Privacy Impact Assessment
for the

Operational Data Store (ODS) and Enterprise Data Warehouse (EDW)

DHS/FEMA/PIA-026

June 29, 2012

Contact Point
Anabela Serra
Enterprise Data Warehouse Program Manager
Office of the Chief Information Officer
Federal Emergency Management Agency
(540) 678-2285

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

Abstract

The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Office of the Chief Information Officer (OCIO) owns and operates the Operational Data Store (ODS) and Enterprise Data Warehouse (EDW) systems. ODS and EDW replicate source system-provided data from other operational FEMA systems and provides a simplified way of producing Agency reports for internal use as well for external stakeholders. These reports are related to the various FEMA mission-related activities such as FEMA's readiness to deploy, disaster response, internal operations, oversight etc. Reports are on based on the needs of the particular program requirements or mission related activity. Each source system has a separate data mart within the ODS to ensure that information is not commingled and that the source system rules for use are followed within the ODS. Data marts allow for the manipulation of data while at the same time ensuring that the exact same data within the source system remains static. FEMA is conducting this PIA because ODS and EDW collect, use, maintain, retrieve, and disseminate personally identifiable information (PII) pulled from the source systems.

Overview

FEMA OCIO developed, owns, and operates the ODS and EDW systems. These systems together provide a centralized data reporting application through which numerous FEMA systems throughout the Agency's divisions can load data on a regularly scheduled basis and create reports related to operational and oversight needs of FEMA. ODS is a consolidated repository of information from different FEMA source systems for reporting purposes. EDW is designed for summarization of information, retrieval of information, reporting speed, and ease-of-use (i.e., creating reports). Typically, EDW receives information from ODS. These systems do not archive data or provide backup capabilities for FEMA source data systems.

In support of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 100-707 (1988), and as required by other congressional, statutory, and DHS requirements, FEMA provides reports on the status of emergency management and financial programs, projects, and funding. To ensure that all of FEMA's programs and their related information technology systems are able to generate reports as needed and required, FEMA OCIO has developed the ODS and EDW systems as an enterprise solution. Reports generated assist in the detection and avoidance of duplication of benefits by FEMA. Additionally, EDW creates reports that may be used to provide current status of FEMA's disaster deployment readiness in support of FEMA's mission to "support our citizens and first responders, while ensuring that we work

together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards."[1]

The ODS system is a data mart repository of different FEMA source systems. Each source system has its own data mart which allows for the manipulation of data while at the same time ensuring that the exact same data within the source system remains static. Information from the different FEMA source systems is separated within ODS by data mart and has individual access requirements, individual rules, and does not commingle with other source system data marts within ODS. EDW is designed for summarization and retrieval, for reporting speed and ease-of-use. Data is updated and refreshed daily to provide updated and easily accessible data in a secure location for use throughout the agency. EDW allows the agency to more readily access large amounts of data required to perform the agency's analysis, reporting, summarization, and emergency management duties. Rapid customizable access to high quality data assists FEMA in improving efficiencies in disaster mitigation, preparedness, and response and recovery efforts. The reports created may contain sensitive PII including name, address, and social security number.

Typically, EDW receives information from ODS. The information in the ODS originates from the source systems data mart (i.e., Human Resources, Disaster Deployment, Financial Systems, Environmental Specialist, and Individual Assistance Programs) that assist Agency management in determining the appropriate measures and decisions to apply in the event of a national disaster or emergency. Each source system's data is separated by data mart within the ODS to prevent inadvertent access of information and to facilitate ease of report creation. Before data is shared between the underlying source system and ODS, each source system must have an approved memorandum of understanding (MOU) with ODS outlining the roles and responsibilities of both systems in the exchange. All rules and authorities associated with the source system data remain with the data as it is transferred to its data mart within ODS.

Each source system data steward defines the data fields required for their reporting purposes. Data that is required for each reporting purpose is extracted from the source system data within ODS and is populated into the appropriate ODS fields for access by the EDW reporting tool. The data not required remains in the source system and is not transferred to the reporting tool. Data marts are created within ODS to facilitate transfer of data from the source systems and to separate the different source system data within ODS and then EDW. Data marts help to ensure that source system data or records are not commingled within the system and help prevent inappropriate access and use of source system data.

[1] *http://www.fema.gov/about* for more information regarding FEMA's mission is accessible.*t.*

EDW users with assigned roles, including a "need to know" standard for access to PII, can then access EDW through the Business Objects tool log-in from the FEMA Intranet. The EDW Business Objects tool is the EDW user access and interface application. Users create individual reports based on the available data fields within their data mart, their user role, and level of PII access. The user cannot access other source systems data and data marts unless additional specific assess rights have been granted by that source system's data steward. A user may be granted data mart access rights by more than one source system data steward depending on the complexity and need-to-know for the reporting requirement. For instance, a user that needs to report current benefits paid out to disaster assistance applicants may be granted access to the disaster assistance data mart by the source system data steward and the financial data mart by the financial source system data steward. The user would only be able to access data from those two data marts.

Once the user has identified the fields needed for his report, the EDW report tool populates the fields with data retrieved from the specific ODS data mart, subject to access rights granted for the specific source system's data mart and the role-based access restrictions to certain fields based on a user's "need to know." If the user has printing permissions assigned to his user role and account, then the user may print the report as needed. Reports are based on the specific source system data marts only, and cannot be changed or manipulated in the EDW system once created. Data-populated reports are not saved within the EDW system. EDW only saves the required fields that the user needs for reporting. When the user needs to run an updated report, the user can select saved reporting criteria and the saved fields will populate with current information stored in the EDW.

Previously, the functions associated with ODS and EDW were covered by the National Emergency Management Information System (NEMIS) certification and accreditation (C&A) boundary and associated documentation. In July 2011, NEMIS was decoupled and the functions previously designated as the NEMIS-wide reports and shared references function/module are now performed by the ODS and EDW systems. This PIA provides documentation on how these systems collect, use, maintain, retrieve, and disseminate PII from FEMA source systems.

FEMA identified several privacy risks associated with ODS and EDW during the system development and PIA review process. Generally, there is the risk that ODS and EDW may use erroneous information for reporting purposes by relying on outdated information from source systems and that information contained within the systems may be accessed, viewable, or used for purposes other than those for which the data were originally collected by the source system. FEMA mitigates these privacy risks by having ODS and EDW initiate regular updates and refreshes from the source system and by implementing the ODS/EDW Data Quality Plan based on the DHS Data Quality Guide. Additionally, FEMA mitigates privacy risk by establishing data

marts that separate all source system's data, thus preventing users from viewing all information within ODS, and by employing strict access controls that only allow individuals with an established need-to-know access rights. FEMA also requires initial and annual refresher privacy training for all users.

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 authority for this system is based on the Joint Financial Management Improvement Program, other statutes, Executive Orders, Office of Management and Budget (OMB) and Treasury guidance, regulations, and DHS and FEMA policies:

- Debt Collection Improvement Act of 1996, Pub. L. No. 104-134 (1996);
- Federal Claims Collection Act, 31 U.S.C. § 3711, et. seq.;
- 31 C.F.R. part 370;
- Federal Records Act, 44 U.S.C. §§ 2901 et. seq., and chapters 21, 25, 31, and 33 of this title, 44 U.S.C. §§ 2101 et. seq., 3101 et seq., and 3301 et seq.;
- Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 100-707 (1988);
- Homeland Security Act, Pub. L. No. 107-296 (2002);
- Federal Managers' Financial Integrity Act, Pub. L. No. 97-255 (1982);
- Chief Financial Officers Act, Pub. L. No. 101-576 (1990);
- Federal Financial Management Improvement Act, Pub. L. No. 104-208 (1996);
- Executive Order 9397;
- Executive Order 12472;
- OMB Circular A-130; and

- OMB Circular A-127.

All legal authorities and agreements associated with the data maintained in the source system follows the data collected, used, maintained, retrieved, and disseminated within ODS and EDW.

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

Since ODS and EDW do not collect information directly from individuals and no new information is created through the system about individuals, the information contained in the source systems performing the original collection is covered by the individual SORNs for those systems as listed below:

- DHS/ALL-004 General Information Technology Access Account Records System of Records (GITAARS), 74 Fed. Reg. 49882 (Sep. 29, 2009);

- DHS/ALL-007 Accounts Payable System of Records, 73 Fed. Reg. 61888 (Oct. 17, 2008);

- DHS/ALL-008 Accounts Receivable System of Records, 73 Fed. Reg. 61888 (Oct. 17, 2008);

- DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records System of Records, 73 Fed. Reg. 61888 (Oct. 17, 2008);

- DHS/FEMA-003 National Flood Insurance Program Files System of Records, 73 Fed. Reg. 77747 (Dec. 19, 2008);

- DHS/FEMA-004 Grant Management Information Files System of Records, 74 Fed. Reg. 39705 (Aug. 7, 2009);

- DHS/FEMA-008 Disaster Recovery Assistance Files System of Records, 74 Fed. Reg. 48763 (Sep. 24, 2009); and

- DHS/FEMA-2006-0002 National Emergency Management Information System—Mitigation Electronic Grants Management (NEMIS-MT eGrants) System of Records, 69 Fed. Reg. 75079 (Dec. 15, 2004).

All Privacy Act provisions and requirements associated with the data in each source system remains in effort within ODS and EDW.

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

ODS is currently within the FEMA Support System (FSS) General Support System (GSS) Certification and Accreditation boundary. The FSS GSS System Security Plan (SSP) was completed on August 17, 2011. ODS is operational and was granted an eighteen-month Authority to Operate (ATO), effective August 31, 2011. The EDW SSP was completed on July 15, 2011. EDW is operational and was granted a two-year Authority to Operate (ATO), effective July 15, 2011.

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

The ODS and EDW systems do not archive data. Each source system and its responsible data steward are responsible for records management compliance. As data are added or deleted in the source systems, it is also added or deleted in ODS and EDW during regular daily updates and refreshes. Data are retained within EDW as long as indicated by each source system's NARA-approved records retention and disposal schedule. Additionally, each source system must comply with FEMA's policies and procedures for records retention. FEMA's policies and procedures for expunging data at the end of the retention period are consistent with DHS policy and guidance.

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.

ODS and EDW are not subject to PRA requirements because a specific form completed by the public is not used to populate the information in EDW. EDW receives information from various source systems. Each source system is responsible for compliance with the PRA.

Section 2.0 Characterization of the Information

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

The ODS and EDW systems collect, use, maintain, retrieve, and disseminate the following information:

Automated Deployment Database (ADD)
(FEMA employees and other government deployment personnel, including volunteers for the Surge Capacity Force):

- Unique Identification (SSN and system-generated);
- Name (e.g., individual, supervisor, requestor, or contact);
- Program Assignment;
- Job Type;
- Job Title;
- Addresses (office and personal);
- Date of Birth;
- Gender;
- FEMA Employee (yes/no);
- Employee type (e.g., Disaster Assistance Employee);
- Employee type description (e.g., Disaster Assistance Employee);
- Employee Status (active or terminated);
- Deployment Status;
- Pay Type and Description;

- Grade;
- Step;
- Series;
- Salary Period (i.e. per hour, per day, per annum, etc.);
- FEMA Organization, Section, Branch, and Unit;
- Federal Annuitant (yes/no);
- Dates (i.e. last call-in, release, deployment, and assignment, etc.);
- Military Affiliation Information;
- Security Determination;
- Specialties (e.g., foreign language, biologist); and
- Tour of Duty Station.

Environmental Historic Preservation (EHP)

- User Identification; and
- User name (full).

Finance (FIN) Related

Recipient Information:

- Unique Identification (Data Universal Numbering System (DUNS) 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.

General Information:

- Unique Identification (ID) (e.g., ADD ID or network user ID);
- User Name; and
- User Assignment.

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 leasor);
- 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.

Mitigation (MT) Grantee

- Unique Identifier (e.g., employer identification number (EIN), recipient account numbers, or Duns and Bradstreet Number);
- Applicant Name (Recipient or Organization);
- Type of Organization (e.g., private, public, non-profit, or government);

- Applicant Address;
- Applicant State Code;
- Applicant Phone Number;
- Applicant Grant Status (e.g., grantee or sub-grantee of the state);
- Applicant Smart Link Status;
- Applicant Eligibility Status;
- Applicant POC Name;
- Applicant POC Title;
- Applicant POC Address;
- Applicant POC Phone Number;
- Applicant POC Facsimile Number;
- Small Impoverished Community Status (yes/no); and
- Certifying Official.

Public Assistance (PA) Grantees

- Unique Identifier (applicant identification numbers);
- Public Assistance Coordinator;
- Dates;
- Applicant Name (organization);
- Type of Organization (e.g., private, public, non-profit, or government);
- Applicant Address;

- Applicant Grant Status (e.g., grantee or sub-grantee of the state);
- Applicant Smart Link Status;
- Applicant Eligibility Status;
- Applicant POC Name;
- Applicant POC Phone Number; and
- Applicant POC Facsimile Number.

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

ODS and EDW do not collect information directly from individuals. Information collected and stored in ODS and EDW is collected from the source FEMA system. Source systems are interconnected to data marts within the ODS pursuant to a MOU. Source system data within ODS are separated by data marts. Information is retrieved from the data mart within ODS, using an interconnection to EDW. Reports generated are limited to specific source system data marts. All source systems and their associated PIAs and SORNs are listed in the Appendix of this PIA.

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

ODS and EDW do not collect information from commercial sources or publicly available data. Each source system may use information from commercial sources or publicly available data. This information may be requested by the source system data steward to be fed into ODS and EDW for reporting purposes.

2.4 Discuss how accuracy of the data is ensured.

Information is collected from the source system for use by FEMA staff with roles assigned by the source system's administrator or system owner. Accuracy of information is the responsibility of the underlying source system. The DHS Data Quality Guide channels the development process and the FEMA Enterprise ODS/Data Warehouse Data Quality Plan is

followed. The purpose of the FEMA Enterprise ODS/Data Warehouse Data Quality Plan is to provide an implementation baseline for applying data quality standards across the ODS and EDW. Following the System Engineering Life Cycle (SELC), the data goes through user acceptance testing (UAT) and independent verification and validation (IV&V), where the information is reviewed by the tester for accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that EDW may receive more information than is needed to provide the reports requested or required by the user access and interface application.

Mitigation: This privacy risk is mitigated by EDW only receiving the relevant data elements from the source systems. Information within ODS is separated by data marts accessible only by users approved by the source systems' data steward with an established need to know. This process limits users from creating reports that contain more information than is needed for the report supporting their specific mission. The source systems collect information on individuals pursuant to the source systems guidelines and legislative limitations. No additional information is collected on paper or orally.

Privacy Risk: There is also a privacy risk that EDW may collect, use, maintain, retrieve, and disseminate erroneous or inaccurate information due to its reliance on underlying source system data.

Mitigation: Although EDW relies on the data quality and integrity fed to it by the source systems outlined in Section 2.2, this privacy risk is mitigated by regular daily updates to ODS from the source systems. EDW initiates regular updates and refreshes information from the ODS to ensure up-to-date source system data. Source system data updated in ODS either refreshes existing data or deletes data not refreshed. ODS and EDW do not archive data.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

ODS collects information from the source systems to allow a central database to fulfill its mission as an enterprise-wide repository of emergency management information. Information in each source system's data mart is accessible through EDW only to users granted access to that data mart by the source system's data steward. Information is not commingled within ODS. EDW collects information from specific ODS data marts to provide reports that source systems'

owners may need to fulfill the FEMA mission, congressional requests, or statutory requirements. Source systems' designated users of EDW set report criteria for which data elements EDW collects from ODS.

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.

EDW allows source systems to run reports based on reporting requirements. The source system owner or designee sets the data elements requested for the reports. The reports may be used for trend analysis. For instance, queries are used to compare disaster assistance applications and to look for errors in the data or reports created by the user access and interface tool. Data quality reports in the EDW may look for anomalies in the data such as misspellings, negative numbers, and wrong latitude/longitude. The EDW-generated reports help the data owners identify the issues in the data quality so they can then fix the data in the source systems. Users can only access and view information within the specific source system data mart if the source system data steward has granted the user access. A user granted access to individual disaster assistance information cannot access data from a public assistance data mart unless the public assistance source system data steward has granted that user additional access to the public assistance data mart.

For instance, a trained analyst can create a report based only on the specific ODS data mart to which the analyst has been granted access. The analyst then views and prints the ODS data as a report of disaster applicants. Then the analyst will review the report for possible matches and make a determination as to whether or not an individual already has an application for disaster assistance for the same disaster and property. This allows FEMA to delete duplicate applications and avoid duplicate benefits. EDW can help identify an individual who has applied for assistance to confirm the person's eligibility and that the person has not already requested and received aid.

An EDW report can be configured so that only data needed to determine whether or not a registrant, applicant, or employee is eligible for assistance or benefits is retrieved from the source systems. The data is used for reporting; no changes are made to the source system.

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

FEMA's ODS and EDW systems are internal to FEMA and only used by the source systems staff and authorized FEMA components.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that information within ODS and EDW may be used in a manner inconsistent with the purpose of the original collection of information.

Mitigation: This privacy risk is mitigated by ODS setting up data marts for each of the source system data. The data marts section data by source system and are only accessible by staff authorized by the source system's Data Steward. Reports are only shared pursuant to the applicable source system's SORN.

Privacy Risk: There is a privacy risk that too much information may be disclosed to individuals without authorization.

Mitigation: This privacy risk is mitigated by the system steward and the Information System Security Officer (ISSO) monitoring the use of the system for official purposes only in conjunction with governance information outlined in this PIA. Information collected is only those data fields deemed necessary by the source systems. User access is based on 'need to know' only. The source system's data steward must approve an individual's request to access the data.

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.

ODS and EDW do not collect information directly from individuals; the information is pulled by EDW from source systems described in Section 2.2. However, notice is provided to the public with respect to records maintained in ODS and EDW through this PIA and the SORNs described in Section 1.2 above.

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

ODS and EDW only provide reporting technology for FEMA's systems. Any opportunities for individuals to consent to uses, decline to provide information, or opt out of EDW reporting would be processed through the individual FEMA source system's program office, as described in Section 2.2 above.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that the individual will not have prior or existing notice of ODS' and EDW's collection and uses of information after collection by the source system.

Mitigation: This privacy risk is mitigated by FEMA providing notice to individuals through this PIA, as well as through each source systems' subsequent PIA, and the SORNs in Section 1.2.

Privacy Risk: There is also a privacy risk that ODS and EDW source systems do not have their own SORN documentation.

Mitigation: This privacy risk is mitigated by FEMA privacy and program managers completing this PIA and the PIAs and SORNs on source systems identified as collecting PII. Each source system's PIA and SORN address the source system's collection of PII and all privacy-related risks and mitigations.

Section 5.0 Data Retention by the project

5.1 Explain How Long and For What Reason the Information is Retained

The ODS and EDW systems do not currently archive data. Each source system and its data steward are responsible for records management compliance. As data is added or deleted in the source systems, it is also added or deleted in ODS and EDW during regular daily updates and refreshes. Data is retained within ODS as long as each source system's NARA-approved records retention schedule indicates. Additionally, each source system must comply with FEMA's policies and procedures for records retention. FEMA's policies and procedures for expunging data at the end of the retention period are consistent with DHS policy and guidance.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that this system retains PII longer than necessary in ODS and EDW for reporting purposes.

Mitigation: This privacy risk is mitigated by ODS' and EDW's reliance on the source system's NARA-approved retention and disposal schedule. Since ODS and EDW regularly refresh their data on a daily basis from the underlying source systems, if data is deleted from the source system, it will not be included in the next refresh of data to ODS and EDW. ODS and EDW do not have archival capabilities, thereby mitigating the privacy risk that they will retain data longer than necessary.

In addition, each source system must comply with FEMA's policies and procedures for records retention. FEMA's policies and procedures for expunging data at the end of the retention period are consistent with DHS policy and guidance. The procedures are documented by the FEMA Records Officer and follow guidelines for both paper and electronic copies.

Section 6.0 Information Sharing

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

Neither ODS nor EDW share information outside of DHS. Reports generated by EDW that are routinely shared outside of DHS are shared by the source systems program office and are shared pursuant to the source system's published routine uses within the SORN.

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

Neither ODS nor EDW share information outside DHS. Reports generated by EDW and routinely shared outside of DHS are shared by the source systems program office and are shared pursuant to the source system's published routine uses within the relevant SORN.

6.3 Does the project place limitations on re-dissemination?

Neither ODS nor EDW share information outside of DHS. Reports generated by EDW and routinely shared outside of DHS are shared by the source systems program office and are shared pursuant to the source system's published Routine Uses within the relevant SORN.

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

FEMA's Records Management Division tracks and records all requests and disclosures of information pursuant to Freedom of Information Act (FOIA) and Privacy Act (PA) requests.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that although authorized users are exposed to PII as a routine part of their official duties, they may make inappropriate disclosure of this information, either intentionally or unintentionally.

Mitigation: This privacy risk is mitigated because all ODS and EDW users are required to complete training on privacy, including the appropriate and inappropriate uses and disclosures of the information they receive as part of their official duties. A user's use of the system and access to data is monitored and audited. Should a user inappropriately disclose this information, they are subject to loss of access and the disclosure will be referred to the appropriate internal investigation entity. Additionally, users are required to undergo system access recertification annually.

Additionally, ODS and EDW do not share information outside of DHS, though the source systems may share their data consistent with the routine uses in their respective SORNs. Any disclosure request pursuant to the FOIA or PA is reviewed, tracked, and processed on a need-to-know or legal right-to-know basis.

Section 7.0 Redress

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

Individuals may submit a PA or FOIA request to gain access to their information within the appropriate source system outlined in Section 2.2 and ODS. Requests for PA and FOIA

information must be in writing. The name of the requester, the nature of the record sought, and the required verification of identify must be clearly indicated. Requests should be sent to: FOIA Officer, Records Management Division, Federal Emergency Management Agency, Department of Homeland Security, 500 C Street, SW, Washington, D.C. 20472. FEMA PA and FOIA analysts will search both the source system and ODS.

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

Corrections or amendments cannot be made directly within ODS and EDW. Individuals may submit a PA or FOIA request to correct erroneous information within the appropriate source system outlined in Section 2.2. Redress is provided through the source systems program offices. When these corrections and updates are made, they are updated or corrected in ODS and EDW during the subsequent regularly scheduled system refresh and update.

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

Individuals are notified through this PIA as well as through the SORNs listed in Section 1.2 of how to correct their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that individuals cannot access, correct or amend their records directly within ODS and EDW.

Mitigation: This privacy risk is mitigated by providing notification through this PIA and each source system's SORN on the procedures to access and correct or amend information stored within ODS. Once information is corrected or amended in the source system, ODS will be updated during its regularly scheduled updates with the corrected information.

Privacy Risk: There is a privacy risk that corrected or amended records from the underlying source systems will not update the records within ODS and EDW.

Mitigation: This privacy risk is mitigated because each source system's MOU with ODS and EDW indicates that source system data will be regularly updated in ODS to ensure accurate reporting by EDW.

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?

Pursuant to the system access procedures mentioned in Section 8.3 of this PIA, the ODS and EDW system owners and designated data warehouse administrators are responsible for the creation of new users, assignment of roles and privileges, and user account management. Users of ODS and EDW are identified by the establishment of a user ID providing access to the FEMA network. The security measures for ODS and EDW user IDs are consistent with the security controls employed by the FEMA network. ODS and EDW cannot be accessed outside the FEMA network. User account information is secured through the FEMA network administration. An additional security layer in the EDW user access and interface application authenticates users to specific roles. FEMA policy requires authorized users to ensure their access aligns with the appropriate roles in the system. Likewise, the system administrators and ISSO receive and review audit logs including failed login attempts, database users that should be removed, and super-user activity. An additional safeguard is the separation of duties (described in 8.3) to safeguard the assets of FEMA by ensuring that no single individual has the ability to view all the source system data within ODS.

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

Annual privacy training is required for all employees and contractors who use or access the ODS and EDW systems. It is the policy of FEMA that all personnel successfully complete a FEMA security training course before receiving access to ODS or EDW. The FEMA training course must correspond with the type of access required. In addition, new users must sign the ODS and EDW user access form, which includes user standards of behavior and user responsibilities.

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 that, in accordance with OMB Circular A-123, defines FEMA's internal control standard for user access privileges. This standard is applied to all requests for ODS and EDW access to ensure FEMA assets are protected from fraud, waste, and abuse.

Each source system's data steward is responsible for identifying who should see those fields containing PII when running reports on EDW. FEMA staff may request access via a web form. The form is then sent to the EDW operations staff. Upon concurrence of the requesting FEMA staff member's supervisor, the EDW operations staff creates the account. The user's roles and level of data access decision is based on the individual user's need to know and with the recommendation of the user's supervisor. The user's role is based on the source system data under their responsibility. The user level assigned is based on need-to-know.

All users with PII access levels and data stewards must read and sign the DHS Non-Disclosure Agreement, which outlines the terms of agreement for accessing information that is owned by, produced by, or in the possession of the United States Government.

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?

Any ODS or EDW system interface or information data sharing within DHS or with other outside organizations requires an MOU and/or ISA reviewed by the system steward, and will be fully vetted through the FEMA IT Security Branch, FEMA Privacy Officer, and Office of Chief Counsel prior to sending to the DHS Privacy Office for formal review and clearance. All FEMA systems will be required to comply with FEMA Office of the Chief Information Officer standard operating procedures (SOP) for Authorization to Connect to ODS and EDW. The SOP requires MOUs for all FEMA source systems connecting to ODS and EDW.

Responsible Officials

Eric M. Leckey

Privacy Officer

Federal Emergency Management Agency

Department of Homeland Security

Approval Signature

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

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

Interconnected Systems

EMMIE: The Emergency Management Mission Integrated Environment/Public Assistance Module provides automated information on grants related to public assistance and disaster mitigation. The following is a list of privacy compliance documents supporting this system:

PIA: DHS/FEMA/PIA-013 Grant Management Program, July 14, 2009.

SORN: DHS/FEMA-004 Grant Management Information Files, 74 Fed. Reg. 39705 (Aug. 7, 2009).

AFG: The Assistance to Firefighters Grant Application is the competitive grant opportunity that is administered by the Assistance to Firefighters Program Office and assesses the needs of each individual applicant compared to the other applicants interested in the opportunity. The following is a list of privacy compliance documents supporting this system;

PIA: DHS/FEMA/PIA-013 Grant Management Programs, July 14, 2009.

SORN: DHS/FEMA-004 Grant Management Information Files, 74 Fed. Reg. 39705 (Aug. 7, 2009).

IFMIS-Merger: The Integrated Financial Management Information System – Merger is FEMA's official accounting and financial management system that tracks all financial transactions. The following is a list of privacy compliance documents supporting this system:

PIA: DHS/FEMA/PIA-020 Integrated Financial Management Information System Merger, December 16, 2011.

SORN: DHS/ALL-007 Accounts Payable System of Records, 73 FR 61880, October 17, 2008 and DHS/ALL-008 Accounts Receivable System of Records, 73 Fed. Reg. 61885 (Oct. 17, 2008).

ADD: The Automated Deployment Database tracks and monitors the deployment of FEMA and Non-FEMA personnel assigned to support incident and disaster

operations.The following is a list of privacy compliance documents supporting this system:

PIA: PIA in development.

SORN: DHS/ALL-023Department of Homeland Security Personnel Security Management, 75 Fed. Reg. 8088 (Feb. 23, 2010);

DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 Fed. Reg. 5609 (Feb. 3, 2010); and

DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 Fed. Reg. 30301 (Jun. 25, 2009).

EMIS: The Emergency Management Information System evaluates and reviews FEMA-funded grant projects to ensure compliance with Environmental and Historic Preservation (EHP) laws and Executive Orders.The following is a list of privacy compliance documents supporting this system:

PIA: DHS/FEMA/PIA-013 Grant Management Programs, July 14, 2009.

SORN: DHS/FEMA-004 Grant Management Information Files, 74 Fed. Reg. 39705 (Aug. 7, 2009).

DMARTS: The Document Management and Records Tracking System provides document capture, repository, and workflow functions of data collected as the result of disaster assistance applications from individuals affected by nationally declared disasters.The following is a list of privacy compliance documents supporting this system:

PIA: DHS/FEMA/PIA-009 Document Management and Records Tracking System (DMARTS), September 8, 2008.

SORN: DHS/FEMA-008 Disaster Recovery Assistance Files,74 Fed. Reg. 48763 (Sep. 24, 2009).

NEMIS IA Module: The National Emergency Management Information System – Individual Assistance Module system processes registrations taken via the Disaster Assistance Improvement Program (DAIP/Disaster Assistance Center(DAC) and encompass a duplication of benefits function related to individual disaster assistance.

PIA: PIA in development.

SORN: DHS/ALL-008 - Department of Homeland Security Accounts Receivable System of Records, 73 Fed. Reg. 61885 (Oct. 17, 2008).

MT e-Grants: The Mitigation Electronic Grants system is an online grant application and grant management information system forstate, territory, and native american tribal governments.The following is a list of privacy compliance documents supporting this system:

PIA: DHS/FEMA/PIA-006 FEMA National Emergency Management Information System Mitigation Electronic Grants Management System, January 16, 2007.

SORN: DHS/FEMA-2006-0002 National Emergency Management Information System - Mitigation Electronic Grants Management System, 69 Fed. Reg. 75079 (Dec. 15, 2004).

HMGP-MT: The Hazard Mitigation Grant Program System is an online grant application and grant management information system forstate governments, local governments, Native American tribal governments, and private non-profit organizations.The following is a list of privacy compliance documents supporting this system:

PIA: PIA in development.

SORN: DHS/FEMA-2006-0002 National Emergency Management Information System - Mitigation Electronic Grants Management System, 69 Fed. Reg. 75079 (Dec. 15, 2004).