Privacy Impact Assessment
for the

Electronic Document and Records Management System (EDRMS)

DHS/FEMA/PIA–053

August 24, 2018

<u>Contact Point</u>
Bridget Hutchins
Federal Emergency Management Agency (FEMA)
Federal Insurance and Mitigation Administration (FIMA)
(202) 646-3612

<u>Reviewing Official</u>
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) Federal Insurance and Mitigation Administration (FIMA) owns and operates the Electronic Document and Records Management System (EDRMS). FIMA uses EDRMS for document management and record management. FIMA also uses EDRMS for conversion of paper documents to an electronic format in compliance with the National Archives and Records Administration (NARA) requirements, Office of Management and Budget (OMB) management of Federal records guidance and regulations, and Executive Directives. EDRMS is used as central storage of FIMA documents that are electronically scanned and that are not stored in other FIMA information technology (IT) systems. FEMA is conducting this Privacy Impact Assessment (PIA) because EDRMS collects, disseminates, retrieves, and maintains FIMA documents and copies of records with personally identifiable information (PII) from FIMA organizations.

Overview

FIMA's mission is to increase the capabilities necessary to reduce loss of life and property by lessening the impact of disasters. These capabilities include, but are not limited to, community-wide risk reduction projects; the transfer of flood risk through insurance; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred. In 2012, NARA and OMB issued a directive to reform federal records management in response to a 2011 presidential memorandum on managing government records. In accordance with OMB Memorandum M-12-18 (OMB M-12-18),[1] documents and records must be managed in an electronic format. This allows FIMA to convert paper documents and records into electronic form and to store, retrieve, and use electronic documents and records to accomplish their mission and support communities. FIMA's conversion of paper documents for storage in EDRMS complies with OMB M-12-18.

FIMA uses the EDRMS for FIMA document management (i.e., process of managing and tracking documents), record management (i.e., process of controlling and governing records through their life cycle), converting paper documents to an electronic format in compliance with OMB M-12-18, and as central storage of electronically scanned FIMA documents that are not stored in other FIMA IT systems.

[1] *See* OMB Memorandum M-12-18, Managing Government Records Directive, *available at* https://www.archives.gov/files/records-mgmt/m-12-18.pdf.

EDRMS is an operational system which uses a commercial-off-the-shelf application that provides standardized document and record life cycle management and an approved access control process for documents and records stored in the EDRMS. EDRMS uses the following electronic document and record store functionalities: a) searches using document or record metadata, b) centralized storage of documents and records, c) indexing of documents and records, d) storage of metadata in a database associated with the document and record electronic data store, and e) formatted/structured titling of the records and documents in the classification plan.

EDRMS functionality increases accessibility and reduces time needed to archive and retrieve records. Documents are submitted to EDRMS for storage by the following FIMA directorates and offices: the Risk Management Directorate, Mitigation Directorate, Fund Management Directorate, Federal Insurance Directorate, the Office of Environmental Planning and Historic Preservation, FIMA Legal Division, FIMA Flood Insurance Advocate, and FIMA Office of the Associate Administrator.

The documents in EDRMS originate from the aforementioned directorates and offices and may contain PII. EDRMS also includes PII such as FEMA user's username in the record's metadata and its audit logs.

EDRMS is accessible only by FIMA employees and contractors within FEMA's Enterprise Network (FEN) and is not accessible by the public. The EDRMS Regional Administrator and the System Owner authorize access to EDRMS records and documents based on the EDRMS user's position and region. Authorized FIMA users access EDRMS after successful authentication by the FEMA Enterprise Identity Management System (FEIMS) Single Sign-On (SSO) process using their Personal Identity Verification (PIV) cards. EDRMS includes functionality that restricts access to documents and data based on the user's position and region. All user activity is logged and reviewed by the operating system administrator and the Information System Security Officer (ISSO).

FIMA employees and contractors are not currently required to use EDRMS, however, EDRMS does comply with OMB M-12-18 for FIMA and will become the system for all FIMA users to upload documents for longer storage and for the life cycle of documents/records by December 31, 2019. If a FIMA employee chooses to use EDRMS, FIMA EDRMS users either directly upload or scan and upload records and documents into EDRMS that FEMA usually stores on its SharePoint sites, email system, or shared drive. All of FIMA's related documents and records are not stored with EDRMS. EDRMS contains the following electronic documents and records: 1) Community files (i.e., regional transactions and correspondence between the communities and the states); 2) Community Assistance Contacts (CAC); 3) Community Assistance Visits (CAV); 4) Ordinances; 5) FEMA correspondence (internal to FEMA); 6) general correspondence (external); 7) State correspondence; 8) Letters of Map Amendment (LOMA); 8) Risk Management; and 9) Hazard Mitigation Assistance (HMA) Grant, Public Assistance (PA) Grant, and Disaster Loan documents and records. The following records may contain information about Mitigation Grant applications into EDRMS: Office of Environmental Planning and Historic Preservation (OEHP) documentation, State-Level Mitigation acquisitions, and Flood Elevation and Floodproofing declarations. FIMA-related documents and records in EDRMS may include information about individual members of the public such as name, address, flood insurance policy information, and phone number information. This information is in the body (text) of the document or record and is not included in the record metadata. FEMA/FIMA personnel name may be stored in the document or records metadata to track who added the document or records into the system.

EDRMS uses record types to categorize documents and records. A record type defines the default attributes for the different types of information items that an organization wants to manage. Every FIMA document or record in EDRMS is categorized as one of the following FIMA record types: FEMA Region (I - X) and Headquarters. Regions IV and VI have the following additional record types: 1) Acquisition, 2) Hazard Mitigation Grant Program (HMGP), 3) Non-Disaster Grants, and 4) Technical Assistance. Each FIMA record type has one record entry form the EDRMS user completes when entering the documents and records into EDRMS. The record entry form data is stored as metadata with the document or record.[2]

An EDRMS user can retrieve information from the stored documents by executing a 'Document Content Search,' whereby all or part of the information is known and is in the search criteria.[3] The type and amount of PII present in the document is dependent on the record.

FIMA retains and makes available records requested by FIMA personnel and contractors through EDRMS. Records that are in the EDRMS are preserved according to the retention policy. The formal point of contact is responsible for securing the record or document. The record or document may contain a community identification number (CID). The classifications in EDRMS are a general description of the FEMA records disposition schedule.

There are existing Systems of Records Notices (SORN) and Routine Uses for the source systems from which these records are pulled. The existing SORNs cover the records maintained within the EDRMS system. The originating FIMA directorate, FIMA office, or the Office of Chief Counsel are responsible for identifying PII within their documents submitted for storage and the identification of the correct General Records Schedule (GRS). EDRMS functionality provides its users with different mechanisms for managing documents and records throughout the life cycle of the document or record.

[2] Metadata is information about the individual document or record which distinguishes it as a unique object from other documents or records in EDRMS.

[3] For example, Document Content Search = "Sarah Jones" AND "Connecticut" returns every document or record the user has access to that contains the words Sarah Jones and Connecticut in the text of the document.

EDRMS Record and Document Life Cycle

The EDRMS record and document life cycle consists of 1) Add or Remove; 2) Capture and Organize Phase; 3) Use and Maintain; 4) Retain and Appraise; and 5) Dispose phases.

Add or Remove Phase

FIMA receives the record or document. The recipient, a FIMA employee or contractor, sends documents for storage to an EDRMS user either electronically or in hard copy.

Capture and Organize Phase

Hard copy documents are scanned and converted to a pdf document for storage in EDRMS. Electronic documents are uploaded for storage in EDRMS. The EDRMS user completes the record entry form, which includes the classification, also known as the file plan, for the record or document. The classification is prepopulated based on FIMA's record series.

Use and Maintain Phase

EDRMS users can search for records and documents using any field in the EDRMS record entry form or any word within the pdf documents. As an example, the EDRMS document content search function could be used to search for any word within a pdf document, a policy number, a name within the document, or a property address. One use of the search function is to support the record searches in response to Freedom of Information Act (FOIA) requests.

Retain and Appraise Phase

Records and documents are retained based on FEMA's record retention and disposition schedules that have been approved by NARA and the FEMA Records Officer. The retention and disposition schedule is added to the record or document based on the selected classification (i.e., file plan). The FIMA program office's EDRMS user updates the system with a record's specific records retention and disposition schedule.

Disposal Phase

Records and documents are eligible for disposal based on the record retention and disposition schedule for the record or document. The records or documents are disposed in accordance with the disposal schedule. EDRMS has the capability to provide a forecast for items approaching their disposition date. The EDRMS System Owner uses the system to generate a report for documents and records that have reached their scheduled disposition time. The EDRMS System Owner or his or her designee destroys the records within EDRMS based on the above disposition report. EDRMS retains the record entry form data, including the date the record was destroyed within the system. Records and metadata are destroyed in accordance with the NARA disposition schedule Record disposition includes both destruction and transfer of Federal records to NARA and specific record dispositions as defined in FEMA's Record Disposition Schedule (i.e., FEMA Manual 141-1-1b).

EDRMS Typical Transaction

Typically, an individual of the public sends correspondence to FEMA regarding the National Flood Insurance Program (NFIP). A Federal Insurance Directorate (FID) employee or contractor receives the NFIP correspondence by way of an email or postal carrier. The employee or contractor signs into EDRMS as a system user using the EDRMS application that they have downloaded onto their FEMA laptop. The EDRMS user scans, uploads, and classifies the document or record in EDRMS. The EDRMS user classifies the documents or records as an NFIP record. Other EDRMS users with a need to know, as determined by the Regional Administrator and approved by the system owner, can access and use the records for NFIP business. Later, in accordance with the records retention schedule embedded in the classification of the document, the EDRMS System Owner designee manually deletes the record from the EDRMS.

EDRMS security mechanisms and security procedures were implemented and assessed based on the National Institute Standards and Technology (NIST) Special Publication (SP) 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans;[4] NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations;[5] NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;[6] and DHS Sensitive Systems Policy Directive 4300A.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The following authorities allow for the collection of information in EDRMS. They ensure a greater accountability of agency records, allow for transparency of agency records, and meet the mandates for a transition from paper records to electronic records management. An EDRMS user can create a list of records eligible for destruction, based on the record file plan. Additionally, legal holds/freezes can be placed on or removed from specific records in a timely and compliant manner.

- The Homeland Security Act of 2002[7] created the Department of Homeland Security and authorizes FEMA under its auspices;

[4] *Available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.
[5] *Available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[6] *Available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.
[7] 6 U.S.C. §§ 313-314, *available at* https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

- 5 U.S.C. § 301, Departmental Regulations, authorizes the head of an Executive department to prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.
- Section 408 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act[8] authorizes FEMA, as the designee of the President of the United States, to provide federal assistance to individuals and households.
- The E-Government Act of 2002[9] requires enhancements to improve the performance of governments in collaborating on the use of information technology to improve the delivery of government information and services.
- The National Flood Insurance Act of 1968, as amended,[10] establishes the legal authority for the administration and marketing of the NFIP.
- 31 U.S.C. § 7701(c) (1)[11] and Executive Order 13478[12] confer the authority to collect Social Security numbers (SSN).[13]
- The Federal Records Act of 1950, as amended, 44 U.S.C. §§ 21, 29, 31, and 33, requires responsible records management including the creation, retention, and disposal of records.

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

All information collected and stored within the EDRMS system is consistent with the following SORNs:

- GSA/GOVT-4 Contracted Travel Services Program[14] covers federal official travel

[8] 42 U.S.C. § 5174, *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-sec5174.pdf.
[9] Pub. L. 107-347, 116 Stat. 2899 (2002), *available at* https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.
[10] 42 U.S.C. § 4001 et seq., *available at* https://www.fema.gov/media-library-data/20130726-1752-25045-9854/frm_acts.pdf.
[11] *Available at* https://www.gpo.gov/fdsys/pkg/USCODE-2010-title31/pdf/USCODE-2010-title31-subtitleV-chap77-sec7701.pdf.
[12] Executive Order 13478, "Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers," 73 FR 70239 (November 20, 2008), *available at* https://www.gpo.gov/fdsys/pkg/WCPD-2008-11-24/pdf/WCPD-2008-11-24-Pg1431.pdf.
[13] Older attachments within EDRMS may contain SSN; however the new SOP for entering data and attaching documents requires the redaction of SSNs. Additionally, the Rules of Behavior includes a statement restricting the entry of SSNs in EDRMS.
[14] GSA/GOVT-4 Contracted Travel Services Program, 41 FR 26700 (June 3, 2009), *available at* https://www.gpo.gov/fdsys/pkg/FR-2009-06-03/html/E9-12951.htm.

documents for FIMA employees.

- DHS/ALL-004 General Information Technology Access Accounts Records System (GITAARS)[15] covers user access accounts records specifically, user's unique project ID number.
- DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records[16] applies to personnel records of FIMA employees.
- DHS/FEMA-003 National Flood Insurance Program Files System of Records[17] applies to information related to the NFIP.
- DHS/FEMA-004 Non-Disaster Grant Management Information Files System of Records[18] applies to non-disaster related grant files.
- DHS/FEMA-008 Disaster Recovery Assistance Files System or Records[19] applies to disaster recovery assistance files.
- DHS/FEMA-009 Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs[20] applies to information related to HMA and PA files.
- DHS/FEMA-014 Hazard Mitigation Planning and Flood Mapping Products and Services Records System of Records[21] applies to information related to LOMAs and hazard mitigation planning files.

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

EDRMS is a major application and a security plan (SP) was completed for the EDRMS. An Authorization to Operate (ATO) for EDRMS was granted on August 25, 2014, and is

[15] 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.
[16] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records, 80 FR 58283 (September 28, 2015), *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-09-28/html/2015-24589.htm.
[17] DHS/FEMA-003 National Flood Insurance Program Files System of Records, 79 FR 28747 (May 19, 2014), *available at* https://www.gpo.gov/fdsys/pkg/FR-2014-05-19/html/2014-11386.htm.
[18] DHS/FEMA-004 Non-Disaster Grant Management Information Files System of Records, 80 FR 13404 (March 13, 2015), *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05799.htm.
[19] DHS/FEMA-008 Disaster Recovery Assistance Files System or Records, 78 FR 25282 (April 30, 2013), *available at* https://www.gpo.gov/fdsys/pkg/FR-2013-04-30/html/2013-10173.htm.
[20] DHS/FEMA-009 Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs, 79 FR 16015 (March 24, 2014), *available at* https://www.gpo.gov/fdsys/pkg/FR-2014-03-24/html/2014-06361.htm.
[21] DHS/FEMA-014 Hazard Mitigation Planning and Flood Mapping Products and Services Records System of Records, 82 FR 49404 (October 25, 2017), *available at* https://www.federalregister.gov/documents/2017/10/25/2017-23205/privacy-act-of-1974-system-of-records.

undergoing reauthorization. EDRMS is compliant with NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans; NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach; and DHS Sensitive Systems Policy Directive 4300A.

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

EDRMS only stores a copy of official FIMA records and documents including emails. FIMA Directorates and Offices are responsible for proper records and retention for all original paper and electronic documents and records that are uploaded into EDRMS. EDRMS implements the retention schedule the FIMA program offices provide for their documents and records stored in EDRMS. It is the responsibility of the FIMA program office submitting the documents and records to identify the correct retention schedule. The metadata associated with the document and records follow the same records and retention schedule of the document and record.

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.

EDRMS itself is not subject to the requirements of the Paperwork Reduction Act (PRA) as it does not create any new forms or information collection tools completed by the public. Any forms or information collections uploaded into EDRMS are covered by their source systems' PRA requirements.

Section 2.0 Characterization of the Information

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

EDRMS stores record entry forms which contains FEMA employee and contractor PII and digital documents which contains general public PII. Audit log entries include FIMA user names and metadata includes the FIMA employee's first and last names.

EDRMS Record Entry Forms

Record entry forms are used to enter metadata about the documents and records stored in the EDRMS electronic data store.

EDRMS collects and maintains the following information from EDRMS users related to the document or record entered into EDRMS:

Metadata Fields

- Classification (the FIMA electronic file plan that describes the function or subject of the document/record);
- Title (a free form text field that describes the individual characteristics of the record);
- Owner Location (set to the default region or corresponding region);
- Home Location (set to the default region or corresponding region);
- Retention Schedule (an official policy for records and information retention and disposal);
- Disposition (the final administrative action taken with regards to records and documents);[22]
- Default Media types (unknown (default), paper, electronic document, optical disk, (Compact Disk (CD)/Digital Video Disc (DVD)/etc.), engineering drawings/computer aided drafting (CAD), magnetic storage, memory storage, microfilm/microfiche, photographs/slides and video tape); and
- Default Record Access (allows enforces the logical access control base on the region).

FEMA Employee or Contractor Information

- Username (unique identification);
- User First Name;
- User Last Name;
- User Phone Number;
- Employee Role(s); and
- Government Email Address.

[22] The disposition options are as follows: 1) destroying, 2) transferring to another entity (e.g., Federal Record Center), and 3) preserving them permanently (e.g., NARA).

Regions I, II, VI, VII, VIII, and IX Form Metadata Fields

- Classification;
- Title;
- Community ID Name (a unique identification number created when a community enrolls in the NFIP Community Information System (CIS)); and
- Date Created.

Regions III and V Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Author (the name of the originator of the document stored in the electronic data store); and
- Date Created.

Region IV Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Case Number (an additional record type identifier for acquisition records stored in the electronic data store); and
- Date Created.

Region IV – Acquisitions Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Date Created;
- Program (a field that describes the category of the program);
- Disaster Number (a unique identification number assigned to the disaster);
- Project Number (a unique identification number assigned by the National Emergency Management Information System-Individual Assistance);

- Funding Cycle (describes the funding cycle (year));
- Case Number;
- Federal Grant Number (a unique identification number the Federal Grant Program Office assigns to the Federal Grant document); and
- Status (representative of the current stage of entering the metadata and document in the EDRMS).

Region IV – Grants (HMPG) Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Date Created;
- Disaster Number;
- Project Number;
- Status;
- Federal Grant Number; and
- Funding Cycle.

Region IV – Non Disaster Grants Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Date Created;
- Project Number;
- Federal Grant Number; and
- Funding Cycle.

Region IV – Technical Form Metadata Fields

- Classification;
- Title;

- Community ID Name;
- Date Created;
- Task Order (a unique identification number assigned to the task);
- Contract Number (a unique identification number assigned to the contract); and
- Disaster Number.

Region VI – Acquisitions Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Date Created;
- Program;
- Disaster Number;
- Project Number;
- Funding Cycle;
- Case Number;
- Federal Grant Number; and
- Status.

Region VI – Grants (HMPG) Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Date Created;
- Disaster Number;
- Project Number;
- Status;
- Federal Grant Number; and
- Funding Cycle.

Region VI – Non Disaster Grants Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Date Created;
- Project Number;
- Federal Grant Number; and
- Funding Cycle.

Region VI – Technical Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Date Created;
- Task Order;
- Contract Number; and
- Disaster Number.

Region X Form Metadata Fields

- Classification;
- Title;
- Community ID Name;
- Author/Signatory;
- Recipient (field that reflects the recipient of the record; and
- Date Created.

Headquarters Form Metadata Fields

- Classification;
- Title;
- Date Created;

- Author;
- FIMA Offices (field that reflects the FIMA Office associated with the record); and
- Container (field that reflects the folder where the record may be).

<u>EDRMS Digital Documents and Records</u>

FEMA may store the following information found in FIMA's Mitigation and NFIP documents and records:

FIMA Mitigation Records

Documents and records stored in EDRMS may contain the following hazard mitigation data:

Organization Point of Contact (POC) Information from Federal, State, and Local Communities

- Name of Organization's or Community Designated POC Full Name;
- POC Title;
- POC's Office Mailing Address;
- POC's Office Phone Number And Extension;
- POC's Office Cell Number;
- POC's Office Fax Number;
- POC's Email Address; and
- Organization Name.

Disaster and Non-Disaster Grant Applicants

- Name of Organization's Designated POC;
- POC Title;
- POC's office mailing address;
- POC's office phone number and extension;
- POC's office cellphone number;
- POC's office fax number;
- POC's work email address;
- Organization Name;
- Organization's Federal Employer Identification Number (EIN);

- Organization’s Bank Routing Number;
- Organization’s Bank Account Number;
- Organization’s activity or activities proposed under requested grant; and
- Urban Area Affiliation (if applicable).
- Unique Identifier (e.g., employer identification number (EIN), recipient account numbers, or Data Universal Numbering System (DUNS) Number);
- Type of Organization (e.g., private, public, non-profit, or government);
- Applicant Grant Status (e.g., grantee or sub-grantee of the state);
- Applicant Smart Link Status;
- Applicant Eligibility Status;
- Small Impoverished Community Status (yes/no); and
- Certifying Official.
- Occupant Information (of the damaged dwellings)
  - Name (First, Middle, Last);
  - Age; and
  - Relationship to Applicant.
- Estimates of Damage (Home or Personal Property)
  - Claimant Name (full);
  - Address; and
  - Amount.

Finance (FIN) Related

- Recipient Information: Unique Identification (number, employer/federal ID, etc.);
- Vendor/Organization Name(s);
- Vendor/Organization Address(es);
- Place of Performance Address;
- Congressional District;
- Indication of Reporting Applicability (yes/no);

- Type of Recipient (e.g., state government, local government, Indian tribe, non-profit, or individual);
- Individual‘s Name (POC, employee of organization, etc.);
- Individual‘s Email Address;
- Individual‘s Phone Number;
- Vendor/Organization Name(s);
- Vendor/Organization Address(es);
- Vendor/Organization Category (e.g., commercial, employee, federal, government, individual, or private);
- Type of Action (e.g., award or continuation); and
- Individual Assistance (IA) Benefits.

NFIP Records

Documents and records stored in EDRMS may contain the following NFIP data:

Reinsurance Brokers, Reinsurance Companies, Risk Modeling Companies, or Other Stakeholders:

- **Organizational/Brokerage/Other Stakeholders Information**
  - Organization Name;
  - Point of Contact Full Name;
  - Address(es);
  - Email Address(es);
  - Telephone Number(s); and
  - Insurance/Claims Statistical Data.
- **Claimant Information**
  - Full Name;
  - Address(es);
  - Email Address(es);
  - Telephone Number;
  - User ID; and

- Personal Identification Number (PIN)/Password(s).

NFIP Applicant Information

- Unique ID (e.g., registration ID, SSN);
- Type of Damaged and/or Current Residence;
- Names;
- Date of Birth;
- Age;
- Email Address;
- Relationship to Property (owner or lessor);
- Damaged and/or Current Property Address;
- Damaged and/or Current Property Notes;
- Damaged and/or Current Property Phone Number(s);
- Damaged Property Geographical Information (e.g., GPS information, directions);
- Dates;
- Number of Dependents;
- Pre-Disaster Household Composition;
- Income Information;
- Occupant Relationship to Applicant; and
- Notes.

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

EDRMS does not collect information directly from individuals. The EDRMS user enters the document/record metadata based on the information provided by the originating FIMA office. EDRMS user activity is captured in EDRMS storage and retrieval reports.

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

EDRMS does not use information from commercial sources or publicly available data. The originating FIMA office document may include information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

FIMA documents and records are assumed to be accurate when uploaded into EDRMS. It is the responsibility of the originating FIMA office to ensure the accuracy of the data. It is the responsibility of the EDRMS users, FIMA managers, and process owners to ensure the accuracy of the EDRMS metadata. FIMA provides training to FIMA Headquarters and Regional offices regarding the proper way of adding information into the system and on the Record Entry Forms. Data entered and documents and records saved in the EDRMS data store are National Information Exchange Module (NIEM) compliant. Appropriate record entry form input validation error messages are displayed to the EDRMS user for invalid data entries. FEMA's Regional EDRMS administrations and the System Owner perform weekly input validation of data entered into the Record Entry Forms.

2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

<u>Privacy Risk</u>: EDRMS users may input incorrect records classification or metadata information which can cause an EDRMS user to inadvertently access records without an appropriate need to know.

<u>Mitigation</u>: This risk is partially mitigated through training of EDRMS users on how to add documents and records to reduce input of inaccurate information into the system. Additionally, the EDRMS administrator checks weekly for the correct entry of classification and CID on the record entry forms for new documents and records entered in EDRMS. Users receive access to files based on their role and region. FEMA cannot fully mitigate this risk due to possible human errors inherent with entering information into a system.

<u>Privacy Risk</u>: FIMA is over-collecting information with information being stored in paper files and digitally in EDRMS or other FIMA-related systems.

<u>Mitigation</u>: FEMA does not fully mitigate this risk. EDRMS is not a requirement for all of FIMA to use. Some offices, therefore, may continue to use paper records while some are able to benefit from the use of EDRMS. EDRMS does not connect to any other FEMA system with the exception of the FEN and the FEIMS for security and access control. EDRMS does not replace other FEMA systems and is not intended to duplicate other systems. FIMA continuously provides training through FIMA and the Regional Offices and highlights that EDRMS is to reduce paper and to have a repository of emails used for purposes such as replying to correspondence using FEMA's emailing system.

Privacy Risk: FEMA may maintain inaccurate or outdated data within EDRMS.

Mitigation: This risk is not mitigated. As a document repository EDRMS cannot update or correct individual records uploaded into the system. Metadata for records may be updated using the EDRMS user interface to correct inaccurate metadata. If information within a record is corrected via a method similar to that of the initial data entry (i.e., by refiling a corrected form), that correction will also be uploaded within EDRMS. As long as the inaccurate and correct records share similar metadata, both will be retrieved by any queries within EDRMS. The date of the document and other metadata will allow the newer document to supersede in order the previous copies reducing the probability that inaccurate data will be used. EDRMS users will be able to compare dates and identify the most recent information provided to FEMA. FEMA further mitigates the risk of inaccurate data by not using any information contained within the system for the purposes of granting benefits or making operational decisions.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

EDRMS standardizes the storage of FIMA documents and records. EDRMS users are able to retrieve documents and records stored in the EDRMS electronic document\record store to reply to FOIA requests, to support FIMA requests, and to support FIMA research. EDRMS provides FIMA personnel and contractors the ability to electronically manage documents and records through the document and record life cycles. Document management includes identification, storage, securing and archiving documents. Records management includes identification, classification, prioritization, storage, security, archiving, retrieval, tracking and disposal of records. Metadata will be entered for the scanned documents and records using specific record types for the appropriate region. The metadata will be saved as data fields and will be used to create more relevant search and retrieval options and capabilities. The EDRMS user can then search by any key methodology as dictated by the information provided in the metadata. Use of the fields identified as key fields will greatly enhance the accuracy of the search.

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.

EDRMS users do not use EDRMS to conduct electronic searches, queries, or analyses to discover or locate predictive patterns or anomalies. Storage, retrieval, and query activity is audited by the EDRMS program managers. Retrieval of documents from EDRMS is based on the user's authorization. The originating FIMA office is responsible for approving the user's authorization to access documents stored in EDRMS. It is the source documents program office's responsibility to ensure the use of documents retrieved by their authorized EDRMS users is in accordance with their PIAs and SORNs.

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

No other DHS or FEMA component or external system has access to EDRMS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that data within EDRMS may be used for an unintended or unauthorized purpose.

Mitigation: Only authorized EDRMS users have access to documents and records stored in EDRMS. The authorization to create an EDRMS user account is the responsibility of the EDRMS program managers, the EDRMS system owner, and the originating FIMA office. It is the responsibility of the originating FIMA office to ensure its EDRMS users use retrieved EDRMS documents in accordance with its PIA and its SORN. Users' access to data and functionality is based on the users' location, position description, projects, and EDRMS user role assignment. EDRMS users are required to annually sign Rules of Behavior.

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.

FEMA provides notice to individuals on the use of EDRMS through this PIA and the associated SORNs mentioned in Section 1.2 that provide public notice of FEMA's collection, use, dissemination, or maintenance of PII. Notice is provided through the source information/systems mechanisms that feed into EDRMS.

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

Individuals submit their consent, decline to provide information, or opt out of the project by communicating that choice to the originating FIMA program office or directorate. EDRMS only stores official copies of documents and records from the originating FIMA office.

4.3 <u>Privacy Impact Analysis</u>: Related to Notice

<u>Privacy Risk</u>: There is a risk that individuals are not given sufficient notice regarding the use of their information in EDRMS.

<u>Mitigation</u>: FEMA manages this risk through publication of this PIA and the SORNs mentioned in Section 1.2 that provide public notice of the system collection, use, dissemination, and/or maintenance of PII. Additionally, the DHS/FEMA/PIA-011 National Flood Insurance Program PIA provides additional notice of FEMA's use of NFIP policy information.

<u>Privacy Risk</u>: There is a privacy risk the originating FIMA offices do not provide notice through their own PIA documentation.

<u>Mitigation</u>: This privacy risk is partially mitigated by FEMA privacy and program managers completing this PIA and the PIA and SORNs for the originating FIMA offices identified as collecting PII. Each originating FIMA office's PIA and SORN address the originating FIMA office's collection of PII and all privacy-related risks and mitigations. Additionally, DHS policy requires the FEMA Privacy Office to review PIAs triennially and continuously monitor SORNs to ensure accuracy and transparency.

Section 5.0 Data Retention by the project

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

In accordance with the FEMA Records Schedule (FRS) and NARA Disposition Authority, records are destroyed based on the originating FIMA office and NARA disposition schedule. EDRMS only stores a copy of the official record. EDRMS has the capability to provide a forecast for items approaching their disposition date, and the EDRMS System Owner uses the system to generate a report for documents and records that have reached their scheduled disposition time. The EDRMS System Owner or his or her designee destroys the records within EDRMS based on the disposition report. The originating FIMA offices are responsible for the retention and destruction of the official records residing in the source systems, in accordance with the approved records retention schedule.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that policyholder information (including PII) is retained for a period longer than necessary.

Mitigation: FEMA manages this risk through the performance of weekly reviews of files maintained by EDRMS to determine if any information is no longer needed for audit or administrative purposes. For instance, FEMA may need the results or responses of operation reviews longer than the flood insurance policy information supporting the results. Any information that is no longer necessary for retention is disposed of in accordance with the appropriate NARA records retention schedule. Furthermore, all FEMA employees (including the EDRMS system owner) are required to take DHS records management and privacy training annually.

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.

FIMA does not share their day-to-day correspondence with outside individuals, organizations, or agencies. The external entity must submit a formal request to FEMA. FIMA retrieves and uses documents and records entered in EDRMS to generate EDRMS document and record storage activity and retrieval reports. FIMA Program Offices may retrieve documents and records from EDRMS and share them outside of DHS as part of FIMA's normal operations. Any sharing of information by the originator of the record stored in EDRMS is the responsibility of the originating FIMA program office in accordance with the applicable SORN and PIA.

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

Sharing of information retrieved from EDRMS is the responsibility of the respective FIMA offices. Any sharing of information by the originator of the record stored in EDRMS is the responsibility of the originating FIMA program office in accordance with the applicable SORN and PIA.

6.3 Does the project place limitations on re-dissemination?

Re-dissemination of information retrieved from EDRMS is the responsibility of the respective FIMA office. Any sharing of information by the originator of the record stored in EDRMS is the responsibility of the originating FIMA program office. FIMA includes a routine use letter or executes an Information Sharing and Access (ISAA) with any sharing of information that has language to limit the re-dissemination of information shared.

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

FEMA's Information Management Division Disclosure Branch tracks and records all requests and disclosures of information pursuant to FOIA and Privacy Act (PA) requests. Additionally, each FEMA Program Office that uses EDRMS must track any disclosures to third parties via their respective methods.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information within EDRMS may be erroneously disclosed outside of DHS.

Mitigation: FEMA manages this risk by only sharing information outside of the Department as permitted by the SORNs mentioned in Section 1.2 and as documented in this PIA. It is the responsibility of the FIMA originating program to properly disclose information in accordance with the appropriate PIA and SORN. Access to EDRMS is extremely limited based on various EDRMS parameters, including location and role-based access granted only for those individuals who need to know the information to perform their jobs. Sharing of information pursuant to the FOIA and PA is tracked by FEMA's Information Management Division and the EDRMS system. The source system for the records is responsible for tracking all other disclosures as documented in their respective PIA and SORN.

Section 7.0 Redress

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

Access to EDRMS is granted only to FEMA personnel authorized by their Regional Administrators, FIMA program offices and directorates, and the EDRMS system owner. Individuals of the public do not have access to EDRMS. Individuals can access their information via the information access procedures associated with the respective source systems and associated FEMA office. Individuals can submit a Privacy Act (PA) request (for U.S. citizens and lawful permanent residents) or FOIA request (for all other members of the public) to the FEMA Information Management Division Disclosure Branch in writing to: FEMA Disclosure Branch, Federal Emergency Management Agency, Department of Homeland Security, 500 C Street, SW, Washington, D.C. 20472. The request should include the name of the requester, nature of the record(s) sought, and the required verification of identity. Individuals may also choose to receive information directly from EDRMS by following the access procedures above.

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

Individuals who wish to correct their information must go to the FIMA program office's SORN or PIA to identify the procedures in place to allow correction of inaccurate or erroneous information. Individuals can provide updated information to their respective insurance provider or FIMA office. The FIMA program office updates the source record. Individuals who are U.S. citizens or legal permanent residents can correct inaccurate or erroneous information by using the information access procedures as identified above in Section 7.1. EDRMS users can correct access information such as telephone number or email address by sending an email message to the regional or headquarters system administrator to correct the user's contact information in EDRMS.

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

Individuals are notified of the procedures for correcting their information through this PIA as well as through the respective SORNs referenced in Section 1.2 and other source system PIAs. Also, EDRMS users receive training and have access to EDRMS user manuals on how to correct contact information within the system.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are not aware of the procedure for correcting erroneous information in connection with EDRMS especially because EDRMS does not collect information directly from individuals.

Mitigation: FEMA manages this risk by informing the public of procedures for correcting their information through this PIA and the source information collection's PIA and the SORNs listed in Section 1.2. Additionally, WYO companies typically provide their policyholders with information on their respective privacy policies and the procedures to correct erroneous data. EDRMS users receive training and have access to EDRMS user manuals on how to correct contact information within the system.

Privacy Risk: There is a risk that records corrected in the source system pursuant to a Privacy Act amendment request will not be updated in EDRMS.

Mitigation: FEMA does not mitigate this risk as EDRMS is a document and records repository with record management functions and is not a requirement for the various FIMA program offices to use. The FIMA program office can scan and upload the Privacy Act redress request and response into EDRMS to document FIMA's response.

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?

EDRMS institutes technical security controls, rules of behavior policies, security awareness communications, and other security processes, such as periodic audits and log reviews. Only a relatively small group of authorized users have access to EDRMS, based upon specific, established responsibilities and permissions set within the system. Users include FEMA employees and contractors only. Individuals that engage in unauthorized access to EDRMS are subject to disciplinary action that can result in account termination or suspension. Additionally, FEMA ensures that the practices stated in this PIA are followed by leveraging standard operating procedures, which are updated annually.

EDRMS only allows authorized FEMA personnel access within the FEMA firewall and no public access is possible. EDRMS users gain access to the system through the FEIMS SSO using their PIV card. All EDRMS activity is logged and reviewed on a daily basis. Auditable events are retained for one year when there are no security incidents. If a security incident is reported, the audit logs are retained for three years after the end of the security event investigation. EDRMS security mechanisms (i.e., technical, operational, and managerial) are assessed based on DHS 4300A and NIST SP 800-53A. EDRMS is approved by FEMA and is included in the DHS Technical Reference Model.[23]

8.2 What privacy training is provided to users either generally or specifically relevant to the project?

Annual privacy training is required for all FEMA employees and contractors. Additionally, EDRMS users are provided specific training on how to use EDRMS.

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

FEMA has established a separation of duties standard in accordance with DHS Sensitive Systems Handbook. The EDRMS system owner and EDRMS system Regional Records Administrators are responsible for ensuring users are authorized to access the stored EDRMS documents and records based on the users' responsibilities and need-to-know. Authorized user

[23] *Available at* https://intranet.fema.net/org/ms/ocio/aees/EA/Lists/FEMA%20Technical%20Reference%20Model%20TRM/By%20Manufacturer.aspx.

account requests are submitted to FEIMS. For example, FEMA privileged users (i.e. system administrators and database administrators) have full access to the EDRMS operating system and database, but are prohibited from accessing or executing EDRMS functionality. Need-to-know is based on the originating FIMA office data access requirements.

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?

FEMA's process for reviewing and approving Memoranda of Understanding (MOU) and Information Sharing Access Agreements involve FEMA's IT Security Branch, FEMA Privacy Officer, and the Office of Chief Counsel, as well as the appropriate authorities from the other agency or organization to the agreement.

Responsible Official

William H. Holzerland
Senior Director for Information Management
Office of the Chief Administrative 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 Office
Department of Homeland Security