Privacy Impact Assessment
for the

National Responder Support Camp

DHS/FEMA/PIA - 037

May 28, 2014

Contact Point
Abraham Gunn
Office of Response & Recovery
Federal Emergency Management Agency
(202) 646-3811

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) established the National Responder Support Camp (RSC) initiative to support FEMA's mission to improve its ability to prepare for, protect against, respond to, recover from, and mitigate all hazards. RSCs are contractor-built and operated structures that are assembled (as requested) during emergencies and disasters to provide shelter, food, and other basic needs to emergency response personnel. FEMA published this Privacy Impact Assessment (PIA) for the initiative because FEMA collects personally identifiable information (PII) from the emergency response personnel to provide secured access to the RSC.

Overview

The DHS/FEMA Office of Response & Recovery (OR&R), Response Directorate (RD), Logistics Management Division (LMD) awarded contracts to establish the National Responder Support Camp (RSC) initiative. FEMA is responsible for developing an efficient logistics system for procurement and delivery of goods and services that are necessary for an effective and timely response to a natural disaster, act of terrorism, or other man-made disaster under the Post-Katrina Emergency Management Reform Act (PKEMRA).[1] This initiative upholds FEMA's responsibility to ensure the effectiveness of emergency response personnel responding to various emergencies and disasters. Responders require basic needs such as shelter, food, medical care, and other necessities to sustain response efforts during disaster situations or other emergencies. FEMA has secured contracts for the construction and operation of RSCs nationwide to meet these needs. This PIA examines the collection of PII associated with the check in and badging process at the RSCs, provision of medical aid, and privacy risks and mitigations associated with each collection.

FEMA contractors set up the RSCs during presidentially-declared disasters to provide basic needs to responders at a disaster site. RSCs services include: office spaces; lodging facilities; perimeter security (fencing and barricades); restrooms and mobile showers; morale, welfare, and recreation; power and heat ventilation and air conditioning (HVAC); kitchen and dining facilities; hand-washing stations; medical units; and waste collection and janitorial services. FEMA may request that the RSCs be phased into action when a disaster is a presidentially-declared disaster. FEMA can provide RSC services onsite to 100 personnel within the first 36 hours of a disaster, and to between 301 to 2000 personnel within 72 hours.

Contractors must provide secure, access-controlled facilities along with medical units within the RSCs for emergency personnel and responders as part of the contract requirements. Contractors register and check in all responders into the RSC, issue facility access cards (FAC), and set up badge readers at entry points so that only approved responder personnel are allowed

---

[1] 6 U.S.C. §§ 791- 796 (2006)

access into the RSCs. Contractors also provide space for medical units where trained medical staff may provide medical aid and services to responders as required.

Identity Verification and Issuing FAC

RSCs are accessible to authorized emergency responder personnel responding to the disaster or emergencies and are not accessible to the general public. This may include FEMA, DHS, or other federal, state, and local government employees, contractors, and responders, as well as volunteers from non-governmental organizations (NGO) such as the American Red Cross (herein collectively referred to as responders). RSC contractors coordinate with the FEMA Office of the Chief Security Officer (OSCO), the Joint Field Office (JFO), and the Regional Field Office (RFO) to ensure that only authorized personnel are at the disaster site and allowed access to the RSCs. All responders check in at the disaster JFO or RFO immediately upon arrival as part of the deployment protocol and process. This allows FEMA to generate a list of all responders at disaster areas and account for them. By checking in, responders are verifying that they have been deployed to respond to the disaster and should have access to the RSCs.

In most cases an individual responding to a disaster already possesses a FEMA-issued personal identification verification (PIV) card, other federal agency-issued identification (ID) card, state or local government-issued responder identification card, or other ID indicating the individual is responder personnel. Responders present their ID cards upon arrival at the RSCs to verify their identities and gain access to the RSCs. In some cases an individual responding to a disaster may not have a PIV card prior to the event (e.g., FEMA contractors or local members of the public who are hired immediately after a disaster to facilitate a response effort). FEMA OSCO conducts a suitability and background clearance process for the individual in such cases when the individual checks in at the JFO or RFO. This is the typical clearance process that all contractors undergo when onboarding as FEMA personnel. The process includes providing fingerprints, completing the PIV form (FEMA Form 121-3-1-2), and undergoing a credit check. The only difference in this case is that the clearance process is being performed onsite at the JFO. FEMA OSCO conducts the suitability and clearance process and handles all information collections in accordance with the DHS Personal Identification Verification (PIV) PIA[2] and the DHSPIV SORN.[3] All identity verification for FEMA personnel is conducted prior to their arrival at the RSCs. FEMA does not perform background checks or issue PIV badges at the RSCs.

Responders should check in at the JFO or RFO by the time they arrive at the RSCs. In doing so they verify that they have been deployed to respond to the disaster and are authorized to

---

[2] For additional information see the DHS/ALL – 014(b) Personal Identification Verification (PIV) PIA (August 23, 2012) at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_pivupdate.pdf.
[3] For additional information see the DHS/ALL - 026 Department of Homeland Security Personal Identification Verification Management System of Records Notice (SORN) at: http://www.gpo.gov/fdsys/pkg/FR-2009-06-25/html/E9-14905.htm.

access the RSCs. All responders present photo IDs issued by their home federal, state, or local agency, or volunteer organization that identifies them as a responder upon arrival at the RSCs. Contractors register responders and check them into the RSC. Contractors collect PII elements from responders including name, sponsoring organization, general contact information, emergency contact information, and date of birth in order to check the responder in to the RSC. Contractors may also check the responders identities against the original check in list generated at the JFO or RFO. The responder's PII is then entered into the RSC database, which is a standalone system not connected to the FEMA network or the internet. Collecting this information allows FEMA to maintain a roster of the RSC occupants for situational awareness purposes, and to account for the occupants. The roster is not used for any other purposes.

Once responders are checked into the RSC the contractors issue them a FAC. The FAC enables the responders to gain access to all areas in the RSC, including dining and lodging facilities. The FAC is a basic photo ID badge that contains a photograph of the responder and his or her full name. Responders present the FAC to electronic badge readers at RSC facility entry points.

Except lodging facilities, FEMA RSCs may grant limited access to authorized visitors or non-occupant RSC visitors who are able to use certain RSC services (e.g., dining or laundry) and are not living at the RSCs during the disaster. The non-occupant visitors include elected officials, fire inspectors, affected property owners, or other individuals. The FEMA RSC site lead determines who is permitted to tour, visit, dine, or use RSC facilities. FEMA determines the identity of the individuals, deciding whether they are related to the response effort, and based on the purpose of their visit. Non-occupant RSC visitors may be checked into the RSCs and issued temporary access card (different than the FAC issued to the responders). All other members of the general public are not given access to the RSCs and no one under the age of 18 is permitted in the RSCs.

Contractors collect all the FACs and destroy them by putting through a cross shredder at the conclusion of the disaster response or when the RSC is demobilized. Contractors destroy or delete any PII collected during the check in/registration process from the RSC database with the exception of copies of the roster, which FEMA may retain after the disaster in accordance to the approved records retention schedule.

Medical Information

FEMA contractors provide medical units in the RSCs that are staffed with Federal Occupational Health (FOH) nurses from the U.S. Department of Health and Human Services (HHS). Nurses provide basic care for minor illnesses and injuries including dispensing common over-the-counter medication and providing first aid. Storage space and refrigeration for personal medications is also available. RSC occupants make arrangements with the medical staff if such services are necessary.

The medical staff triages the medical needs of responders in the RSCs and determines which issues or injuries can be treated on-site and which require more in-depth examination off-site at a hospital or treatment facility. Medical staff collects and records all medical and treatment-related information that an individual receives, whether in the RSC medical units or offsite facility or hospital for record-keeping purposes, and to ensure that proper immediate and follow up treatment is provided. Medical information collected by RSC medical staff is secured in file cabinets or safes to ensure only authorized medical staff have access. All medical information collected at the RSCs belongs to the FOH nurses and HHS. FEMA does not collect, maintain, or store any medical information.

Medical staff may notify both Regional and FEMA Headquarters about an incident for situational awareness purposes depending on the severity of the medical incident. The respective sponsoring organization may also be contacted if the incident involves a non-FEMA employee. Medical staff may contact the individual's emergency contact, which is provided by the individual upon arrival to the RSCs in the event that an incident requires medical care or treatment. The medical staff maintains, uses, and disposes of the medical information in accordance with policies and procedures set forth by HHS and the Health Insurance Portability and Accountability Act (HIPAA).[4]

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 provides FEMA with legal authority to collect information for the RSC initiative:

- Title VI of the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA)[5] gives FEMA the responsibility to develop an efficient logistics system for procurement and delivery of goods and services necessary for an effective and timely response to natural disasters, acts of terrorism, and other man-made disasters.

- The Homeland Security Act of 2002[6] gives FEMA the responsibility ensure effectiveness of emergency response providers in responding to a natural disaster, act of terrorism, or manmade disaster.

---

[4] P.L. No. 104-191 (http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm)
[5] P.L. No. 109-295 (http://www.gpo.gov/fdsys/pkg/PLAW-109publ295/pdf/PLAW-109publ295.pdf)
[6] P.L. No. 107-296 (http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf)

- The Robert T. Stafford Relief and Emergency Assistance Act,[7] as amended, authorizes FEMA to provide individual and public assistance under Presidential declarations of a disaster and emergency.

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

The following SORNs cover the collection of identity verification and check in/registration information from the responders:

- DHS/ALL – 014 Department of Homeland Security Emergency Personnel Location Records SORN;[8]

- DHS/ALL – 024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management SORN;[9]

- DHS/ALL – 026 Department of Homeland Security Personal Identity Verification Management System SORN;[10]

The following SORNs cover the collection of medical information from the

responders:

- HHS 09-90-0040 National Disaster Medical System (NDMS) Patient Treatment and Tracking SORN;[11]

- OPM/GOVT – 10 Employee Medical File System Records SORN.[12]

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

Not applicable; the RSC database is a standalone system that is not connected to any other FEMA system, network, or internet.

---

[7] P.L. No. 93-288 (http://www.fema.gov/pdf/about/stafford_act.pdf)

[8] DHS/ALL-014 - Department of Homeland Security Emergency Personnel Location Records System of Records (October 17, 2008, 73 FR 61888)

[9] DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management (February 3, 2010, 75 FR 5609)

[10] DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System (June 25, 2009, 74 FR 30301)

[11] http://www.gpo.gov/fdsys/pkg/FR-2013-12-27/html/2013-31118.htm (December 27, 2013, 78 FR 78959)

[12] OPM/GOVT-10 - Employee Medical File System Records (June 21, 2010, 75 FR 35099)

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

FEMA contractors destroy or delete all RSC registration data from the database at the conclusion of the event once the RSC is shut down, with exception to the RSC occupant roster. FEMA may retain the RSC occupant roster in accordance with a pending NARA retention schedule. FEMA's Records Management Division (RMD) is collaborating with partner agencies and NARA to establish an approved retention and disposal schedule for the RSC occupant rosters that is consistent with the above referenced SORNs and the mission-driven needs of the agency. This data will be retained until the retention schedule is approved. This PIA will be updated and all data will be retained and disposed of in accordance with the NARA-approved schedule, including retroactively, once NARA has approved the retention and disposal schedule.

Any medical information collected at the RSC by the FOH nurses is retained in accordance to HHS retention policies and procedures.

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 RSC check in/registration process is currently under review for Paperwork Reduction Act requirements.

Section 2.0 Characterization of the Information

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

Responders must present their federal, state, or local government or volunteer organization photo identification upon arrival to the RSCs. Contractors register and check in the responder as an occupant of the RSC. During this process, the contractor may collect the following information from all responders (federal, state, local, or volunteers) and non-occupant visitors:

- Name;

- Contact information (email, address, and phone number);

- Date of birth;

- Sponsoring organization; and

- Emergency contact information.

The medical staff at the RSCs is comprised of FOH nurses from HHS. They may collect the following medical-related information from responders that require medical attention or treatment:

- The nature of the medical incident or injury;

- Any actions or treatments taken (e.g., referred to hospital for further examination);

- Emergency contact information (name, email, address, and phone number).

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

Contractors collect the check in/registration information directly from the responders and non-occupant visitors at the RSCs and enter the information into the RSC system database and issue a FAC to the responders or a temporary access card to the non-occupant visitors. Medical staff collects and records medical information before (or as) the responder is treated. Emergency contact information is collected directly from the responders upon arrival to the RSCs through the check in process.

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.

2.4 Discuss how accuracy of the data is ensured.

Contractors collect check in/registration information directly from responders so the information is assumed to be correct and accurate. Contractors can also check the responder's identities against the original check in list generated at the JFO or RFO to verify that the responder is involved in the disaster effort and should be at the RSC. If there are any inaccuracies or discrepancies, the contractor or FEMA may call the JFO or RFO to verify the responder's identity.

Medical staff collects medical information directly from the responders. Any medical information collected is based on the professional assessment of the medical staff or other medical professional treating the responder and is assumed to be correct. Emergency contact information is also collected directly from the responders and is assumed to be correct.

2.5 **Privacy Impact Analysis**: Related to Characterization of the Information

Privacy Risk: There is a risk that sensitive personally identifiable information (SPII) may be collected, or that more information than what is necessary may be collected from the responders.

Mitigation: FEMA mitigates this risk by only collecting information that is relevant and necessary to checking the responders into the RSC and maintain a roster of occupants for situational awareness. Contractors collect only limited PII data elements (name, contact information, emergency contact information, organization, and date of birth); no sensitive PII is collected. The FAC contains only a photo and the name of the individual for identification and access control purposes.

Privacy Risk: There is a risk that inaccurate information may prevent responders from gaining access to the RSCs.

Mitigation: FEMA mitigates this risk by collecting information directly from individuals, and therefore assumed to be accurate. Responders are given the opportunity to review their information and correct any inaccuracies. Furthermore, responders must present a photo ID card (which is issued by a sponsoring federal, state, or local government, or organization) that identifies them as responders and verifies that they should have access to the RSCs.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

This information is used to verify that responders are authorized to be at the RSC and to check responders in as occupants of the RSC. Contractors issue FACs to the responders, which allow them access to the RSC facilities once the responders are checked in. FEMA may use this information to maintain situational awareness of who is staying at the RSCs to keep track of responders and ensure they are accounted for. Information from non-occupants is also collected to keep track and account for all visitors.

FEMA uses this information to provide immediate and/or follow up treatment to the responders. The medical information may be shared as appropriate if responders require further medical attention or treatment from offsite medical facilities or hospital. The medical information may also be shared with FEMA Regional or Headquarters Office, or the sponsoring office of the responder for situational awareness purposes depending on the severity of the incident. Emergency contact information is only used in the event that an incident requires notification of next of kin. All information collection by the HHS system is done so under HHS's

legal authority to collect such information. Contractors are only involved with the registration when responders arrive to the RSCs.

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.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information collected may be used for unauthorized purposes.

Mitigation: FEMA mitigates this risk by using the check-in/registration information to maintain a roster of the RSC occupants for situational awareness purposes. RSC occupant and non-occupant badges are used to gain access to RSC facilities. The information is not used for any other purposes. Medical information is used to provide immediate or follow up treatment to responders. Emergency contact information is only used in the event an incident requires next of kin to be notified.

Privacy Risk: There is a risk that unauthorized parties may seek or gain access to the information.

Mitigation: FEMA mitigates this risk by ensuring the computer system has access controls in place that restricts access to authorized users with an appropriate user ID and password. This privacy risk is also mitigated by limiting check in/registration information to basic PII that is entered into a standalone system that is not connected to a network or the internet.

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.

Contractors may provide verbal and written notice through a Privacy Act Notice to the responders and non-occupant visitors at the time of the check in/registration information

collection. This PIA and the applicable SORNs also serve as notice for information collection at the RSCs.

Medical staff and HHS are responsible for providing notice of information collection to the responders seeking medical treatment. This PIA also serves as notice of the information collection.

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

Responders are given the opportunity to decline (or "opt-out") to provide check-in/registration information to contractors at the time of information collection. However, by opting-out they may not be issued a FAC or permitted access to the RSC facilities.

Responders are not given the opportunity to decline to provide medical information; if responders seek medical treatment or attention from medical staff, medical information will be collected. This information is collected to ensure that the appropriate immediate and follow up treatment is provided to the responder.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that responders are unaware of how their information is collected and used.

Mitigation: FEMA mitigates this risk by giving responders verbal and written notice during the check-in process that FEMA is collecting information. This PIA also provides notice of this information collection. With regards to medical information, FOH nurses provide notice at the time the data is collected, as needed, to give the necessary medical assistance. Medical information collected from responders is only used to ensure proper treatment and care.

Section 5.0 Data Retention by the project

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

Contractors destroy or delete the check-in/registration information from the RSC database at the conclusion of the disaster response or when the RSC is demobilized. All FACs are collected and destroyed as well, except for the RSC roster. FEMA may maintain the roster of RSC occupants and non-occupant visitors in accordance with the approved records retention schedule, once it is developed. FEMA may maintain this information for situational awareness purposes and to account for responders staying at the facilities and visitors during the disaster response. Contractors are required to notify FEMA when RSCs are demobilized and information is disposed.

The medical information collected from responders is retained in accordance with approved HHS retention schedules and policies; FEMA does not retain this information.[12]

5.2   Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be retained longer than required, increasing potential risk of unauthorized disclosure of PII.

Mitigation: FEMA mitigates this risk by retaining only limited, non-sensitive PII of responders in accordance with an approved records retention schedule. Medical staff retains medical information in accordance with HHS-approved records retention schedules, policies, and procedures.

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.

Contractors and FEMA do not typically share the check in/registration information outside of DHS as part of the normal agency operations. However, FEMA may provide information on a case-by-case basis about those specific responders to the sponsoring organization if a sponsoring organization (from state, local government, or non-governmental organization) is trying to locate or account for its personnel. HHS medical staff collects and stores the medical information that may be shared with medical professionals at offsite medical facilities or hospitals to ensure proper care is provided to the responder. Information may also be shared with the responder's sponsoring agency for situational awareness depending on the severity of the medical situation.

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

The DHS/ALL – 014 Department of Homeland Security Emergency Personnel Location Records SORN allows FEMA to collect and disclose information to state, local government, or non-governmental organization to support proper coordination and assistance during a disaster response. Sharing check-in/registration information is compatible with the original purpose for information collection identified in the SORN. All information sharing is consistent with the routine uses published in the SORN. Any sharing of medical information is done in accordance with HHS policies and procedures and the routine uses listed in the HHS 09-90-0040 NDMS Patient Treatment Tracking SORN.

---

[12] http://www.gpo.gov/fdsys/pkg/FR-2013-12-27/html/2013-31118.htm (December 27, 2013, 78 FR 78959)

6.3 Does the project place limitations on re-dissemination?

Yes, any information sharing is done pursuant to routine uses listed in the applicable SORN. Information is only shared with individuals with an authorized need to know. It is the responsibility of medical facilities and hospitals to comply with their respective privacy policies and procedures when sharing the information. The FOH nurses may share medical information in accordance with HHS policies and procedures, and the routine uses listed in the SORN. Medical facilities and hospitals must comply with applicable privacy laws regarding medical information, including HIPAA.

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

The FEMA RSC site lead is responsible for maintaining a record of any disclosures outside the Department. HHS is responsible for complying with its own policies, procedures, and other applicable laws and regulations, including HIPPA in regards to sharing medical information outside of DHS.

6.5 <u>Privacy Impact Analysis</u>: Related to Information Sharing

Privacy Risk: There is a risk that information could erroneously be disclosed.

Mitigation: FEMA mitigates this risk by only disclosing information pursuant to the routine uses of the applicable SORNs listed in 1.2. Medical staff discloses medical information to outside agencies (i.e., hospitals or other medical facilities) as necessary, in accordance with HHS policies and procedures and other applicable privacy laws, including HIPAA.

Section 7.0 Redress

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

Responders are given the opportunity to review their information during the check in process. FEMA may maintain a copy of the roster in accordance with the pending NARA retention schedule. Responders may consult the SORNs for additional information regarding how to access their information via 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 Street, SW, Washington, DC 20472.

Responders can consult the HHS SORN to submit HHS FOIA Officer to access their medical information.

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

Responders are given the opportunity to correct any inaccurate check-in/registration information at the time of data collection. Responders can also follow the procedures outlined in 7.1 above to correct inaccurate information. Medical information is based on the professional assessment of the medical staff or medical professional. Responders are not given the opportunity to correct that information because they do not have the expertise to do so. Any medical information provided by the responders is assumed to be correct. Responders may provide additional medical information to the FOH nurses, as needed.

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

Responders are given the opportunity to review the check in information for accuracy at the time of original collection. Additionally, this PIA and the SORNs listed in 1.2 notifies responders about procedures for correcting their information.

7.4   <u>Privacy Impact Analysis</u>: Related to Redress

<u>Privacy Risk</u>: There is a risk that if inaccurate information is collected from the responder, proper identity verification cannot be performed preventing the responders from getting access to the RSCs.

<u>Mitigation</u>: FEMA mitigates this risk by giving responders the opportunity to check and correct any inaccurate information at the time of information collection. Responder's names may also be checked against the original check in list generated by the JFO or RFO to verify the responder's identity. If there are any discrepancies or inaccuracies on the list the contractors or FEMA may contact the JFO or RFO for verification.

<u>Privacy Risk</u>: There is a risk that responders may not be aware of the redress process.

<u>Mitigation</u>: FEMA mitigates this risk by providing notice through the applicable SORNs listed in 1.2 and this PIA. Responders are also given the opportunity to correct any inaccurate information at the time of data collection.

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?

Badge readers and the database that are used to input check-in/registration information and issue badges are only accessible with appropriate user ID and password. The database is a standalone system that is not connected to any other systems, network, or the internet. All FEMA

contractors working at the RSC are issued FEMA PIV cards stating that the individual is "Under Contract to FEMA" so that he or she is easily identified. FEMA ensures the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, standard operating procedures (SOP), auditing, and accountability.

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 successfully meet initial and annual privacy awareness and information-security training requirements according to FEMA training guidelines. The training makes users aware of what PII is and the risks associated with handling PII. Users are also trained to prevent and mitigate these risks. FEMA provides supplementary security-related training to those with additional security-related 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 provides guidance and oversight to the contractors by ensuring the appropriate SOPs, statements of work, and training are in place prior to any information collection. Contractors provide a copy of the RSC rosters only to designated FEMA personnel and do not share the information with any other entities. Medical staff is comprised of FOH nurses from HHS and only designated medical staff has access to medical information collected from responders.

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?

It is rare that FEMA shares the check-in/registration information outside of DHS, uses the information in new ways, or allows system access by outside organizations. However, FEMA follows strict guidelines in the event that these processes are necessary. For example, FEMA only shares check-in/registration information in limited situations in which a sponsoring organization is trying to locate or account for its personnel. FEMA reviews each instance on a case-by-case basis to ensure it is appropriate to share this information.

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.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security