly available data only to the extent that it is already contained in the records loaded into the EDSS repository for litigation or FOIA/PA purposes. The commercial and publicly available data is merely a category of data that could be included in the records input into EDSS for review. Because ICE does use commercial source of data and publicly available data in executing its law enforcement mission, it is possible that such data may be included in EDSS. ICE agents and officers may use public and commercial data in a variety of ways, such as to identify locations as targets for investigation or surveillance, to assist ICE personnel in operations such as detainee transportation, or to identify nearby emergency or medical facilities. In some cases, ICE agents may obtain commercial financial information about targets of investigation to investigate the movement of funds that could be proceeds or instrumentalities of illicit activity.

2.4 Discuss how accuracy of the data is ensured.

EDSS operates under the principle of full and open discovery of whatever information exists in ICE recordkeeping systems. ICE may not alter, withhold, redact, or delete existing documents in the course of litigation discovery except as permitted by the Federal Rules of Civil or Criminal Procedure and as authorized by the court. Federal discovery rules and the FOIA/PA require the preservation and production of records in ICE recordkeeping systems, notwithstanding the accuracy of those records. The accuracy of the information in the documents themselves depends on their nature and source.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: EDSS could present a risk of the over-collection of PII or the aggregation of disparate PII from separate agency recordkeeping systems.

Mitigation: ICE only collects and aggregates information in EDSS only when it is under a legal mandate to respond to discovery and FOIA/PA requests. The agency does not have discretion to limit the scope of the collection. The risks present are mitigated by the limited use of the system to support the review and production of records in litigation and FOIA/PA matters, the limited role-based access to the information in EDSS to those ICE attorneys and paralegals assigned to those matters, and a robust audit trail of all user activity, including the viewing of records in the system.

Privacy Risk: EDSS could present a risk that the PII in the system is not accurate, complete, and current.

Mitigation: This risk is mitigated by the fact that the information in EDSS is not used by the agency to make decisions about individuals. The system contains only copies of records from other agency recordkeeping systems and is not used as an internal source of agency records about individuals. The purpose of EDSS is to support the mandatory production of agency records in pending litigation and in response to FOIA/PA requests. By law such records must be produced in their original form, even if they contain erroneous, incomplete, or outdated information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The purpose of EDSS is to support the mandatory production of agency records in pending civil or criminal litigation and in response to FOIA/PA requests. Records in EDSS are compiled, created, and used for this purpose. Specifically, the records gathered and loaded into EDSS are used by ICE to respond to discovery requests and orders, and requests from the public for agency records under FOIA/PA. The tags are used by ICE attorneys and paralegals to categorize and group the records based on their subject matter and whether they have been marked as containing information that may be withheld from production in the litigation or in response to a FOIA/PA request. ICE attorneys and paralegals use the filter and search terms to scope the larger records gathered in EDSS into a smaller group of records that the parties may have agreed to produce in the litigation or FOIA/PA request. ICE uses the privilege log to identify and justify the withholding of records and information, and the basis for such withholding, to other parties in the litigation. The search and filter report is used by ICE to document to other parties how ICE identified the records that are considered subject to production in the litigation or FOIA/PA request. The unique key is used by ICE to verify that the original documents loaded into EDSS were not altered. The audit trail may be used by OPLA supervisors, IT security personnel, ICE Office of Professional Responsibility investigators, or other offices with oversight responsibility for employee conduct or system security, to review the actions of EDSS users and to investigate any allegations or indications of system-related misuse or misconduct by such users.

ICE uses the production file generated by EDSS to produce releasable portions of records in electronic and searchable form to the DOJ to allow it to represent the United States' interests in the litigation, to other parties in litigation as required or agreed to in discovery, and to the court. ICE may use the production file in a FOIA/PA matter to provide this information to the ICE FOIA Office, which may then provide it to the FOIA/PA requester in paper or electronic form, depending on the requester's preference.

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.

EDSS does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

There are no other DHS component personnel with assigned roles and responsibilities within the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of unauthorized access to the information maintained in EDSS.

Mitigation: To mitigate this risk, EDSS employs appropriate role-based access controls so only authorized OPLA personnel have access to the system and to the individual cases in the system, based on their work assignments. OPLA supervisors decide which OPLA personnel are granted access to records stored under a particular EDSS case, what functions those personnel will be able to perform in the system, and even which records individual users may view or review. Additionally, all users receive training regarding the proper use of EDSS prior to being granted access to the system. All users also complete annual mandatory privacy and security training, which stresses the importance of appropriate and authorized use of personal data in government systems and the penalties for violations.

Section 4.0 Notice

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

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

As EDSS is not a primary information collection system, notice is not provided to individuals prior to EDSS's collection of information. Litigants in civil cases are likely to be generally aware that ICE may be compelled to search for and produce agency records pertaining to them and their claims during the litigation process. This PIA serves as notice to the general public as to the collection and use of information in EDSS for the purposes described in this PIA. With respect to the operation of EDSS, the DHS General Legal Records SORN provides notice of the records that may be collected by OPLA in the context of litigation and the DHS FOIA and Privacy Act Record System SORN provides notice of the

internal collection and processing of agency records in the context of FOIA/PA. ICE's other PIAs and SORNs also provide general notice to the public of the type of records and information ICE collects and maintains generally, which helps provide transparency as to the nature of the agency records which may be collected and loaded into EDSS for litigation or FOIA/PA purposes.

Prior notice at the point of original collection is provided where possible; however, in cases where the data collection supports an ICE law enforcement activity, opportunities for the individual to be notified of the collection of information may be limited or nonexistent. In some instances, a compulsory legal process such as a search warrant, court order, or subpoena is used to compel production of the materials to ICE and notice is usually required to be provided to the individual at least concurrently with the collection. Whether notice is provided highly depends on the purpose and context of the original collection of information.

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

As EDSS is not a primary information collection system, any right or opportunity to consent or decline to provide information occurs at the point of original collection from the individual and is described in the relevant PIA and SORN for that recordkeeping system, program, or activity from which the EDSS data are gathered. Because the litigation discovery process is compulsory upon ICE, ICE may have little or no discretion to control how records about individuals are disclosed, and may only request that the court limit public disclosure of EDSS information by placing the information under seal or obligating the other parties to not further disclose it without court permission.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals are not aware of the existence of EDSS and the data it collects and maintains.

Mitigation: This PIA serves as public notice of the existence of EDSS, the data it collects and maintains, and the limited purposes for which it is used. Because EDSS supports a secondary collection of information from records already compiled in existing agency recordkeeping systems, individualized notice is not possible or practical.

Section 5.0 Data Retention by the project

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

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

The information retained is the same as that collected, which is any ESI or other agency records that may be relevant to the matter. Records are retained in EDSS until the final resolution of the case, claim, or action causing the collection of the documents for processing within EDSS.

For civil litigation, final resolution means an administrative settlement of the claim or case, a dismissal with prejudice of all claims arising from the same subject matter, a final judgment on the case or claim, and the exhaustion of appeals, whichever comes last. In the event litigation was anticipated but never filed, but records were collected and uploaded to EDSS, those records will be stored only until the expiration of the appropriate statute of limitations, currently two (2) years from the date of injury for common law tort claims, or as long as the state statute of limitations mandates for constitutional claims. For common law tort claims, the statute of limitations requires an administrative claim to be submitted within two (2) years of the date of loss, after which the agency has six (6) months to adjudicate the claim. For constitutional tort claims, statutes of limitations vary from as little as two (2) years to as long as eight (8) years; the limitations are set by state law, and the laws of the fifty states vary between two (2) and six (6) years from the date of the injury.

For criminal litigation, EDSS records will be retained until final resolution. Final resolution means the dismissal with prejudice of all related charges, an acquittal of all related charges, or the exhaustion of appeals on all related charges.

ICE proposes to retain EDSS records gathered in response to a FOIA/PA request for two (2) years after date of reply, if access to all requested records is granted, or six (6) years after date of reply, if access to requested records is denied in whole or in part.

Retention of records gathered for input into EDSS: (1) Records on the secure shared drive will be deleted once it is confirmed that they have been properly uploaded into EDSS; (2) Copies of any hardcopy records received will be scanned and saved as a PDF document. The PDF document will then be uploaded to the secure shared drive. Upon successful upload into EDSS, the hardcopy records will be will be maintained in their original form by the ICE attorney with the case file until final resolution.

System administrators destroy all EDSS data in accordance with DHS guidance on the secure destruction of electronic information.

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: The information in EDSS will be retained for the timeframes that are appropriate to the purpose of the system. These timeframes allow ICE to properly respond to anticipated or actual civil litigation, criminal litigation, and FOIA/PA requests. Shorter timeframes could jeopardize the integrity of the discovery process in ongoing litigation, undermine an individual's rights in litigation or on appeal, and/or subject the agency and its employees to penalties for violating its obligation under federal discovery rules and the FOIA/PA.

Section 6.0 Information Sharing

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

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

Yes. ICE shares information stored and processed in EDSS with the DOJ and any outside agency requested to opine on or concur with the disclosure of responsive information during civil or criminal proceedings. Any information that is subject to discovery in litigation must be shared with the Department of Justice, the court, and opposing counsel to fulfill ICE's obligations and ensure that all parties to the litigation have fair and equal access to the evidence. The information may be disclosed in encrypted form via secure email or delivery of the data on portable storage media.

In the FOIA/PA context, the information stored and processed in EDSS may ultimately be shared with the FOIA/PA requester through the ICE FOIA Office to the extent the information is not subject to withholding under a FOIA/PA exemption or exception. The records may be shared with other agencies that own or originated the records or data contained therein, or otherwise have equities in the records or information, to determine whether the records are releasable or exempt. The information may also be shared with the Department of Justice in the event that the FOIA/PA requester files a lawsuit challenging the adequacy of the agency's response to the FOIA/PA request.

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

The purpose of the DHS General Legal Records SORN is to support the mission of the DHS Office of the General Counsel and DHS component legal offices, including OPLA, to provide the agency with legal services, including supporting the agency during litigation. The external sharing of the records in EDSS for the litigation-related uses described above is compatible with this purpose.

The purpose of the DHS FOIA and Privacy Act Records SORN is to support the gathering and processing of agency records in response to FOIA/PA requests from the public. The external sharing of the records in EDSS for the FOIA/PA-related uses described above is compatible with this purpose.

6.3 Does the project place limitations on re-dissemination?

No. EDSS is a document storage and processing tool only. It is expected that any records input into EDSS may need to be disclosed during litigation or during the processing or response to a FOIA/PA request, as described in Question 6.1 above. The re-dissemination of records processed through EDSS may not be discretionary for ICE and may be mandated by law. In civil and criminal discovery, all disclosure of EDSS information will be done through the Department of Justice and the courts. Limitations on the re-dissemination of information will generally be those described in the Privacy Act, the exemptions under FOIA/PA, the civil discovery privileges, court rules and orders, and agency policies limiting the re-dissemination of law enforcement sensitive information.

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

EDSS's audit trail captures actions associated with the creation of a production file. EDSS maintains an audit trail of the date and time when a production file was created, as well the user performing the action. EDSS does not track the recipients of the productions or whether it was further re-disseminated by third parties. However, in the event case information is provided to a third party, the production file will be saved in a format that identifies the third party recipient, case name, and the date the file was created.

For FOIA/PA matters, the ICE FOIA Office maintains separate records that document any disclosures made in response to a FOIA/PA request.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that disclosure of information collected in EDSS will be incompatible with the original purposes for which the information was collected.

Mitigation: This risk is mitigated by the fact that EDSS is used only to facilitate the agency's production of records as mandated by statute or federal court rules. Disclosures of records in litigation to which they are relevant, or as mandated by open records statutes such as FOIA/PA, support with the underlying democratic principles of fairness, transparency, and accountability.

Section 7.0 Redress

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

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

Individuals may request access to records about them in EDSS. 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 interests or if the information is compiled in reasonable anticipation of litigation. Providing individual access to records contained in EDSS could inform the subject of an actual or potential investigation or reveal investigative interest on the part of DHS. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

Because of the nature of EDSS as a repository for records gathered from other ICE recordkeeping systems pursuant to discovery obligations or open records laws, opportunities for the individual to correct inaccurate or erroneous information about themselves in EDSS are non-existent. Federal discovery rules and the FOIA/PA require the preservation and production of records in ICE recordkeeping systems, notwithstanding the accuracy of those records. ICE is not permitted to modify those records even if they contain inaccurate or outdated information. For this reason, the information in EDSS is exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests or if the information is compiled in reasonable anticipation of litigation. Permitting amendment of EDSS records could interfere with ongoing litigation, investigations and law enforcement activities.

Because information in EDSS is obtained from other ICE recordkeeping systems, individuals are able to request correction of any inaccurate or erroneous information in the source systems themselves, subject to any Privacy Act exemptions intended to prevent harm to law enforcement investigations or interests. Individuals seeking notification of and access to any record contained in EDSS or the source system, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

The procedure for submitting a request to correct information is outlined in this PIA in Questions 7.1 and 7.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have access or the ability to correct their information in EDSS.

Mitigation: Individuals can request access to information about them in EDSS through the FOIA/PA process and also have a right to seek correction of such information. The nature of EDSS and the information it collects and maintains is such that the ability of individuals to access or correct their information will be limited. Depending on the nature of records about them in EDSS, individuals may have the ability to access and correct information about them in the original agency recordkeeping system from which the EDSS records were retrieved.

Section 8.0 Auditing and Accountability

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

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

Certain user activities within EDSS's document review function are monitored and tracked by the creation of an audit trail. This audit trail can assist in identifying unauthorized use of the system so that appropriate follow up action may be taken. The audit trail tracks the specific action taken within the EDSS application (e.g., information on when users logged in and logged out of the system; search terms and the date and time they were executed; exports of metadata, native, and production files; printing of PDF and CSV files; tagging; and redactions), the user performing the action, the identity of ICE employees who are authorized to access a particular case, any changes to or redactions of data with EDSS, any determination that a document is privileged or PII using tags, and any information that is exported. Designated users, such as system administrators or OPLA supervisors, can access the audit trail. If an OPLA employee were to disclose EDSS information inappropriately, ICE management would be able to review this audit trail to determine the potential sources of the unauthorized disclosure and take appropriate corrective action. For matters in litigation, the supervision of the federal courts would be an additional control on the unauthorized disclosure, dissemination, or re-dissemination of PII or privileged information.

In all cases, access to EDSS data is limited to personnel assigned by OPLA managers to work on those matters. OPLA personnel will access EDSS from their ICE computers, which are password protected and have other security features such as automatic locking of the desktop after fifteen minutes of inactivity.

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

All ICE employees and contractors complete annual mandatory privacy and security training, specifically the Culture of Privacy Awareness Training and the Information Assurance Awareness Training. Additionally, all users receive on-the-job training regarding the proper use of EDSS.

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

OPLA managers in charge of teams and divisions responsible for litigation support assign ICE attorneys and paralegals to individual cases. The assigned attorneys and paralegals are responsible for assuring a complete and diligent discovery search, preservation, collection, and production of relevant records. They will have access to records gathered and input into EDSS for that particular litigation matter, along with the OPLA and OCIO personnel who serve as EDSS system administrators.

There are three user roles within EDSS: system administrator, super user, and end user.

(1) *System administrators* have full privileges to perform all functions in EDSS. System administrators can create user groups and grant customized levels of access and privileges to these groups and the users within them. Certain functions are reserved for the system administrator such as the ability to load and process ESI into an existing EDSS case, and to generate the production version of records in the system. System administrators can also assign users to any user role or group.

(2) *Super users*, by default, have more restricted privileges than system administrators. Super users can assign other super users and end users to user groups or assign them levels of access and privileges for particular EDSS cases. Super users may also access the audit trails in the system. Super users may not perform certain functions that are reserved for system administrators, such as loading records into EDSS. ICE supervisors will often be assigned the role of super user.

(3) *End users* have the most limited privileges in EDSS. End users may only access and take actions on those EDSS cases and/or records based on the levels of access and privileges they are granted and groups to which they are assigned by a system administrator or a super user. ICE attorneys and paralegals will usually be assigned the role of end user.

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?

Currently, the system owner (OPLA) does not have any information sharing agreements concerning this information, nor does it envision the expansion of the users of EDSS or the intended uses of the information collected and maintained in the system in such a way that an information sharing agreement would be required. In the event that such changes were considered, OPLA would engage the ICE Privacy Office to discuss the intended expanded users and/or uses of this information and update the relevant privacy compliance documentation (including this PIA) as appropriate.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security