Privacy Impact Assessment
for the

Emergency Operations Center Network

DHS/FEMA/PIA-042

December 16, 2016

Contact Point
Lisa Hart
Mount Weather Information Technology Systems Division
FEMA
(540) 542-4756

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) maintains, owns, and operates the Emergency Operations Center Network (EOCNet) in support of the FEMA Mount Weather Emergency Operations Center (MWEOC) facility mission. The EOCNet is a FEMA General Support System (GSS) that is comprised of a database server that hosts three databases used to support MWEOC. FEMA is conducting this Privacy Impact Assessment (PIA) because the databases hosted on EOCNet maintain personally identifiable information (PII) from members of the public, contractors, FEMA employees, and employees from other federal agencies.

Overview

The EOCNet is a GSS that is operated and funded by FEMA under MWEOC's emergency operations mission to be "ready to support our partners at all times, under all conditions." EOCNet is a network infrastructure that enables FEMA to create databases to support their mission and office objectives. EOCNet is made up of a single database server installation – space where users can create and host databases on the FEMA Local Area Network (LAN). EOCNet hosts three separate databases: 1) the FireHouse Database[1]; 2) the Billeting Database; and 3) the Emergency Service Database. Some of the databases in EOCNet collect and contain PII. The EOCNet databases do not share data with any external partners or other DHS partners or components. The information stored on each of the EOCNet databases are only used and accessed by FEMA MWEOC employees who are granted access to the FEMA network through PIV authentication or user name and passwords, and have an authorized need-to-know. Other federal agencies also have emergency operations offices located at MWEOC; however, they do not have access to the EOCNet.

FireHouse Database

The FireHouse Database is used by the MWEOC Fire Department to store data related to the fire department operations. Such information includes: building pre-plans, building

[1] The FireHouse Database was previously documented in DHS/FEMA/PIA-019 Firehouse Database (Unclassified and Classified), December 15, 2011. While the system was named FireHouse Database, it was actually a multifunctional database comprised of various different database systems. FireHouse Database, as documented in 2011, has since been broken up and its FISMA boundaries redefined. Parts of FireHouse Database were assumed into EOCNet, and will be documented in this PIA. Other portions of the FireHouse Database were separated into their own IT systems, to include the FEMA Electronic Medical Records System (privacy compliance documentation pending) and the Physical Access Control System (PACS) (PTA adjudicated on September 12, 2014). With the publication of this PIA, FEMA is retiring the previously published FireHouse Database PIA.

inspections, fire flow calculations, and fire hydrant records. The information is accessed from the Commercial off the Shelf (COTS) FireHouse database application that is installed on the MWEOC fire chief's FEMA LAN workstation and connects back to the EOCNet database server to store and retrieve the data. The FireHouse database does not collect or store any PII. Access to the FireHouse database is limited to MWEOC Fire Department staff through operating system and database permissions access control.

Billeting Database

The Billeting Database is used by the MWEOC logistics billeting staff to store and track all overnight guest stays at MWEOC. Overnight guests may include FEMA employees and cleared contractors (who have been granted unescorted access to MWEOC by Mount Weather (MW) Office of Administrative Security), employees from other federal agencies, state and local emergency responders, or other members of the public. Visitors or employees conducting business at Mount Weather may be required to stay overnight at the facility for a various reasons, including ensuring staffing levels at the facility during inclement weather, attending an onsite training activity, or attending any supervisor-approved activity that requires non-standard work hours. All overnight guests have already been cleared for site access by the MW Office of Administrative Security through a separate clearance process[2]. All guests who visit MWEOC must be sponsored by a MWEOC federal employee. The MWEOC sponsor is responsible for the guest during the entire visit. A guest is not allowed past guards at the front gate without presenting the credentials previously approved through the MW Office of Administrative Security access control team. No site access or security data is collected or stored by the Billeting Database.

Once an overnight guest is cleared by security for MW access, the sponsor must provide the guest's information to the MWEOC Guest Registration Office prior to the stay in order to register and reserve a room for the guest. This is typically done over the phone, via email, or in person. The sponsor provides the guest's name, organization/agency, and dates of lodging. The MWEOC Guest Registration office staff enters this information into the system, which is stored in the Billeting Database for tracking and emergency contact purposes. Once the registration staff has a completed registration, a room assignment is generated for the guest, and the information is saved in the Billeting Database. Each guest is identified by name and a system generated unique identifier. MWEOC uses the information to keep a record of all overnight stays to support future logistics and financial planning, to contact or locate individuals during their stay in the event of an emergency, to validate the need for billeting, to facilitate the registration of returning guests, and to track if a guest has paid for the overnight stay.

[2] This visitor clearance process is described in the DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System (PIV/IDMS) found here: https://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-014-c-oct-2015.pdf.

When a visitor arrives at the MWEOC, he or she is screened by the front gate police using his or her credentials that were previously approved through the MW Office of Administrative Security access control team prior to the visit. When the visitor arrives at the MWEOC Guest Registration Office, he/she provides his/her name and the guest registration staff verifies the individual's identity with information in the Billeting Database. The registration staff then provides the guest with the room number and keys. Payment for the rooms is completed through a separate transaction outside of the EOCNet. MWEOC registration staff collect payment using a separate credit card reader connected to a phone line, not connected to the FEMA LAN or EOCNet. The credit card reader is a Payment Card Industry Data Security Standard (PCI DSS)-approved device that only transmits credit card data; it does not store any credit card information. PCI DSS compliance ensures that industry wide standards of encryption and access are in place per credit card vendor (e.g., VISA, American Express, and MasterCard) to secure credit card data in transit to the vendors. The Billeting Database does not contain any credit card information. It only stores the verification that a payment was received.

Each night, MWEOC staff generate a hard copy report of all the overnight guests, along with their room numbers and unique identifier. The report is hand carried with a privacy coversheet to the Mount Weather Police so that they are aware of who is staying at the facility overnight. This provides the MW Police with situational awareness and ensures that they can contact and locate guests in the event of an emergency at the facility. The reports are generated daily. Each morning, reports from the previous night are shredded or placed in burn bags for destruction.

Access to the billeting database is limited to MWEOC logistics billeting staff. Access controls and database permissions are in place to restrict access to only approved users. Additionally, user names and passwords are also required to access the billeting database.

Emergency Service Database

The MW Police and the Office of Administrative Security use the Emergency Service Database to store current and old incident reports. Anytime an incident occurs at the MWEOC (e.g., car accident, lost or stolen property), a MW police officer creates a report to document the nature of the incident and information related to the individuals involved. The contents of the report depend on the nature of the incident, but they may typically contain the name of the employee or visitor, driver's license numbers (if the incident involves vehicles), work or home phone numbers, cell phone numbers, home addresses, photographs of the incident, and any other supporting information related to the incident. When an incident occurs at MWEOC, the police officer collects data and compiles police reports for investigation and follow up purposes. The incident reports are stored in the Emergency Service Database and are used by the MW Office of Administrative Security to support follow up interviews, administrative actions, criminal complaints, or lawsuits. If the incident results in an arrest, the police officer transports the

individual to a local police department or jail for booking and fingerprinting. At that time, the individual's fingerprints are run against local, state, and federal law enforcement databases. While the fingerprints are not stored in EOCNet – they are stored at the respective police department or jail – the resulting fingerprint report is sent to MW Police and is stored in EOCNet along with the incident report. The contents of the fingerprint report include name, arrest history, criminal history, outstanding warrants, missing person status, gang affiliations, and terrorist organization affiliations.

The MW Police and the Office of Administrative Security are the operational components of the Mount Weather Emergency Services Division (MWESD), whose mission is to render MWEOC safe and secure for federal employees, officials, and visitors in a professional and cost-effective manner by deploying a highly trained and multi-disciplinary police/security force. Officers of the MW Police and the Office of Administrative Security carry out a variety of responsibilities in support of this mission, such as providing law enforcement support for special events and conducting investigations into criminal activity, including threats against employees, visitors, or federal property. In conducting these law enforcement and security functions the police officers must keep documented records of encounters with witnesses, victims, and suspects. These records include PII, which is voluntarily provided by the individuals. This information may be used in investigations by investigators, in court, or for administrative actions by FEMA. MW Police officers do not collect or store any information for incidents that occur offsite; those incidents are relayed to local police jurisdictions.

The initial incident data are usually in the form of written notes taken by the officer. The officers later transfer the report into the Emergency Service Database. The officers then either place the notes in a locked location (file cabinet, locked desk) or properly dispose of the notes in a shred bin or burn bag. Transferring the data into the database enables the MW Office of Administrative Security to easily and quickly query police reports to support ongoing or future investigations.

The incident report form only contains fields for incident date, time, incident type, and then generic text box (for free form writing). Any PII that is captured in the report is included in the generic text box. The database is set up so that officers can only query using the incident date, time, or type; the database cannot be queried using individual names or any other PII. The database does not have any analytical capabilities beyond search and retrieve functions; it does not perform any data mining activities on the data. Only the MW Police on their workstations and the Office of Administrative Security employees on their desk workstations have access to this database. Access controls are accomplished through operating system and database permissions.

Privacy Risk and Mitigations

The primary privacy risk associated with the EOCNet system is unauthorized access to the information by individuals without a need-to-know. This risk is mitigated through access controls of the EOCNet. EOCNet is PIV-enabled so all user access to the server requires PIV credentials. Each separate database relies on role-based permissions to ensure that only individuals with an appropriate need-to-know can access specific databases. The system is protected through DHS Trusted Internet Connection firewalls and intrusion detection. Furthermore, the EOCNet does not interconnect or exchange information with any other systems.

The analysis of the PIA focuses on the Billeting Database and the Emergency Service Database, as these databases collect and maintain PII.

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 legal authorities permit the collection of the billeting and incident information:

- Homeland Security Act, codified in 6 U.S.C. §§ 101 through 644. The Homeland Security Act created the Department of Homeland Security and authorizes the authority of FEMA under its auspices;
- 44 U.S.C. § 3101. Records management by agency heads; general duties. Empowers and requires the head of each federal agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities;
- 40 U.S.C. § 1315. Police powers to protect the building, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed ownership corporation thereof) and persons on the property;

- 18 U.S.C. § 13. The Assimilative Crimes Act. Allows the Federal Government to use state law to prosecute offenses committed on Federal Government land or in federally-owned buildings.

- Executive Order 12968. Access to Classified Information. Requires security policies designed to protect classified information to ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security; and,

- 44 C.F.R. § 15. Rules allows guest access with a legitimate Government interest and prohibit, among other things, access except with approval by the Administrator or Executive Director.

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

The following SORNs apply to the EOCNet system: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) System of Records,[3] which covers users access to the IT network, and DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management[4] System of Records, which covers the collection of guest registration information in the Billeting Database.

The Emergency Services Database can only conduct searches using incident date or time and incident type; the database cannot be queried using name or other personal identifier. Therefore, no SORN is required for this database.

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

An ATO was granted to the EOCNet on September 24, 2014, by the FEMA CIO. EOCNet is maintained on the FEMA/DHS FISMA inventory and complies with the DHS Management Directive 4300A.

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

Yes. The project has a NARA defined retention schedule. The information is

[3] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[4] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).

stored in the Billeting Database is retained pursuant to N1-311-86-1, Item 1H2a. Records kept pursuant to N1-311-86-1, Item 1H2a should be destroyed one year after completion of next visit or on completion of related study, whichever is first. The information stored in the Emergency Services Database is retained pursuant to GRS-18, Item 14a and GRS-18, Item 14b. Records kept pursuant to GRS-18, Item 14a are to be destroyed three years after final entry. Records kept pursuant to GRS-18, Item 14b are to be destroyed when they are two years old.

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 FEMA Records Management Division (RMD) is currently reviewing the associated forms and undergoing the PRA approval process.

Section 2.0 Characterization of the Information

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

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

Billeting Database

MWEOC Registration Office maintains the following information in the Billeting Database:

- Guest's name;
- A system generated unique identifier;
- Agency/organization;
- Guest check-in and check-out dates;
- If payment was received for room (Yes or No only); and
- Room assignment.

Emergency Service Database

The MW Police and the Office of Administrative Security collect and maintain the following information in the Emergency Service Database:

- Incident date, time, and type;
- Other incident-related details. Depending on the incident, information may include:
  - Employee's or visitor's name;
  - Driver's license number;
  - Work or home phone number;
  - Cell phone number;
  - Photograph of the incident; and
  - Home address.
- Results from fingerprint report. The contents of the fingerprint report include:
  - Name;
  - Arrest history;
  - Criminal history;
  - Outstanding warrants;
  - Missing person status;
  - Gang affiliations; and
  - Terrorist organization affiliations.

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

Billeting Database

The guest initially provides his/her information to the MW sponsor for all visits to the MWEOC facility. The MW sponsor then provides the MWEOC registration staff the relevant guest

registration information that is stored in the Billeting Database. Overnight guests may include FEMA employees and contractors, employees from other federal agencies, state and local emergency responders, or other members of the public. The MW sponsor provides the guest's information to the MWEOC registration staff either over the phone via email, or in person. Once information is collected, the MWEOC registration staff enters and stores it in the Billeting Database.

Emergency Service Database

Information stored in the emergency service database is collected directly from individuals involved in an incident. These individuals may be government employees, contractors, or visitors to the facility. The MW Police officers collect information from individuals in written police notices. After an incident, the officers enter their notes into the Emergency Service Database. In incidents leading to an arrest, the MW police officers are sent the individual's fingerprint report from the respective local police department or jail. The fingerprint report is stored along with the incident report in EOCNet.

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

The system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Billeting Database

MWEOC registration staff directly verifies accuracy of the information with the individual when he or she checks in and out of his or her room.

Emergency Service Database

The MW Police officers verify the accuracy of the information with the individual at the time of data collection. Data is validated in person at the time of collection for accuracy. In terms of the fingerprint reports, MW Police officers rely on the accuracy of local, state, and federal law enforcement databases.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Though the MW Police officers are authorized to collect information for the specific purpose of investigating law enforcement incidents, there is a risk that more information may be collected in incident reports than is necessary.

Mitigation: This is risk is mitigated because MW Police officers are required to follow specific guidelines regarding the collection of incident information. MW Police officers may only collect information that is relevant to the incident investigation.

Privacy Risk: There is a risk that inaccurate information may be collected and stored in the emergency service database.

Mitigation: This risk is mitigated because the MW Police officers verify the accuracy of the information at the time of collection. Officers collect the information directly from the individuals involved in the incident. MW Police will correct and update information in the incident reports at any time during the investigation, if they become aware of any inaccurate information.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

Billeting Database

MWEOC registration staff collects PII in order to assign and track lodging of overnight guests, and to validate a guest has paid. Additionally, each night a report is sent to MW Police Dispatch with overnight guests' names and system-generated unique identifier to provide situational awareness to MW police. This ensures that MW police can locate and contact guests in the event of an emergency. This report includes name and unique identifier to ensure the correct identity of the individual, especially in the case of individuals sharing the same names. The MW police do not use the information for any other purposes.

Emergency Service Database

The MW Office of Administrative Security requires MW Police officers to collect incident-related information, including name and other relevant PII, in order to follow up on investigations. MW Office of Administrative Security and the MW Police do not use the information for any other purposes. The database does not have any analytical or querying capabilities beyond search and retrieve functions.

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.

No.

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

No other DHS components have access to this database. It is only accessed and used by MWEOC employees with an authorized need-to-know.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information in the billeting database is used for unauthorized purposes that are inconsistent with the original purpose of collection.

Mitigation: This risk is mitigated because MWEOC registration staff only use the information in the Billeting Database to register and check-in/check-out guests, and contact or locate them in the event of an emergency. They do not use the information for any other purpose. Besides the MW Police, the MWEOC registration staff are instructed not share the information with any other entities. Additionally, MWEOC registration staff limits information collection to only what is necessary to accomplish their purpose.

Privacy Risk: There is privacy risk that information in the Emergency Service Database is used for unauthorized purposes that are inconsistent with the original purpose of collection.

Mitigation: This privacy risk is mitigated because the MW Police and MW Office of Administrative Security only use the information in accordance with their law enforcement authority, for the purpose of supporting ongoing and future investigations. The information is not used for any other purposes. The MW Office of Administrative Security use the database to query and retrieve information related to a specific incident. The database does not have any other analytical capabilities. Furthermore, the MW Office of Administrative Security can only query the database by incident date and time and incident type; it cannot search the database using names or other personal identifier. All officers and agents accessing the information, including any PII, has an authorized need to know that information.

Section 4.0 Notice

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

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

MWOEC facilities provide individuals notice prior to information collection through the Privacy Act (e)(3) statement published on the form. Additionally, this PIA and the SORNs listed in 1.2 provide serve as notice of the information collections.

Billeting Database

By seeking overnight accommodations with MWEOC facilities, the guest is agreeing to the collection of information. Additionally, a Privacy Act (e)(3) statement is published on the form. Guests also receive notice through this PIA and the SORNs listed in 1.2.

Emergency Service Database

The MW Police provide verbal notice of information collection at the time of the incident. No additional written notice is provided.

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

Billeting Database

Any overnight guest can decline to stay at the Mount Weather site and choose to stay offsite. When guests reach the registration process, they have already made the decision to stay at the MWEOC facilities and have been cleared through the MW Office of Administrative Security. By providing information to the MWEOC registration staff, the guests are agreeing to its use. Confirmations are communicated via email or telephone, and generally go through the agency sponsor or POC.

Emergency Service Database

The MW Police collect the incident information in accordance with standard law enforcement procedures. Individuals are asked for the information and they may refuse to provide the information at any time. If the information is being gathered in conjunction with an arrest, individuals can refuse to provide the information but MW Police will transport the individual to a local police department or jail for booking. At that time, local police officers or jail officials will run the individual's fingerprints against local, state, and federal law

enforcement databases. The resulting fingerprint report will yield information such as name, criminal history, arrest history, and outstanding warrants that may be necessary for the incident investigation.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that inadequate notice is provided prior to collecting information for incident reports.

Mitigation: This risk is partially mitigated. As a law enforcement agency performing law enforcement investigations, MW Police may not be able to directly provide notice to individuals prior to information collection. However, this PIA provides notice to individuals about this information collection. Additionally, officers only collect information in accordance with their law enforcement authorities under 40 U.S.C. § 1315.

Section 5.0 Data Retention by the project

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

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

The information stored in the Billeting Database is destroyed after one year per NARA approved schedule N1-311-86-1, Item 1H2a. The information is retained, for that period, and used to plan for future logistics purchases and to facilitate the registration of returning guests.

The information stored in the Emergency Services Database related to ledger records of arrests, cars ticketed, and outside police contacts are destroyed three years after final entry per NARA approved schedule GRS-18, Item 14a. Information related to reports, statement of witnesses, warning notices, and other documents relating to arrest, commitments, and traffic violations are destroyed after two years, per NARA approved schedule GRS-18, Item 14b.

5.2 Privacy Impact Analysis: Related to Retention

There is minimal risk associated with retention because the information in EOCNet is kept for a relatively short amount of time and the system has scheduled periodic purges to ensure that no data is kept beyond the retention period.

Section 6.0 Information Sharing

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

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

No, MWEOC does not routinely share any information outside of DHS. In the event that MW Police need to share incident information with external entities, such as a state or local law enforcement entity, the MW Police will get approval from the FEMA Privacy Office and Office of Chief Counsel to ensure the sharing is appropriate.

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

MWEOC does not routinely share information outside of DHS.

In the event that the MW Police needs to share information, it will coordinate with the FEMA Privacy Office and Office of Chief Counsel for review and approval of the sharing. The Emergency Services Database does not retrieve information using personal identifier, therefore no SORN is required. If the MW Police needs to retrieve a specific file, it will search the database by date and time or incident type.

6.3 Does the project place limitations on re-dissemination?

At the time of sharing, the MW Police will indicate to recipient to limit the re-dissemination of the information and only use it for authorized purposes.

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

MW Police will maintain records of any disclosures outside of DHS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be shared with unauthorized recipients.

Mitigation: This risk is mitigated because MW Police will obtain FEMA Privacy Office and Office of Chief Counsel review and approval prior to sharing information with external entities. This oversight helps to ensure sharing, when appropriate, is consistent with the safeguards in this PIA.

Section 7.0 Redress

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

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

Billeting Database

Guests are given the opportunity to review and correct their information at the time of information collection and during the check-in process. Guests also receive a receipt at the time of check-out and have the opportunity to correct any inaccurate information. Additionally, guests may consult the DHS/ALL-024 SORN listed in Section 1.2 for additional information regarding how to access their information via a Privacy Act or Freedom of Information Act (FOIA) request submitted to the FEMA Disclosure Office. Such requests should be sent to: FEMA Disclosure Officer, Records Management Division, 500 C St. SW, Washington, D.C., 20472.

Emergency Service Database

Individuals involved in incidents are given the opportunity to correct their information when the officers initially collect it. Individuals may also have the opportunity to correct erroneous or inaccurate information during the investigation. Individuals do not access their information in the database; they must communicate updates/corrections directly to the investigating officer(s).

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

See Section 7.1 above.

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

Billeting Database

Guests are given the opportunity to verify their information at the time of registration and check-in. Additionally, individuals are notified of the procedures for correcting their information through this PIA as well as through the SORNs listed in Section 1.2.

Emergency Service Database

Individuals are notified of their opportunity to correct their information at the time of collection. No additional notice is provided. The MW Police will correct the information during the course of its investigation when it is informed of inaccurate information.

7.4 Privacy Impact Analysis: Related to Redress

There are no risks associated with redress. Individuals have the opportunity to access and correct their information at any time.

Section 8.0 Auditing and Accountability

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

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

EOCNet uses a separation of access capabilities based on roles and responsibilities. All users receive annual training and receive rules of behavior prior to gaining access to the system.

Billeting Database

Access to the Billeting Database is restricted to only two individual users that are assigned to the system to perform registration functions. Access to the database can be logged and audited as necessary by reviewing database and operating system event logs containing usernames, times, dates, and database actions. These logs can be searched, filtered, and printed as necessary for audits.

Emergency Service Database

Access to the Emergency Services Database is limited to only MW Police and employees in the MW Office of Administrative Security assigned to the system. Access to the database can be logged and audited as necessary by reviewing database and system event logs. Logs contain user names, times, dates, and database actions. These logs can be searched, filtered, and printed as necessary for audits.

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

All FEMA employees and contractors are required to complete initial on-boarding and annual privacy awareness and security training.

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

Billeting Database

User access to the billeting database is granted by the database administrator with approval by the Logistics Division Director. Users must first access the FEMA LAN using their two-factor PIV credentials then have another database username/password to access the data.

Emergency Service Database

User access is granted to the emergency services database by the database administrator with approval by the Chief MWEOC Office of Administrative Security. Access to the database is controlled by Microsoft Active directory permissions and requires PIV credentials.

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?

In general, FEMA's process for reviewing and approving new MOUs and Information Sharing 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. FEMA reviews these agreements on an annual basis for appropriate security documents, for new uses of information, and for any newly identified risks. FEMA mitigates any newly identified risks between the partnering agents in accordance with applicable laws.

There are no current MOUs in place because EOCNet does not routinely share information externally or with other DHS systems.

Responsible Officials

William H. Holzerland
Senior Director for Information Management
Federal Emergency Management Agency
U.S. Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security