Privacy Impact Assessment
for the

Firehouse Database

(Unclassified and Classified)

DHS/FEMA/PIA-019

December 15, 2011

Contact Point
Judith Lainer
Office of the Chief Information Officer
Federal Emergency Management Agency
(540) 542-5793

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) Mount Weather Emergency Operations Center (MWEOC) Emergency Services Division (ESD) owns and operates two Firehouse Databases: 1) Firehouse Database (classified); and 2) Firehouse Database (unclassified). The difference between the two databases is that the classified Firehouse Database contains classified locations on which MWEOC ESD may respond at the MWEOC facility. FEMA uses the unclassified and unclassified Firehouse Database to manage the collection, documentation, and reporting of information about emergency incidents, incident investigations, site inventory and inspections, staffing, scheduling, and personnel certifications and training of FEMA paramedics, emergency management technicians, firefighters, and other first responders at MWEOC ESD. FEMA is conducting this Privacy Impact Assessment (PIA) because FEMA's unclassified and classified Firehouse Database collects, uses, maintains, retrieves, and disseminates personally identifiable information (PII) of MWEOC residents, employees and contractors, visitors, as well as members of the immediate local community surrounding MWEOC. This PIA covers both the unclassified and classified Firehouse Databases.

Overview

FEMA MWEOC is a secured facility supporting various FEMA, DHS, and government-wide missions. The MWEOC ESD ensures a ready status for these missions, providing emergency services and life safety support to all MWEOC residents, employees and contractors, visitors, as well as members of the immediate local community surrounding MWEOC. MWEOC procured and installed two Firehouse Databases: 1) Firehouse Database (classified); and 2) Firehouse Database (unclassified) to serve as a comprehensive record management system for the collection, documentation, and reporting of information about emergency incidents, incident investigations, site inventory and inspections, staffing, scheduling, and personnel certifications and training of FEMA paramedics, emergency medical technicians, firefighters, and other first responders at MWEOC ESD.

The primary responsibility of MWEOC ESD personnel is the MWEOC facilities. However, MWEOC ESD personnel provide emergency services, including emergency medical and fire, in coordination with local county and city fire departments, to members of the immediate local community surrounding MWEOC.

MWEOC ESD personnel collect information at MWEOC and in the immediate local community surrounding MWEOC when responding to an emergency. During emergency responses, investigations, or inspections, the responding MWEOC ESD personnel note all pertinent data on a standardized working form called the Mount Weather Fire and Rescue Department EMS Run Sheet (Run Sheet). Incidents involving a transfer of injured persons to medical facilities includes a written or verbal transfer of data to medical facility personnel regarding condition and vital statistics, name, phone number, age of the injured. After responding to an incident, authorized MWEOC ESD personnel with the appropriate level of systems access, enter the information about the individuals and incident into the Firehouse

Database. The information typically includes the date, time, and location of the incident, environmental factors, responder information, and contact information for individuals requesting response. In the future, information will be entered into the DHS/Office of Health Affairs (OHA) Electronic Patient Care Reporting System (ePCR). To view the ePCR PIA, go to www.dhs.gov/privacy. The ePCR system establishes a standardized approach across DHS to document care rendered by MWEOC ESD personnel and medical care providers in pre-hospital environments. The ePCR system enhances OHA's capability to evaluate quality of care delivery, quality assurance, performance improvement, and risk management activities. After administering emergency care, MWEOC ESD personnel will manually enter emergency medical care information into ePCR. The ePCR system captures all aspects of patient care, from the initial dispatch to a designated site, demographics, vital signs (initial assessment), treatment, and transfer of care and/or patient transport. After information is entered into the Firehouse Database and ePCR, the hardcopy Run Sheets are locked in a file cabinet where they are maintained until the end of the National Archives and Records Administration (NARA) approved retention period at which time they are shredded in accordance with the NARA approved retention and disposal schedule.

FEMA's Firehouse Database collects, uses, maintains, retrieves, and disseminates PII, including medical and health-related information of MWEOC residents, employees and contractors, visitors, and members of the immediate local community surrounding MWEOC that are involved in incidents requiring emergency services by MWEOC ESD personnel. This is done in accordance with 42 U.S.C. § 1856a, which specifically gives FEMA the authority to provide emergency services. FEMA uses the Firehouse Database pursuant to The National Fire Prevention and Control Act (P.L. 93-948), which established the need to collect data through the National Fire Incident Reporting System (NFIRS).

MWEOC ESD personnel share information from the Firehouse Database in report form with the U.S. Fire Administration, which collects statistics on fire incidents. In addition, MWEOC ESD personnel share information from the Run Sheets externally on a "need-to-know" basis, with appropriate hospital emergency room medical personnel to provide medical care to an individual treated by MWEOC ESD personnel. MWEOC ESD personnel share information externally in report form, such as with the Commonwealth of Virginia, Office of Emergency Services, which collects information on non-fire related emergency incidents.

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?

FEMA's Firehouse Database collects, uses, maintains, retrieves, and disseminates PII, including medical and health-related information of MWEOC residents, employees and contractors, visitors, and members of the immediate local community surrounding MWEOC. This is done in accordance with 42 U.S.C. § 1856a, which specifically gives FEMA the authority to provide emergency services. FEMA also uses its Firehouse Database pursuant to The National Fire Prevention and Control Act (P.L. 93-948), which established the need to collect data through the National Fire Incident Reporting System (NFIRS).

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

PII in the Firehouse Database is collected, used, maintained, retrieved, and disseminated in accordance with the following SORNs:

Members of the Public Medical Records: DHS/OHA – 002 Emergency Care Medical Records System of Records (August 30, 2011, 76 FR 53921); and

Federal Personnel Medical Records: OPM/GOVT – 10 Employee Medical File System of Records (June 19, 2006, 71 FR 35360);

MWEOC ESD Personnel and Training Files: OPM/GOVT – 1 General Personnel Records System of Records (June 19, 2006, 71 FR 35356).

Individuals covered by the Firehouse Database include MWEOC residents, employees and contractors, visitors, as well as members of the immediate local community surrounding MWEOC that are involved in incidents requiring emergency services by MWEOC ESD personnel. When emergency services are provided to DHS or other federal employees, their records are considered part of the OPM/GOVT – 10 Employee Medical File System of Records (June 19, 2006, 71 FR 35360). When emergency services are provided to individuals who are not DHS or other federal employees, including contractors and other members of the public, their records are considered part of the DHS/OHA – 002 Emergency Care Medical Records System of Records (August 30, 2011, 76 FR 53921). When MWEOC ESD personnel provide emergency services pertaining to care they administer while on duty, and maintain certifications and required training, their records are considered part of the OPM/GOVT – 1 General Personnel Records System of Records (June 19, 2006, 71 FR 35356).

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

A Systems Security Plan (SSP) as well as the Certification and Accreditation (C&A) process is complete for the Firehouse Database. The Firehouse Database has a current Authority to Operate (ATO) signed in August 2011 (classified) and December 2011 (unclassified).

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

The following are NARA approved authorities for the retention and disposal of information in the Firehouse Database:

Fire and other related investigative records retained and disposed of in accordance with General Records Schedule (GRS) 18, 4 (credential files) and GRS 9 – 11. MWEOC ESD personnel certification and training qualifications are included in personnel records and are therefore permanent as authorized in GRS 1 and 29B.

Survey and inspection files are destroyed when 3 years old or upon discontinuance of the facility, whichever is sooner or are destroyed when 4 years old or when security cognizance is terminated, whichever is sooner. Investigative files are destroyed when 2 years old pursuant to the GRS 18.

Identification credentials are destroyed 3 months after return to issuing office. Related papers including receipts, indexes, listings, and accountable records are destroyed after all listed credentials are accounted for pursuant to GRS 11.

Personnel records are destroyed when 5 years old or when superseded or obsolete, whichever is sooner pursuant to GRS 1.

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.

The Firehouse Database is not subject to the requirements of the Paperwork Reduction Act (PRA) because a specific form or other information collection tool completed by the public is not used to populate the information in the Firehouse Database. Information collected and maintained is done so by MWEOC ESD personnel.

Section 2.0 Characterization of the Information

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

MWEOC ESD personnel utilize the Run Sheet at the scene of an emergency incident, whether medical or fire, to collect essential information. Specific information collected in response to a medical incident (e.g., vital signs, allergies, medical history, etc.), is used to provide emergency medical assistance and then transferred to emergency room staff at the hospital. In the future, this information will also be entered manually into the ePCR system. The Firehouse Database does not need or collect medical treatment information and only maintains information needed for incident management and for EMS equipment/property inventory. The following information is maintained by MWEOC ESD:

- Maintained in the Firehouse Database, on the Run Sheet, and loaded into the ePCR system:
    - Incident address (either classified or unclassified);
    - Information on damaged property (e.g., vehicle and/or, structure information either classified or unclassified);
    - Biographic and demographic information about individuals affected by the incident:
        - Full name;
        - Phone numbers; and
        - Age.
    - Information on damaged property:
        - Property owner name; and

        - Damaged vehicle or structure information.
    - Essential medical information about individuals injured at the scene of the incident including:
        - Vital signs;
        - Allergies;
        - Medications;
        - Medical history taken from patient at incident if able; and
        - Assessment and general observations.
- Additional information in Firehouse Database Only (Not on the Run Sheet or within ePCR):
    - Unique system generated incident number;
    - Incident statistics, such as type, number, etc.; and
    - Equipment and apparatus information:
        - Inventory;
        - Equipment calibration records;
        - Annual testing requirements; and
        - General usage data on maintenance and replacement scheduling.
    - Certifications, training, and qualification information on MWEOC ESD personnel:
        - Full name (first, middle, last);
        - Professional certifications and training related to emergency response; and
        - Dates training was completed.

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

MWEOC ESD personnel collect information using the Run Sheet, visual inspections, notepad notations, and interviews directly from the individual in need of emergency assistance, either fire or medical. This information will also be entered manually into the ePCR system. MWEOC ESD personnel also collect training and qualification information directly from MWEOC ESD personnel during the application and hiring process as well as throughout their tenure to maintain competency and certification.

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

No, the Firehouse Database does not use information from commercial sources, nor does it use publicly available data.

2.4 Discuss how accuracy of the data is ensured.

MWEOC ESD personnel collect the information using the Run Sheet, visual inspections, notepad notations, and interviews directly from the individual in need of emergency assistance, either fire or medical. FEMA assumes that this information is accurate at the time it is collected. Non-incident related information is visually inspected during daily quality control checks to ensure accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Privacy risks associated with this system includes collecting information that may be considered excessive or not related to MWEOC ESD's mission as outlined in this PIA.

Mitigation: These privacy risks are mitigated by only collecting information pursuant to 42 U.S.C. § 1856a and the National Fire Prevention and Control Act (P.L. 93-948) enabling MWEOC ESD personnel to provide emergency services and life safety support to all MWEOC residents, employees and contractors, visitors, as well as members of the immediate local community surrounding MWEOC. Information collected is reviewed at least every three years through the DHS privacy compliance review process to ensure the appropriate collection and relevancy of information.

Privacy Risks: Privacy risks associated with this system includes collecting erroneous or in accurate information and using erroneous or in accurate information.

Mitigation: These privacy risks are mitigated by ensuring the accuracy of information received or collected. MWEOC ESD personnel collects information directly from individuals impacted or that witness emergency related incidents. In cases when that is not possible, FEMA attempts to use information such as driver's license, vehicle registration, or other visual identification items to ensure information collected is accurate.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

FEMA uses the information it collects in the Firehouse Database to track MWEOC ESD activity, verify incident responses, document inspection results and violations, and maintains MWEOC ESD personnel certifications, training, and qualification records. In addition, FEMA

uses the Firehouse Database information to produce reports on incidents, incident statistics, and staff personnel training needs.

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.

FEMA's Firehouse Database cannot be used for data mining and does not produce data or utilize tools to analyze data contained therein. However, the Firehouse Database does produce canned reports on incidents, incident statistics, and MWEOC ESD personnel certifications, training, and qualifications needs. There is no searching for predictive patterns or anomalies.

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

FEMA's Firehouse Database is an internal database within FEMA only used by MWEOC ESD personnel.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Privacy risks associated with this system includes using the system for purposes other than those which it was intended for.

Mitigation: These privacy risks are mitigated by monitoring the use of the system for official purposes only by the system steward and the ISSO in conjunction with governance information outlined in this PIA. Information collected is only those data fields necessary for the Firehouse Database. No additional information is collected on paper or verbally. For the Firehouse Database (classified), FEMA is following DHS Sensitive Systems Security Policy Directive 4300B, including hardening guidelines, limiting physical access to system and hardware by placing the Firehouse Database (classified) in a secure server room, and by limiting login access to only authorized MWEOC ESD personnel using dedicated workstations. In addition, for the Firehouse Database (unclassified), FEMA is following DHS Sensitive Systems Security Policy Directive 4300A, including hardening guidelines, and by limiting login access to only authorized MWEOC ESD personnel using dedicated workstations.

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.

Individuals receiving emergency services by MWEOC ESD personnel who are conscious and capable are provided with and sign a Privacy Act statement. Signatures are not obtained from individuals who are unconscious.

MWEOC ESD personnel who provide emergency services are provided with a Privacy Act statement when completing OPM SF182-1 (Authorization, Agreement, and Certification of Training) along with their certifications, training, and qualification information during the interview for hire process.

Notice is also provided through this PIA and the following SORNs:

Members of the Public Medical Records: DHS/OHA – 002 Emergency Care Medical Records System of Records (August 30, 2011, 76 FR 53921); and

Federal Personnel Medical Records: OPM/GOVT – 10 Employee Medical File System of Records (June 19, 2006, 71 FR 35360);

MWEOC ESD Personnel and Training Files: OPM/GOVT – 1 General Personnel Records System of Records (June 19, 2006, 71 FR 35356).

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

Individuals receiving emergency services have the right to decline to provide their information. MWEOC ESD personnel will still provide emergency services.

MWEOC ESD personnel who provide emergency services have the right to decline to provide their information; however, it is a condition of employment.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Privacy risks associated with this system includes transparency to individuals that 1) their information is being collected within the Firehouse Database either because they were involved in an emergency incident or because they are MWEOC ESD personnel and 2) how to correct or redress inaccurate information within the Firehouse Database.

Mitigation: These privacy risks are mitigated by providing notice to individuals, entitled groups, and entities by way of this PIA which also covers the associated SORNs in Section 1.2. This PIA serves as public notice of the existence of the Firehouse Database and the data it collects and maintains. Additionally, when possible notice, is provided at the initial time of collection via a Privacy Act statement.

Section 5.0 Data Retention by the project

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

The following are NARA approved authorities for the retention and disposal of information in the Firehouse Database:

Fire and other related investigative records retained and disposed of in accordance with General Records Schedule (GRS) 18, 4 (credential files) and GRS 9 – 11. MWEOC ESD personnel certifications, training, and qualifications are included in personnel records and are therefore permanent as authorized in GRS 1 and 29B.

Survey and inspection files are destroyed when 3 years old or upon discontinuance of the facility, whichever is sooner or are destroyed when 4 years old or when security cognizance is terminated, whichever is sooner; and investigative files are destroyed when 2 years old pursuant to the GRS 18.

Identification credentials are destroyed 3 months after return to issuing office. Related papers including receipts, indexes, listings, and accountable records are destroyed after all listed credentials are accounted for pursuant to GRS 11.

Personnel records are destroyed when 5 years old or when superseded or obsolete, whichever is sooner pursuant to GRS 1.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Privacy risks associated with this system includes information being retained for longer than necessary to accomplish the purpose for which the collection was originally planned.

Mitigation: These privacy risks are mitigated by establishing a retention and disposal schedule as outlined in Section 5.1. FEMA's policies and procedures for expunging data, including records pertaining to approved and unapproved applications, at the end of retention period are consistent with NARA and DHS policy and guidance. These procedures are documented by the FEMA Records Officer and follow NARA's GRS guidelines for both paper and electronic copies.

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.

MWEOC ESD personnel share information from its Firehouse Database in report form within FEMA to the U.S. Fire Administration, which collects statistics on fire incidents. In addition, MWEOC ESD personnel share information externally on a "need-to-know" reporting basis, such as with appropriate hospital emergency room medical personnel to provide medical care to an individual treated by MWEOC ESD personnel. MWEOC ESD personnel may also share information externally in report form, such as with the Commonwealth of Virginia, Office of Emergency Services, which collects information on non-fire related emergency incidents.

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

Public Medical Records: DHS/OHA – 002 Emergency Care Medical Records System of Records (August 30, 2011, 76 FR 53921) Shared via routine uses on an as needed basis. Specifically:

> G. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons or to comply with laws governing reporting of

communicable disease, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk.

H. To hospitals, physicians, medical laboratories and testing facilities, and other medical service providers, for the purpose of diagnosing and treating medical conditions or arranging the care of patients who have been treated by DHS EMS providers.

Federal Personnel Medical Records: OPM/GOVT-10 Employee Medical File System of Records (June 19, 2006, 71 FR 35360). Information is shared via routine uses on an as needed basis. Specifically:

B. To disclose information to a federal, state, or local agency to the extent necessary to comply with laws governing reporting of communicable disease.

O. To disclose information, when an individual to whom a record pertains is mentally incompetent or under other legal disability, to any person who is responsible for the care of the individual, to the extent necessary.

MWEOC ESD Personnel and Training Files: OPM/GOVT – 1 General Personnel Records System of Records (June 19, 2006, 71 FR 35356). Information is shared via routine uses on an as needed basis.

6.3 Does the project place limitations on re-dissemination?

Information may not be re-disseminated outside of the sharing outlined in the SORNs listed in Section 1.2 without the written permission of the individual or the FEMA Disclosure Office.

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

Under subsection (c) of the Privacy Act, FEMA retains an accounting of what records are disclosed and to whom. As identified in the SORNs outlined in Section 1.2, requests for information within the Firehouse Database are made to the FEMA Disclosure Office who maintains the accounting of what records were disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Privacy risks associated with this system includes unauthorized use or disclosure of the information in the Firehouse Database.

Mitigation: These privacy risks are mitigated by establishing that any technical interface or information data sharing within FEMA or other outside organizations will require 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 legal counsel prior to sending to DHS for a formal review. Additionally, access and security controls mitigate risks associated with misuse and inappropriate dissemination of data. Authorized users receive assignment to specific user groups with specific access rights, audit trails track and identify unauthorized uses of system

information, and data encryption is standard where appropriate to ensure that only those authorized to view the data may do so and to prevent compromise of data. The Firehouse Database (classified) complies with the DHS Sensitive Systems Security Policy Directive 4300B security guidelines for hardening criteria to secure networks, computers, and computer services against attack and unauthorized information dissemination.

Section 7.0 Redress

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

Individuals receiving emergency services by MWEOC ESD personnel may contact the Chief of the MWEOC Fire Department at: 540-542-2669 or designated representative to request a copy of an incident record and/or request a change to the record if a discrepancy is noted.

MWEOC ESD personnel who provide emergency services may contact the Chief of the MWEOC Fire Department or designated representative at: 540-542-2669 to review their certifications, training, and qualifications records. MWEOC ESD personnel initiate change requests for any noted discrepancies.

Individuals receiving emergency services by MWEOC ESD personnel and MWEOC ESD personnel who provide emergency services may also follow instructions in the following SORNs to request a copy and/or request a change to a record:

Public Medical Records: DHS/OHA – 002 Emergency Care Medical Records System of Records (August 30, 2011, 76 FR 53921); and

Federal Personnel Medical Records: OPM/GOVT – 10 Employee Medical File System of Records (June 19, 2006, 71 FR 35360);

MWEOC ESD Personnel and Training Files: OPM/GOVT – 1 General Personnel Records System of Records (June 19, 2006, 71 FR 35356).

Only designated MWEOC ESD personnel have access to the Firehouse Database for entering and amending incident reports.

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

Individuals receiving emergency services by MWEOC ESD personnel may contact the Chief of the MWEOC Fire Department at: 540-542-2669 or designated representative to request a copy of an incident record and/or request a change to the record if a discrepancy is noted.

MWEOC ESD personnel who provide emergency services may contact the Chief of the MWEOC Fire Department or designated representative at: 540-542-2669 to review their training and qualifications records. MWEOC ESD personnel initiate change requests for any noted discrepancies.

Individuals receiving emergency services by MWEOC ESD personnel and MWEOC ESD personnel who provide emergency services may also follow instructions in the following SORNs to request a copy and/or request a change to a record:

Public Medical Records: DHS/OHA – 002 Emergency Care Medical Records System of Records (August 30, 2011, 76 FR 53921); and

Federal Personnel Medical Records: OPM/GOVT – 10 Employee Medical File System of Records (June 19, 2006, 71 FR 35360);

MWEOC ESD Personnel and Training Files: OPM/GOVT – 1 General Personnel Records System of Records (June 19, 2006, 71 FR 35356).

Only designated MWEOC ESD personnel have access to the Firehouse Database for entering and amending incident reports.

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

Notification is provided though this PIA, through Privacy Act statements, as well as the following SORNs:

Public Medical Records: DHS/OHA – 002 Emergency Care Medical Records System of Records (August 30, 2011, 76 FR 53921); and

Federal Personnel Medical Records: OPM/GOVT – 10 Employee Medical File System of Records (June 19, 2006, 71 FR 35360);

MWEOC ESD Personnel and Training Files: OPM/GOVT – 1 General Personnel Records System of Records (June 19, 2006, 71 FR 35356).

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Privacy risks associated with this system includes incorrect and erroneous information about individuals within the Firehouse Database. In addition, these individuals may not be sure how to make the necessary corrections or updates.

Mitigation: These privacy risks are mitigated by the publication of this PIA which serves as public notice of the existence of the Firehouse Database and the data it collects and maintains as well as redress opportunities. Additional notice is provided through the publication of the SORNs identified in Section 1.2 and at the time of initial collection via a Privacy Act statement on forms.

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?

Auditing and accountability are conducted on a regular basis by the system steward. The Firehouse Database system steward determines which MWEOC ESD personnel have access to the database and what permissions each user needs to perform their official duties. Only

permitted users have access to system resources. Additionally, all FEMA systems are subject to a Privacy Compliance Review by the DHS and FEMA Privacy Offices to ensure compliance with this PIA and other supporting documentation.

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

Initial and annual privacy training is required of all employees and contractors who use the Firehouse Database. Initial and annual computer security awareness training is also required of all users prior to granting them access to the Firehouse Database. This training includes general information on protecting sensitive and personal information. The Firehouse Database rules of behavior signed by all authorized users highlight the proper handling and protection of privacy data.

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

The Firehouse Database system steward determines which MWEOC ESD personnel have access to the database and what permissions each user needs to perform their official duties. Only permitted users have access to system resources. Automated system enforcement and oversight of the system administrator ensure strict adherence to the access control policies. In accordance with the DHS Sensitive Systems Security Policy Directive 4300B, all system administrators, security administrators, electronic technicians, IT specialists, contractors, and MWEOC ESD personnel require a favorably adjudicated background investigation for suitability before receiving access to work on the Firehouse Database.

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 system that the Firehouse Database would interface with or share information within DHS or other outside organizations will require 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 legal counsel prior to sending to DHS for a formal review.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security