Privacy Impact Assessment
for the

Electronic Discovery (eDiscovery)

DHS/FEMA/PIA-047
September 06, 2017

Contact Point
Jon Chase
Office of Chief Counsel
Federal Emergency Management Agency
(202) 646-3102

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

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) Office of Chief Counsel (OCC) uses a commercial off-the-shelf electronic discovery software tool (eDiscovery) to facilitate the production of documents and disclosure of existing FEMA records during litigation or in response to a request for records. eDiscovery is a document processing tool that supports the organization of paper and electronic documents for analysis, review, redaction, and production to meet litigation discovery requirements. FEMA also uses the system to process agency records in response to subpoenas and Touhy requests (written requests for agency records or official information made in accordance with agency regulations). FEMA is conducting this Privacy Impact Assessment (PIA) because eDiscovery collects, maintains, stores, and shares personally identifiable information (PII).

Overview

FEMA uses eDiscovery to support the review, redaction, and production of agency records to comply with discovery requirements during litigation and to provide responsive documents.[1] eDiscovery replaces the manual processes by which OCC gathers, sorts, reviews, and redacts agency records that are potentially responsive to a discovery, subpoena, or Touhy request;[2] assesses its relevance and/or responsiveness; and applies appropriate privileges in litigation.

FEMA increasingly relies upon electronically stored information (ESI) to conduct agency business. Accordingly, FEMA needs to use eDiscovery to review, redact, and produce agency records. In some cases, FEMA 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.[3] Additionally, OCC may scan paper documents into eDiscovery and review them, as it would an electronic document.

eDiscovery streamlines and automates the document review process. First, eDiscovery loads 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, eDiscovery allows OCC 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 the reviewing attorney inputs. This allows the reviewing attorney to customize

[1] By "responsive documents," FEMA is referring to agency records that are potentially responsive to a discovery, subpoena, or Touhy requests.
[2] *See* 6 C.F.R. §§ 5.41-5.49; 44 C.F.R. §§ 5.80-5.89.
[3] Metadata are the data attributes that may or may not be hidden that may reveal sensitive information about a document or file's history, such as its creator, last editor, or version history, among others.

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 then reviews and determines whether the files or information therein should be protected from disclosure. Finally, eDiscovery allows OCC to electronically redact protected portions of documents in the system.

eDiscovery has additional features that speed up the process by which OCC or other FEMA employees designate or redact the same protected information from multiple records. For example, eDiscovery allows for the bulk redaction of any words or terms, including names, or identifies for the attorney all occurrences of a keyword associated with a particular lawsuit so that the attorney can decide whether it is appropriate to redact each instance of that keyword as it appears in multiple records.

Background

FEMA acquired eDiscovery 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. eDiscovery is expected to significantly improve the efficiency of OCC's processing of records during discovery in litigation. OCC's discovery productions can require the preservation, collection, and analysis of tens of thousands of emails, word processing documents, Portable Document Format (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, given this volume of records, OCC cannot possibly review all documents for metadata and privileged information under this current process, and needs the automation eDiscovery brings. Many of the discoverable documents are duplicates, and because it is difficult to manually identify duplicates among voluminous records, OCC often wastes valuable time reviewing multiple identical documents. The automation of this process using eDiscovery dramatically reduces the time OCC spends on administrative tasks related to document management and improves the quality and efficiency of overall document review and production within OCC. Only a small amount of OCC personnel will receive access to the system: those involved in litigation, and those responding to responsive document requests.

Document Collection Process

In lawsuits, litigants typically begin the document review and production process after filing litigation against the agency or in a case in which the agency may have an interest (such as when a civil lawsuit is initiated against another federal agency involving a disaster in which FEMA participated). FEMA also may start gathering documents in anticipation of litigation based on circumstances that may give rise to litigation. Once OCC 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 OCC for review.

OCC may also use eDiscovery to respond to responsive document requests. For responsive document requests where FEMA is not a litigant, OCC gathers, reviews, and marks material as exempt, then produces the records to the requester. For litigious responsive document requests, OCC issues a litigation hold for relevant documents. Individual FEMA employees and technical support personnel then take action to preserve the evidence described by the litigation hold notice. These actions may include additional keywords that allow employees and technical support personnel to identify other relevant documents. OCC emails individual employees who may be custodians of requested information with separate litigation hold notices prohibiting them from deleting or destroying evidence, whether in paper or electronic form. The individual employees are not generally required to identify, harvest, and produce evidence until the case is in litigation and discovery commences. The requirements are dictated by the litigation itself.

When discovery commences, OCC notifies employees of their obligation to identify, harvest, and produce evidence to OCC. 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. OCC may require these technical support personnel 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, based on the needs of the attorney and requirements from the court, 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 will be downloaded to portable storage media or drives maintained on servers. In extreme cases, where an employee likely possesses a significant amount of ESI 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, Office of the Chief Information Officer (OCIO) personnel (local LAN Administrator Team, and cyber security) and OCC personnel, with the help of eDiscovery system administrators, transfer the data in electronic format to a secure shared drive on the FEMA network. The collection may include bulk scanning of paper documents into an electronic format, such as PDF or Tagged Image File Formats (TIFF), and preferably into a machine-readable format. Once all of the data is on the secure shared drive, a system administrator imports the data into eDiscovery. The system administrator deletes the data residing on the secured shared drive once he or she receives confirmation that the data has been successfully uploaded into eDiscovery. The FEMA attorney with the case file will maintain the hardcopy records in their original form. If litigation does not ensue, OCC lifts the litigation hold when the statute of limitations expires, or when OCC otherwise concludes that litigation is not

reasonably likely. FEMA will maintain or delete the records that were covered by the litigation hold, but never uploaded into eDiscovery, in accordance with normal agency retention policy, as set forth in any applicable records disposition schedules.

Document Review Process

eDiscovery supports 400 different file formats for review in a native viewer, avoiding the need for OCIO to install the application used to create the document onto the reviewing attorneys' computers. This also eliminates the necessity of converting documents into formats that OCC can view and redact using their current computer configurations, thereby reducing the risk that others will alter the documents and potentially violate federal evidentiary and discovery rules. eDiscovery can collect and process various formats such as TIFF, PDF files, JPEG images, and Microsoft Office documents. The documents loaded into eDiscovery are exact duplicates of existing data that are already stored in other FEMA paper or electronic recordkeeping systems. FEMA maintains the documents it loads into eDiscovery in their original, unmodified form. eDiscovery does create new information that is associated with those records, and using eDiscovery does not alter the integrity of the original records themselves. The eDiscovery-created data consists of redactions;[4] tags; privilege logs[5] created by the eDiscovery software; search and filter reports; and an audit trail, which eDiscovery automatically creates and maintains as an historical record of all actions users take in each case. eDiscovery also assigns a unique key to the original unaltered file, which helps establish the chain of custody as proof that no one altered the content of the produced file or the original version of the document.

eDiscovery receives uploaded records in a new "case" that it creates for a particular litigation. The OCC supervisory attorney for that litigation manually grants eDiscovery privileges to the attorneys and paralegals assigned to that litigation, allowing them to access and review the documents. During the review process, attorneys may narrow the scope of documents reviewed by executing searches and filtering data, generally using search terms agreed between the litigants. As part of this initial review, eDiscovery automatically identifies and removes duplicate documents from the collection of data in the eDiscovery repository.[6] Attorneys and paralegals then review the subset of documents resulting from the search and filter and place tags on specific documents to classify and categorize those documents. In addition, they redact protected or privileged information. For each document, OCC may enter free-form text describing the reason for the redaction.

[4] Redactions are not considered alterations of the documents in eDiscovery. They merely hide information that should not be produced to opposing parties.
[5] A privilege log lists the location and basis of each redaction or withholding, cross-referencing each redaction to a specific page number within the production.
[6] De-duplication is based on the use of hash values. eDiscovery assigns all records a hash value based on a combination of the content of the file and the metadata associated with the record. eDiscovery maintains only one copy of records that have identical hash values.

Using this information, eDiscovery generates a privilege log to document the redactions or withholding of records on the basis of privilege. OCC typically shares this privilege log with the U.S. Department of Justice (DOJ), with other parties in the litigation, and sometimes with the court. eDiscovery can also generate reports based on the search terms and filters that were used to withhold records. OCC produces the search report to opposing parties to demonstrate a defensible process for gathering the totality of relevant data, as agreed upon between the parties. The presiding judge may also order OCC to produce search reports. 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, as warranted by the case.

Once the review is complete, FEMA attorneys place the reviewed records in a production folder in eDiscovery 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 from the court. Production file formats are typically image files, such as PDFs and TIFFs. While redactions in eDiscovery are temporary (*i.e.*, the eDiscovery 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. eDiscovery still retains a copy of the original records with only temporary redactions, which allows OCC to change the redactions if needed. The originals are also retained, should FEMA need to produce the same records again in cases where the parties' agreement or a court order requires FEMA to produce previously redacted information from those records or change the redactions. Files in any format included in the production file may contain PII data, unless FEMA attorneys redact it prior to production.

Before production, the system administrator extracts the production file from eDiscovery, encrypts it, and then writes it to an external portable storage device, such as a CD-ROM,[7] for transfer to the recipient. Once documents are sent to DOJ, and eventually to the court and opposing counsel, the OCC attorney will "close" the case, and OCC and system administrators will delete the matter from eDiscovery and save an archive file of the matter on regular FEMA-OCC drives.

[7] The CD-ROM is the most-used external portable storage medium for the transfer of large files in FEMA. There is no standardized process for deciding to use a CD-ROM over other external portable storage devices. However, nothing here precludes the use of other external portable storage devices for this purpose.

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, Federal Rules of Civil Procedure 16, 26, 34, and 37 govern most electronic discovery requirements, which the federal courts may enforce. In criminal cases, courts can compel full and open discovery of agency records via the Fifth and Sixth Amendments to the U.S. Constitution and the Federal Rules of Criminal Procedure. For subpoenas and Touhy requests, Rule 45 of the Federal Rules of Civil Procedure and the Administrative Procedure Act[8]mandate the disclosure requirements.

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[9] applies to eDiscovery data gathered in the context of litigation. Specifically, the DHS General Legal Records SORN covers all agency records that are potentially responsive to a discovery, subpoena, or Touhy requests. In addition, the DHS General Information Technology Access Account Records System SORN[10] covers access to DHS information technology systems and resources by authorized individuals.

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

The eDiscovery system is currently in the Certification and Accreditation (C&A) process. The Authority to Operate (ATO) date for the system is pending completion of this PIA.

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

eDiscovery litigation case files are retained under NARA-approved retention schedule N1-311-86-1, Item 1F2, *Official Litigation Case Files*.

---

[8] 5 U.S.C. § 500 *et seq.*
[9] DHS/ALL-017 Department of Homeland Security General Legal Records, 76 FR 72428 (November 23, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-11-23/html/2011-30175.htm.
[10] DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792 (November 27, 2012), *available at* https://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Because the records are already in FEMA's possession and not collected from sources outside of FEMA, eDiscovery is not covered by the PRA.

Section 2.0 Characterization of the Information

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

eDiscovery stores and processes agency records, as necessary, to satisfy litigation discovery requirements and to respond to responsive document requests. Information in eDiscovery could consist of any ESI or other information in any FEMA formal or informal recordkeeping system or any paper documents scanned into an electronic format for review. In some cases, if a responsive document request asks FEMA to provide records in the possession of DHS or other DHS components, FEMA personnel may process those records through eDiscovery.

Because eDiscovery is a document processing tool, the ESI and other records that may be stored and processed in eDiscovery could pertain to any matter in the scope of DHS or FEMA's mission and may contain PII of any nature captured and stored in such records. For civil litigation that is reasonably likely or pending, eDiscovery may collect and maintain any information that is potentially relevant to the matter for discovery purposes. To determine whether a document is "potentially relevant," OCC attorneys generally review the case's history to gain an understanding of the litigation itself, review search terms, and read the documents to determine if they may be responsive to the litigation. To the extent it is applied in the processing of non-litigious responsive document requests, eDiscovery may store and process any agency records that are potentially responsive to those requests. The actual information stored and processed in eDiscovery will always vary and depend on the nature of the particular litigation or responsive document request.

The types of individuals about whom information could be collected in eDiscovery varies on a case-by-case basis, but may include any of the following: anyone involved in litigation with DHS, applicants for Individual Assistance, persons who file responsive documents requests asking for FEMA records, persons who correspond with DHS or FEMA, employees and contractors of DHS and other federal agencies, witnesses and other sources of information, attorneys and authorized representatives, subjects of investigations, 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 FEMA or DHS.

Listed below are examples of general types of records that eDiscovery may store or process:

- **Electronic mail:** messages among FEMA employees, or among FEMA employees and personnel of other federal agencies or outside entities, sometimes with other documents attached;
- **Presentations:** documents such as PowerPoint presentations;
- **Spreadsheets**: typically data collections or tracking of broad information such as aggregate expenditures during a disaster;
- **Database entries:** information collected or compiled from program databases such as National Emergency Management Information System - Individual Assistance (NEMIS-IA) or Emergency Management Mission Integrated Environment (EMMIE), which could contain PII; and
- **Miscellaneous:** letters, memoranda, drafts, and receipts.

Electronic documents eDiscovery stores and maintains may also contain metadata, which may contain PII (*e.g.*, the name of the author of a particular electronic file), which itself may be discoverable in litigation or by a responsive document request. As described in the Overview, eDiscovery 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.

FEMA records may contain the following information from:

System Users

- Identity Credential/Access Management certificate and Personal Identity Verification code

Members of the Public

- Contact information (name, address, phone number, email address);
- Correspondence;
- Applications for assistance and associated files;
- Insurance applications and associated files;
- Survivor medical information;

- Other financial records; and
- Family information, including information about minors.

**it is possible that an array of PII/SPII may be contained within the above documents*

FEMA Employees/Contractors

- Contact information (name, address, FEMA phone number, email address);
- Emails;
- Memos;
- Correspondence;
- Personnel files; and
- Records generated that are related to active FEMA litigation including but not limited to reports, analysis, guidance, training materials, charts, or photography.

**it is possible that an array of PII/SPII may be contained within the above documents*

Employees of other Federal Agencies

- Contact information (name, address, phone number, email address);
- Emails;
- Memos;
- Correspondence; and
- Records or documents related to active FEMA litigation including but not limited to reports analysis, guidance, training materials, charts, or photography.

**it is possible that an array of PII/SPII may be contained within the above documents*

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

eDiscovery may store and process data from any FEMA record keeping system. The nature of those records varies and may include Individual Assistance application files, Public Assistance requests, and associated project worksheets with relevant information, personnel and employment records, financial records, etc. The source of such records varies depending on the type of activity the record is created to support. Any of these records may also contain metadata, which is typically

generated by the source system. Because eDiscovery can contain any records that FEMA receives, creates, or maintains, it is not possible to list all of the possible sources of information for those records.

FEMA personnel originally gather the potentially relevant documents pursuant to direction from OCC (or Disclosure Branch) to produce material in anticipation of 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 information has been identified and litigation ensues, OCIO personnel and OCC personnel, with the help of eDiscovery System Administrators, transfer the data to eDiscovery.

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

eDiscovery could contain commercial or publicly available data only to the extent that it is already contained in the records loaded into the eDiscovery repository for litigation and responsive document requests. Commercial or publicly available information typically appears in contract documents, grant documents, and other similar documents. The commercial and publicly available data is merely a category of data that could be included in the records input into eDiscovery for review. Because FEMA does use commercially-sourced data and publicly available data in executing its mission, it is possible that such data may be included in eDiscovery.

2.4 Discuss how accuracy of the data is ensured.

eDiscovery operates under the principle of full and open discovery of whatever information exists in FEMA recordkeeping systems. FEMA 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, federal statutes, and as authorized by the court. Federal discovery rules require the preservation and production of records in FEMA 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: eDiscovery could present a risk of the over-collection of PII or the aggregation of disparate PII from separate agency recordkeeping systems.

Mitigation: FEMA cannot fully mitigate this risk. FEMA only collects and aggregates information in eDiscovery when it is under a legal mandate to respond to discovery and other

responsive document requests. The agency does not have discretion to limit the scope of the collection. OCC mitigates this risk by only using the system to support the review and production of records in litigation and other responsive document requests. OCC limits role-based access to the information in eDiscovery to those FEMA attorneys and paralegals assigned to those matters, and eDiscovery generates a robust audit trail of all user activity, including the viewing of records in the system.

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

Mitigation: Due to the nature and use of the system, FEMA cannot fully mitigate this risk. FEMA does not use the information in eDiscovery to make decisions about individuals. The system contains only copies of records from other agency recordkeeping systems, and FEMA will not use eDiscovery as an internal source of agency records about individuals. The purpose of eDiscovery is to support the mandatory production of agency records in pending litigation. Federal disclosure laws require production of documents in their original form, even if they contain erroneous, incomplete, or outdated information. Incorrect information can be corrected in the source system. However, active litigation may prevent the correction of the information because federal disclosure laws require production of documents in their original form, which must be maintained throughout the litigation.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FEMA uses the information loaded into eDiscovery to support the mandatory production of agency records in pending civil or criminal litigation and in response to responsive document requests.

FEMA uses the production file generated by eDiscovery to produce releasable portions of records in electronic and searchable form to the DOJ to allow it to represent the United States' interests in litigation, to other parties in litigation as required or agreed to in discovery, and to the court. FEMA may also use the production file to respond to responsive document requests.

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.

eDiscovery does not conduct predictive pattern or anomaly analysis.

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 and use of the information maintained in eDiscovery.

Mitigation: To mitigate this risk, eDiscovery employs appropriate role-based access controls so only authorized OCC personnel[11] have access to the system and to the individual cases in the system, based on their work assignments. OCC supervisors decide which OCC personnel are granted access to records stored under a particular eDiscovery case, what functions those personnel will be able to perform in the system, and which records individual users may view or review. Users will only have access to the cases assigned to them. Additionally, all users receive training regarding the proper use of eDiscovery 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.

Privacy Risk: There is a privacy risk that information in eDiscovery may be used for purposes beyond litigation.

Mitigation: This risk is mitigated. The only time that information would be uploaded into eDiscovery would be when a litigation hold has been issued for a particular matter. No agency records are uploaded into eDiscovery unless it is in anticipation of litigation. Moreover, there is a detailed audit log maintained by eDiscovery that would capture any user's inappropriate access or viewing of information contained within eDiscovery. These logs are automatically generated by eDiscovery, and are reviewed by OCC and cyber security when there is evidence or reason to believe that the integrity of the data has been compromised.

[11] Administrative support personnel will have access to the system, but not to the cases.

Section 4.0 Notice

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

As eDiscovery is not a primary information collection system, FEMA does not provide notice to individuals prior to eDiscovery's collection of information. Litigants in civil cases are aware that courts may compel FEMA 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 eDiscovery for the purposes described in this PIA. With respect to the operation of eDiscovery, the DHS General Legal Records SORN[12] provides notice of the records that may be collected by OCC in the context of litigation. FEMA's other PIAs and SORNs also provide general notice to the public of the type of records and information FEMA collects and maintains generally, which helps provide transparency as to the nature of the agency records which may be collected and loaded into eDiscovery.

FEMA provides notice at the point of original collection where possible; however, in cases where the data collection supports a law enforcement activity, opportunities for the individual to be notified of the collection of information may be limited or nonexistent. For example, FEMA's SORNs allow for the sharing of records to appropriate federal, state, local, tribal, international, or foreign government law enforcement agencies charged with investigating, enforcing, implementing, or prosecuting a law when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law. In these circumstances, notice has already been provided via the SORNs; FEMA will not provide additional notice to affected individuals. In some instances, litigants use a compulsory legal process such as a search warrant, court order, or subpoena to compel FEMA to produce documents. For these cases, FEMA will provide notice to the individuals at least concurrently with the collection, as required by the courts. The purpose and context of the original collection of information determines whether notice is provided.

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

As eDiscovery 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 eDiscovery data are gathered. Because responsive document requests are compulsory upon FEMA, FEMA may have little or no discretion to control how records about

[12] DHS/ALL-017 Department of Homeland Security General Legal Records, 76 FR 72428 (November 23, 2011).

individuals are disclosed, and may only request that the court limit public disclosure of eDiscovery information by placing the information under seal or obligating the other parties to not further disclose it without the permission of the court.

4.3 Privacy Impact Analysis: Related to Notice

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

Mitigation: This risk cannot be fully mitigated. This PIA serves as public notice of the existence of eDiscovery, the data it collects and maintains, and the limited purposes for which FEMA will use the data. However, because eDiscovery 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

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

FEMA retains records in eDiscovery until the final resolution of the case, claim, or action causing the collection of the documents for processing within eDiscovery. eDiscovery litigation case files are retained in accordance with NARA-approved retention schedule N1-311-86-1, Item 1F2, *Official Litigation Case Files*.

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, or the exhaustion of appeals, whichever comes last. In the event litigation was anticipated but never filed, but OCC collected and uploaded records to eDiscovery, FEMA will store those records 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, FEMA will retain eDiscovery 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.

All records will be maintained pursuant to the records retention schedules for the source systems' documents, and as dictated by the courts. Due to the storage limits within eDiscovery, the records that are uploaded to and processed in eDiscovery will be deleted from eDiscovery after processing and production.

Retention of records gathered for input into eDiscovery: (1) Records on the secure shared drive will be deleted once it is confirmed that they have been properly uploaded into eDiscovery; (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 eDiscovery, the FEMA attorney with the case file will maintain the hardcopy records until final resolution.

System administrators destroy all eDiscovery 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: FEMA maintains the records in eDiscovery according to the records schedules and policies discussed in Section 5.1, and disposes of them accordingly. Normally, FEMA's Records Management Division (RMD) would notify OCC that records are eligible for destruction. OCC would then certify that the records can be destroyed, and RMD then would grant OCC permission to destroy. However, due to the storage limits within eDiscovery, the records that are uploaded to and processed in eDiscovery will be deleted from eDiscovery after processing and production. Occasionally, there will be times where records are kept in the system due to ongoing litigation. To ensure that storage limits aren't reached, users will receive periodic housekeeping notices to ensure users review any maintained files to delete those no longer needed.

Section 6.0 Information Sharing

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

Yes. FEMA shares information stored and processed in eDiscovery with the DOJ and any outside federal agency asked to consult on or concur with the disclosure of responsive information during civil or criminal proceedings. FEMA does so in accordance with routine uses in the SORNs listed in Section 1.2. Moreover, FEMA must share any information that is subject to discovery in litigation with the DOJ, the court, and opposing counsel to fulfill FEMA's obligations and ensure

that all parties to the litigation have fair and equal access to the evidence. FEMA discloses the information in encrypted form via secure email or delivery of the data on portable storage media.

For responsive document requests, FEMA may ultimately share the information stored and processed in eDiscovery with the requester through FEMA's Disclosure Branch to the extent the information is not subject to withholding under an exemption or exception. FEMA may share the information 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. FEMA may also share the information with the DOJ in the event that the requester files a lawsuit challenging the adequacy of the agency's response to the request.

For subpoenas and Touhy requests where FEMA is not a party, FEMA shares the information stored and processed in eDiscovery with the requesting party, and any other parties as required by the court under pursuant to 5 U.S.C. § 552a(b)(11). FEMA does not share this information without a privacy waiver or an order from a court of competent jurisdiction.

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

The DHS General Legal Records SORN supports the mission of the DHS Office of the General Counsel and DHS component legal offices, including OCC, to provide the agency with legal services, including supporting the agency during litigation. The external sharing of the records in eDiscovery for the litigation-related uses, as well as subpoena and Touhy request uses, described above is compatible with Routine Uses A and H in of that SORN.

6.3 Does the project place limitations on re-dissemination?

No. eDiscovery is a document storage and processing tool only. FEMA expects to disclose any records input into eDiscovery during litigation or during the processing of responsive document requests. The re-dissemination of records processed through eDiscovery may not be discretionary for FEMA and may be mandated by law. In civil and criminal discovery, FEMA discloses eDiscovery information through the DOJ and the courts. Limitations on the re-dissemination of information will generally be those described in the exemptions under open records statutes, 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.

eDiscovery's audit trail captures actions associated with the creation of a production file. eDiscovery maintains an audit trail of the date and time when a production file was created, as well as the user performing the action. In the event case information is provided to a third party,

FEMA will save the production file in a format that identifies the third party recipient, case name, and the date the file was created.

For all other document requests, FEMA's Disclosure Branch maintains separate records that document any disclosures made in response to such requests.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: FEMA only uses eDiscovery to facilitate the agency's production of records as mandated by statute or federal court rules, and responsive document requests. Disclosures of records in litigation to which they are relevant, or as mandated by open records statutes, support the underlying democratic principles of fairness, transparency, and accountability. Any information sharing is done pursuant to Routine Uses A and H in the DHS General Legal Records SORN.

Section 7.0 Redress

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

Individuals may request access to records about themselves in eDiscovery. 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 FEMA compiled the information in reasonable anticipation of litigation. Providing individual access to records contained in eDiscovery could inform the subject of an actual or potential investigation or reveal an 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, tamper with witnesses or evidence, and avoid detection or apprehension.

Individuals seeking access to any record contained in this system of records may submit a Privacy Act (for U.S. citizens and Lawful Permanent Residents) or Freedom of Information Act (FOIA) (for all individuals) request to FEMA's Disclosure Office by visiting https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form.

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

Because of the nature of eDiscovery as a repository for records gathered from other FEMA recordkeeping systems pursuant to discovery obligations or open records laws, the system is not

designed to allow the individual to correct inaccurate or erroneous information about themselves in eDiscovery. Federal discovery rules require the preservation and production of records in FEMA recordkeeping systems, notwithstanding the accuracy of those records. FEMA is not permitted to modify those records even if they contain inaccurate or outdated information. For this reason, the information in eDiscovery 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 eDiscovery records could interfere with ongoing litigation, investigations, and law enforcement activities.

Because information in eDiscovery is obtained from other FEMA 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 to contest the content of a record may submit a Privacy Act 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 Sections 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 eDiscovery.

Mitigation: This risk cannot be mitigated. While individuals can request access to information, and correct information, about themselves in the system from which their information was originally collected, and seek correction of such information in that system, the nature of eDiscovery and the information it collects and maintains is such that the ability of individuals to access or correct their information is non-existent.

Section 8.0 Auditing and Accountability

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

FEMA will use eDiscovery's audit trail to monitor and track document review functions, as needed. This audit trail can assist investigating officials in identifying unauthorized use of the system so that FEMA may take any appropriate follow-up actions. The audit trail tracks the following within the eDiscovery application:

- Information on when users logged in to 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 all files;
- Tagging (for example, PII);
- Redactions;
- The user performing the action;
- The identity of FEMA employees authorized to access a particular case;
- Any changes to or redactions of data within eDiscovery;
- Any determination that a document is privileged;
- Any information that is exported.

Designated users, such as system administrators or OCC supervisors, can access the audit trail. If an OCC employee were to disclose eDiscovery information inappropriately, FEMA management would be able to review this audit trail to determine the potential sources of the unauthorized disclosure and take appropriate corrective action. For litigation matters, the federal courts would be an additional control regarding the unauthorized disclosure, dissemination, or re-dissemination of PII or privileged information. eDiscovery generates the audit log automatically.

Authorized FEMA personnel access eDiscovery from their FEMA computers, which are encrypted and password protected and have other security features such as automatic locking of the desktop after 15 minutes of inactivity. In all cases, OCC managers control who may access eDiscovery data.

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

All FEMA 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 eDiscovery, which will include privacy information. FEMA will also provide instruction manuals for general use and best practices of using the system.

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

OCC supervisory attorneys in charge of teams and divisions responsible for litigation support assign FEMA 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 inputted into eDiscovery for a particular litigation matter, along with the OCC and OCIO personnel who serve as eDiscovery system administrators.

There is no standardized process for revoking access. Those who have received access will not have their access revoked after a case is completed because of the likelihood of future litigation matters. Users will have access revoked in rare circumstances, such as when an employee transfers to a different department or leaves FEMA. While users will retain access to eDiscovery, they will only be able to access the cases assigned to them.

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

(1) *System administrators* have full privileges to perform all functions in eDiscovery. 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 eDiscovery 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 eDiscovery cases. Super users may also access system audit trails. Super users may not perform certain functions that are reserved for system administrators, such as loading records into eDiscovery. FEMA supervisors will often be assigned the role of super user.

(3) *End users* have the most limited privileges in eDiscovery. End users may only access and take actions on those eDiscovery 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. FEMA 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 (OCC) does not have any information sharing agreements concerning this information, nor does it envision the expansion of the users of eDiscovery or the intended uses of the information collected and maintained in the system in such a way that would require an information sharing agreement. In the event it considers such changes, OCC would engage the FEMA Privacy Branch 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

William Holzerland
FEMA Privacy Officer
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security