Privacy Impact Assessment

for the

Federal/Emergency Response Official (F/ERO) Repository

DHS/FEMA/PIA-017

June 20, 2011

Contact Point
Kenneth Wall
National Capital Region Coordination
Federal Emergency Management Agency
(202) 212-1600

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

Abstract

The Federal Emergency Management Agency (FEMA) Office of National Capital Region Coordination (NCRC) owns and operates the Federal Emergency Response Official (F/ERO) Repository.[1] FEMA uses the F/ERO Repository as the authoritative data source to identify and verify federal employees/contractors, and participating non-federal employees/contractors likely to respond during times of response and recovery for natural disasters, terrorism, or other emergencies. The F/ERO Repository allows for immediate electronic verification of an employee/contractor's personal identity and emergency management attribute at a given disaster zone. The purpose of this Privacy Impact Assessment (PIA) is to document how FEMA collects, uses, maintains, and disseminates personally identifiable information (PII).

Overview

FEMA's mission is to support our nation's citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. The F/ERO Repository provides a centralized way to electronically verify identity of federal and contractor employees responding to a hazard/disaster. The F/ERO Repository supports Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53). Public Law 110-53 requires the Administrator of FEMA to provide a credentialing standard, including detailed written guidance, to each federal agency that has responsibilities under the National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), and the National Continuity Policy Implementation Plan (NCPIP). Public Law 110-53 applies to incident management personnel, emergency response providers, other personnel, and resources supporting the response to a natural disaster, act of terrorism, or other emergencies. The NRF, NIPP, and NCPIP are guides that detail how the Nation conducts all-hazards response – from the smallest incident to the largest catastrophe. The NRF, NIPP, and NCPIP are written especially for government executives, private-sector businesses, and nongovernmental leaders and emergency management practitioners. Not later than six months after receiving the standards, each federal agency with responsibilities are to be credentialed and typed in accordance with the standard. FEMA defines the standard to include the NRF, NIPP, NCPIP, and other national doctrine, Federal Information Processing Standards (FIPS) 201 infrastructures and credentials, and a shared-service (F/ERO Repository) to manage attributes. The NCRC is the lead agent for execution of a pilot that will interface with Homeland Security Presidential Directive (HSPD)-12/FIPS-201 infrastructures for emergency preparedness registrations of public identities.

The F/ERO validation includes three processes: 1) Credential Issuance; 2) F/ERO Registration; and 3) Access Validation. Of these three processes, FEMA directly manages only the F/ERO Registration processes; the F/ERO agency and the jurisdictional authority in charge of the incident control the other two processes.

Credential Issuance

[1] The term F/ERO Repository throughout the PIA refers to the IT system or repository. The term of FERO refers to the designation of Federal Emergency Response Official provided to federal employees only. The use of F/ERO (with a slash) refers to Emergency Response Officials at the federal, state, and local level.

An agency gathers and maintains core information about the identities of its personnel during the credential issuance process. The agency uses the information for access authentication and authorization per the DHS Personal Identification Verification (PIV) PIA[2] and the DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System, June 25, 2009, 74 FR 30301 System of Records Notice (SORN).[3] Each agency is the owner of employee credential/encrypted certificates.

F/ERO Repository Registration Process

Federal Registration

After a federal agency, such as FEMA, provides an employee with a PIV badge[4] and the designation of a F/ERO sends an electronically encrypted certificate containing the credential/PIV badge and F/ERO status of each employee with an active clearance/employment status to the F/ERO Repository. The certificates contain the following data elements:

- Cardholder Name
- Issuing Certificate Authority
- Valid from / to dates
- Certificate serial number

The F/ERO Repository maintains the encrypted certificate of all F/EROs for participating federal agencies. In addition, the process requires each agency's IDMS system to refresh F/ERO with current credential status every 18-hours to ensure certificates reflect the employees who are currently assisting in the response. If the responsible agency does not update an encrypted certificate, the certificate is purged or deleted from the F/ERO Repository at the end of 18 hours.

Non-Federal Registration to include Legislative and Judicial Branches and State, Local, Tribal, and Territorial Entities

The process for non-federal registration for F/EROs includes the same process as federal registration except there is no PIV badge. The F/ERO Repository receives this information from non-federal entities via the individual identity verification and management system. This transmittal occurs on a push basis via a HTTPS secure internet connection, and data concerning the individual's active or inactive status is refreshed at least every 18 hours.

Access Validation

Once DHS has approved a jurisdiction/agency to be a part of F/ERO, the jurisdiction/agency must invest in both a management stations and validation device. These two items allow the jurisdiction/agency to validate individual credentials during a disaster.

---

[2] For additional information see the DHS Personal Identification Verification (PIV) PIA (June 18, 2009) at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_pivupdate.pdf.
[3] For additional information see the DHS Personal Identity Verification Management System SORN at http://edocket.access.gpo.gov/2009/E9-14905.htm.
[4] Note the PIV badge is created in accordance with HSPD-12.

Each federal, state, local, and other approved entities own and maintain the management stations and/or validation devices. The management stations and validation devices must contain the necessary software to connect to the F/ERO Repository. The General Services Administration (GSA) has approved the software[5] necessary to access the F/ERO Repository. Each management station/validation device must satisfy strict authentication criteria prior to accessing data and automatically querying the F/ERO Repository.

F/ERO Validation

To validate identity, the F/ERO inserts the PIV credential into the validation device. The F/ERO enters a Personal Identification Number (PIN) into the validation device. The device matches the PIN to the PIN stored on the PIV credential. If the PINs match, the process proceeds to an examination of fingerprint biometrics. The F/ERO places a finger on the validation device, which scans the print and compares it to the biometric identifier stored on the PIV credential. A positive match to the PIN and biometric provides identity validation, which unlocks the F/ERO's name and other information electronically stored on the PIV credential.

The validation device transmits the unique identifier, the F/ERO's name, and a record of the validation to the management station. The jurisdictional authority uses the data from the management stations to compile an incident manifest of the F/EROs on deployment to a disaster area and available to assist in continuing response and recovery efforts.

Local jurisdictions own management stations and validation devices. The device does not retain any record of the PIN or fingerprint data presented by the employee and/or contractor or contained on the PIV credential. It does record the occurrence and outcome of the validation process. Since jurisdictional authorities include local authorities, the management workstation, validation device, and resulting list may not be protected under federal privacy requirements.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The F/ERO Repository collects, uses, maintains, and disseminates several data elements in the FEMA F/ERO Repository 3-step process: 1) credential issuance; 2) F/ERO registration; and 3) access validation. However, each process does not require all of the data elements. The following explains the usage of information for each of the three steps:

Step One: Credential Issuance

Identity Management System (IDMS)

[5] The software is on the GSA Approved Product List. Owners of the management stations and validation devices may purchase the software from GSA vendors to download onto the management station and/or validation device.

- PIN
- F/ERO Attribute (Emergency Support Function i.e., fire fighter or Sector i.e., Critical Manufacturing)
- Current Status
- Name
- Date of Birth
- Social Security Number
- Organizational Affiliation
- Employment Type
- 10 Fingerprints
- Biometric Identifiers-2 fingerprints
- Digital Color Photograph
- Digital Signature
- Telephone
- Address History
- Signed PIV Request
- Signed SF-85 or equivalent
- Copies of Source Identity Documents

2. PIV-Physical Characteristics

- F/ERO Attribute (red stripe)
- Name
- Organizational Affiliation
- Employment Type
- Digital Color Photograph

3. PIV-Electronic Information

- PIN
- F/ERO Attribute
- Current Status
- Organizational Affiliation
- Employment Type
- Biometric Identifiers-2 fingerprints
- Digital Color Photograph
- Digital Signature

Step Two: F/ERO Registration (encrypted information (alphanumeric—no PII) from agencies to FEMA F/ERO Repository)

- Alpha-numeric Unique Identifier
- F/ERO Attribute
- Current Status

Step Three: Access Validation (local jurisdictions (not FEMA)

1. Management Station
   - PIN
   - F/ERO Attribute

- Current Status
- Name (only after validation occurs and a manifest is created)

2. Validation Device

- PIN
- F/ERO Attribute
- Current Status
- Name (only after validation occurs)
- Biometric Identifiers-2 fingerprints (Collected for validation purposes but not retained beyond the time needed to validate, which is approximately 17 seconds.)

The F/ERO Repository receives and aggregates the following information for each F/ERO assigned by a federal agency

- Public PIV authentication certificate extracted from the PIV credential
- Attribute(s)
- Workstation or server internet protocol (IP) address of the individual or entity that assigned the attribute(s)

1.2 What are the sources of the information in the system?

The source of the F/ERO identification and attribute information comes from each respective agency's PIV issuance infrastructure that is registering F/EROs. Under the NRF, NIPP, NCPIP and associated emergency management governance documents, each agency appoints an Attribute Administrator who will name its agency F/EROs and assign each F/ERO an attribute/designation. The F/ERO Repository will eventually have the capability of receiving information from state, local, tribal, and territorial governments, voluntary organizations, and critical infrastructure/key resources communities. See Appendix B for a complete list of agency issuance infrastructures providing information to the F/ERO Repository.

Each HSPD 12 Infrastructure requires:

Electronic Identity Management System/Card Management System – these systems act as the "traffic cop" linking sponsorship, identity screening and credential issuance and maintenance:

- Certificate Authority (cross certified with the federal Bridge Certification Authority) Enrollment Capability
- Personalization Capability
- Post-Issuance Capability

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is being collected as required by the standard defined in response to P.L. 110-53. All agencies of the federal executive branch with responsibilities under the NRF, NIPP, and/or the NCPIP are required to designate F/ERO responsibilities to agency personnel. Each participating agency appoints an Attribute Administrator to identify its agency F/EROs and assign each F/ERO an attribute. FEMA

uses the information to develop reports to federal leadership outlining the preparedness posture of the federal government based on agency and attributes. The information is used at an incident scene to assist commanders by providing human situational awareness capabilities that allow them to re-allocate existing personnel or request additional personnel as required.

1.4 How is the information collected?

Each agency's Attribute Administrator is responsible for sponsoring and determining the F/ERO designation and attribute or revoking the electronic registration of F/ERO attributes. This registration information is transmitted to the F/ERO Repository on a cycle never to exceed 18 hours. F/ERO Repository registrations or revocations are achieved in one of two ways:

- Manual solution – agency PIV post-issuance process using a computer, FIPS-201 credential reader, and registration application software. The process is the same for non-federal entities.
- Automated solution – the agency PIV issuance process uses the agency issuance infrastructure to interface with the F/ERO Repository via the Back-end Attribute Exchange (BAE) standard. The process is the same for non-federal entities who possess the technology to interface with the F/ERO Repository via the BAE standard.

Additionally, F/ERO collects information via each agencies validation device at the disaster zone. Each individual provides verification information upon entrance to a disaster zone via a validation device. The information is securely transmitted to the F/ERO Repository for positive or negative identity verification.

1.5 How will the information be checked for accuracy?

Each agency is responsible for the currency or revocation of registered F/ERO information to ascertain accuracy every 18 hours.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The following define the requirements for the collection of F/ERO information:

- Title IV of P.L. 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007"
- Homeland Security Presidential Directive-12
- Fair Information Processing Standards-201
- National Institutes of Standards and Technology 800 -79 (Guidelines for the Certification and Accreditation of PIV Credential Issuing Organizations)
- Federal Public Key Infrastructure Common Policy
- DHS/All-026 Personal Identity Verification Management System of Records Notice (74 FR 30301, June 25, 2009)

- National Incident Management System (NIMS) Credentialing Guideline for F/EROs

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: Unauthorized parties may seek to access data contained in the PIV Authentication certificate.

Mitigation: The F/ERO Repository contains the PIV Authentication certificate (a PKI certificate in accordance with federal PKI and common policy) which is provided to all PIV bearers at issuance. It also contains the attribute bound to that individual only, which designates the F/ERO responsibility represented in object identifier format for each individual designated by their agency Attribute Administrator who to respond to a disaster scenario. Section 9.4.3 of the *X.509 Certificate Policy for the US Federal PKI Common Policy Framework* states, "information included in PKI certificates is not deemed private."

Certificates that contain the Federal Agency Smart Credential Number (FASC-N) in the subject alternative name extension, such as PIV Authentication certificates shall not be distributed via public repositories (e.g. via LDAP or HTTP). The F/ERO Repository is not a publicly accessible repository. Authorization to review the data in the repository is assigned to Attribute Administrators of that data for that agency only, and only after authentication is satisfied using a PIV credential, which provides a very high level of identity assurance as defined by E-Authentication standards. Risk is mitigated in this means by using trusted identity credential issuers.

Privacy Risk: Data collected in the F/ERO Repository may not be secure.

Mitigation: In addition, each federal agency has previously issued a PIA related to the PKI certificates and other PII related to all PIV credentials issued because of HSPD-12. The actions of the F/ERO Repository do not adversely affect PIAs issued previously or provide any additional adverse consequence. The F/ERO Repository does not maintain PII, there is a minimal risk that the data in the F/ERO Repository is lost, compromised, or disclosed without authorization, can result in inconvenience or unfairness to the individual. To mitigate these risks, FEMA is required to follow specific guidelines relative to data integrity regarding the issuance of HSPD-12/FIPS-201 credentials. Additionally, FEMA has sought to collect no more information than necessary to verify employees and/or contractors and services provided during a disaster.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The F/ERO Repository uses information to identify the F/EROs with the necessary qualification and credentials on-scene to respond to emergencies. The law enforcement official or a relying party uses this information to determine if the F/ERO can gain access to the incident scene. A relying party relies on

results of an on-line authentication to establish the identity or attribute of a subscriber for the purpose of some transaction. The verifier and the relying party may be the same entity, or they may be separate entities. If they are separate entities, the relying party normally receives an assertion from the verifier. The relying party ensures that the assertion came from a verifier trusted by the relying party. The relying party also processes any additional information in the assertion, such as personal attributes or expiration times. Examples of other uses of this information is for Stafford Act reimbursement; for monitoring movement of personnel into, out of, and within the incident scene; and for assessing liability issues in incidents involving hazardous materials, as experienced during and after 9/11.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Data in the F/ERO Repository synchronizes with incident scene management stations so that authentication of those required to respond to an incident scene can be authorized by a relying party official and the capability and authorization to receive the F/ERO Repository transmissions.

Transaction data collected at the incident scene is the electronic challenge/response of a FIPS-201 compliant or FIPS-201 interoperable credential via a handheld reader. Transaction data collected by individual handhelds is aggregated and digitally signed in the on-site management station by those assigned access rights at the scene and only using a FIPS-201 compliant or interoperable credential for authentication. The transaction data forms a digitally signed electronic manifest and is transmitted by Satellite Communications (SATCOM) or other communication capability to Emergency Operation Centers (EOCs) that require the data for situational awareness of the response to a disaster.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The F/ERO Repository does not use any commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Each agency has an internal process based on the FIPS 201to determine individuals with a need for a PIV credential based on job requirements. The internal process must meet the criteria contained in FIPS 201, have a PIA approved, and a Certification and Accreditation (C&A) conducted of the issuing infrastructure, which meets Federal Information System Management Act (FISMA) compliance. The issuing agency is the entity responsible for identity proofing of all PIV applicants and the assignment of the F/ERO designation in accordance with NRF, NIPP, and/or NCPIP policy. The F/ERO Attribute Administrator in each agency provides the final approval for the assignment of a F/ERO attribute designation to an applicants' PIV credential and designates additional agency Attribute Registrars. Attribute Registrars must meet the following minimum standards:

- A federal government official and designated in writing as an Attribute Registrar;

- Capable of assessing the integrity of the Applicant's PIV credential (i.e. is trained to detect any improprieties in the applicant's PIV credential); and
- Capable of evaluating whether a F/ERO application is satisfactory and apply organization-specific processes to an unsatisfactory F/ERO application.

The individual federal agency sponsoring the issuance of a PIV credential and assignment of the F/ERO designator owns the data transmitted to the F/ERO Repository. Data contained in the F/ERO Repository is only revisable or updatable by the machine-to-machine transmission described previously between the issuing infrastructure and the F/ERO Repository. Data in the F/ERO Repository refreshes on a routine cycle never to exceed an 18-hour period. Each agency can only view and query their own F/ERO data with access rights assigned by the F/ERO Attribute Administrator and only using a PIV credential for authentication. One agency cannot view another agency's F/ERO data. The ability to retrieve or view the F/ERO Repository is controllable by user authentication, which ensures only those with a need to access the data and who possess proper training can retrieve or view information.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The F/ERO Repository retains all information it collects. See section 1.1 for a list of specific data elements.

3.2 How long is information retained?

FEMA retains information until: a) the F/ERO is removed from the repository by the agency; b) the F/ERO's attribute(s) are revoked; or (c) the F/ERO's identity certificate(s) expires without renewal which is 3 years after issuance, in accordance with FPKI policy. Additionally, this information is updated every 18 hours, at a minimum.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, pursuant to NARA General Records Schedule (GRS) 20 "Electronic Files," item 9 " Finding Aids (Indexes)," F/ERO Repository records used as electronic indexes, lists, registers, and other finding aids are deleted with related records or when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes, whichever is later.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: Managing records longer than required increases the amount of harm resulting from an authorized disclosure of information.

Mitigation: To mitigate this risk, records are kept only for the time necessary to complete the verification process.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The information in the F/ERO Repository is shared within all DHS components that require electronic validation of F/ERO identity and attribute(s) for those personnel with responsibilities as defined in the NRF, NIPP, and NCPIP for National Preparedness.

4.2 How is the information transmitted or disclosed?

The HSPD-12/FIPS-201 issuing infrastructure for DHS-sponsored F/EROs transmits data to the F/ERO Repository and can be queried by authorized personnel within DHS only using a FIPS-201 compliant credential for authentication.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: The risk associated with internal sharing of information maintained is that individuals without a need to know could possibly access an employee and/or contractor's credential information by accessing an unsecure website or transmission. Additionally, an individual without a need to know could use the certificates to gain unauthorized access to other need to know information.

Mitigation: To mitigate this risk, the access to the F/ERO Repository information is based on user roles and responsibilities and requires a PIN and credential holder's unique identifier in order to access the information. Additionally, access to information within the F/ERO Repository is via a secure web transmission. Registered users that abuse their rights will have their rights removed and will not be allowed to access the system. Individuals trying to or gaining access to the system by "hacking" are prosecuted to the fullest extent of the law.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

FEMA shares F/ERO Repository information with any entity that requires validation of federal PIV credentials, including but not limited to all federal, state, local, tribal, and commercial organization with software to validate and track entry of PIV badges at disaster locations. The F/ERO Repository is available for use to validate federal PIV credentials during normal day-to-day access into facilities or emergency access into an incident scene. The F/ERO Repository shares or sends the alphanumeric identifier, the approval status, and the PIV holder's Emergency Support Function (ESF) attribute only once the F/ERO Repository receives the alphanumeric identifier and correct PIN associated with the PIV card scanned at the site of a disaster. The F/ERO Repository does not share any other information. FEMA shares the information for the sole purpose of PIV authentication and tracking.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes, the sharing of PII is compatible with the routine uses in the DHS/All--026 Personal Identity Verification Management System Systems of Records Notice. Title IV of P.L. 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007," directs the Administrator of FEMA to establish a national federal preparedness data broker system. FEMA uses the system for real-time accountability and awareness of F/ERO information. FEMA shares information with other federal agencies for the purpose of "real-time accountability and awareness." The F/ERO Repository does not collect, maintain, or transmit PII.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Data in the F/ERO Repository is synchronized with management stations providing the capability and authorization to receive the F/ERO Repository transmissions. This allows a relying party to authenticate those required to respond to an incident scene. Transactional data taken by relying parties is electronically validated.

Transaction data collected at the incident scene is defined as the electronic challenge/response of a FIPS-201 compliant or interoperable credential via a handheld reader. Transaction data is collected by

individual handhelds and is aggregated and digitally signed in the onsite management station by those assigned access rights at the scene and only using a FIPS-201 compliant or interoperable credential for authentication. The transaction data forms an electronic manifest which is digitally signed. Transmission by HTTPS and authentication that meets E-Authentication level 4 criteria is required as the basis for access authorization.

Outside entities must submit a written request for the information and must fit a routine use under as documented in the DHS/All-026 Personal Identity Verification Management System of Records Notice.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: The risk associated with external sharing of information maintained is that individuals without a need to know would seek to access an individual's credential information by accessing an unsecure website or transmission.

Mitigation: Access to information within the F/ERO Repository is via a secure web transmission. Individuals that are found abusing their rights will have their rights removed and will not be allowed to access the system. Individuals found trying or gaining access using to the system by "hacking" will be prosecuted to the fullest extent of the law.

Privacy Risk: An individual without need to know could use the certificates to gain unauthorized access to other need to know information.

Mitigation: Access to the F/ERO Repository information is based on user roles and responsibilities and requires a PIN and credential holder's unique identifier in order to access the information. Thus, any sharing via routine uses does not include the PIV number, PIN, and unique identifier. Only names, work locations, and work phone numbers will be included.

Privacy Risk: Unauthorized parties may seek to access data contained in the PIV Authentication certificate.

Mitigation: The F/ERO Repository contains the PIV Authentication certificate (a PKI certificate in accordance with federal PKI and common policy) which is provided to all PIV bearers at issuance. It also contains the attribute bound to that individual only, which designates the F/ERO responsibility represented in object identifier format for each individual designated by their agency Attribute Administrators who are likely to respond to a disaster scenario. Section 9.4.3 of the *X.509 Certificate Policy for the US Federal PKI Common Policy Framework* states, "information included in PKI certificates is not deemed private."

Certificates that contain the Federal Agency Smart Credential Number, or FASC-N, in the subject alternative name extension, such as PIV Authentication certificates shall not be distributed via public repositories (e.g. via LDAP or HTTP). The F/ERO Repository is not a publicly accessible repository. Authorization to review the data in the F/ERO Repository is assigned to Attribute Administrators of that data for that agency only, and only after authentication is satisfied using a PIV credential, which provides

a very high level of identity assurance, as defined by E-Authentication standards. Risk is mitigated in this means using secure trusted identity credentials.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes, this PIA and the DHS/All-026 Personal Identity Verification Management System of Records Notice provide notice of this collection for the purpose of identity verification and tracking.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

For PIV issuance, this requirement is satisfied by each federal agency's PIA. Additionally, the credential holder has the right to refuse to enter his/her PIN which prevents the identity data and attributes assigned from electronic validation at the incident scene. The process provides for individual right of refusal to decline to provide information. However, such a denial may affect the ability of the individual to become a F/ERO.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The F/ERO Repository only accepts data transmitted by the issuing infrastructure and has no means to analyze the data separately. If the employee/contractor chooses not to consent to the use of this information, he/she may "opt out" by following a different career path or by electing not to become a F/ERO.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: The privacy risks identified with notice are that the individual or employer is not aware of how their information is going to be collected, shared, and maintained.

Mitigation: Each agency's HSPD-12 Program Management Office (PMO) is responsible for providing notice to its employees and contractors regarding the collection of identity information. Agency Attribute Administrators are responsible for providing notice of attribute information collected and the purpose for its collection. Notice is mitigated at the incident scene as PIV credential holders understand that no information can be validated with the PIV credential without the individual's approval by means of entering his/her PIN.

DHS also provided notice to the public via the aforementioned SORN listed in sections 1.6 and 5.2.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Employees/contractors do not have direct access to information provided to the F/ERO Repository. Information is provided by the designated agency Attribute Administrator. If an employee/contractor has a question about the information in the F/ERO Repository, he/she can contact the agency Attribute Administrator.

Additionally, as documented in the DHS/ALL – 026 Personal Identity Verification Management System of Records Notice, when seeking records the requestor must submit in writing full name; current address; date and place of birth; sign the request, and he request should either be notarized or submitted under 28 U.S.C. §1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. In addition the requestor should provide an explanation for requesting the information and when it is believed the records would have been created. Without this bulleted information the component(s) will not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations. All requests should be submitted to: Federal Emergency Management Agency, Attention FOIA Officer, 500 C Street, S.W., Room 840 Washington, D.C. 20472.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Agency Attribute Administrators are responsible for correcting inaccurate information. Individuals do not have direct access to information in the F/ERO Repository. The designated agency Attribute Administrator provides this information. If an individual has a question about the information in the F/ERO Repository, he/she is directed to contact their agency Attribute Administrator. The F/ERO Repository, Management Stations and Validation Devices receive corrections made at the agency level within 18 hours or less. Individuals may first gain access to their records through the process described in 7.1 above.

7.3 How are individuals notified of the procedures for correcting their information?

Designated agency Attribute Administrators are responsible for notifying personnel of procedures for correcting personnel information at the time it is provided to the agency Attribute Administrator. Additionally, individuals are notified by this PIA and the DHS/ALL – 026 Personal Identity Verification Management System of Records Notice.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Each agency's human capital policies and procedures provide formal redress. Additionally, an individual can submit a request for information via the FEMA FOIA process described above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: Erroneous information such as address could allow an individual's records to be redirected to a person without a need to know and result in identity theft.

Mitigation: Formal redress is provided to allow individuals to view and correct erroneous information the agency has on file.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Control of the view, query and run reports relative to F/ERO data for an individual agency is determined by that agency. One agency cannot view another agency's F/ERO data. The F/ERO Repository is viewed or retrieved only by an agency-authorized Attribute Administrator or Attribute Registrar using a FIPS-201 compliant credential for authentication and with the approval of the F/ERO Repository Administrator.

E-Authentication criteria published in OMB M04-04 and NIST SP 800-63 for systems requiring a very high level of assurance of an asserted identity documents the use of the aforementioned authentication criteria as the basis for granting authorization for access.

8.2 Will Department contractors have access to the system?

Granting department contractors access to each agency's system will be determined by each agency and only with the use of a PIV credential.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

FEMA requires safeguarding PII training for all employees and contractors.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The F/ERO Repository received ATO in August 2010. The ATO is valid for one year.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system is established in accordance with and compliant with the requirements of FIPS-201. Mitigation of risk is provided by the establishment of the specific roles that determine who receives access to the system, the authentication method required to attain access, and the specific scope of that access. The system will be able to track the transactions made within the system. Users found abusing his or her rights within the system will have their access revoked.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: Unauthorized access to information and inappropriate uses of the information.

Mitigation: Agencies utilize or recommend the following security controls: credential data is encrypted and stored on the credential; credential is sheathed in electromagnetically opaque sleeve to protect against unauthorized contact-less access to stored information; employees and contractors are alerted to importance of protecting the credential; certificate expiration/renewal within 3 years from issuance; electronic validation of the credential prior to being used as the basis to grant an access authorization; return of credentials to agency when no longer needed (or upon employee contractor separation from the agency); and deactivation of credential in F/ERO within a minimum of 18 hours of employee/contractor separation, loss or expiration of credential.

Privacy Risk: Data collected in the F/ERO Repository will not be secure.

Mitigation: In addition, each federal agency has previously issued a PIA related to the PKI certificates and other privacy information[6] related to all PIV credentials issued because of HSPD-12. The actions of the F/ERO Repository do not adversely affect PIAs issued previously or provide any additional adverse consequence. Given that the F/ERO Repository does not maintain PII, there is a minimal risk that the data in the F/ERO Repository if lost, compromised, or disclosed without authorization, will result in inconvenience or unfairness to the individual. To mitigate these risks, FEMA is required to follow specific guidelines relative to data integrity regarding the issuance of HSPD-12/FIPS-201 credentials. Additionally, FEMA has sought to collect no more information than is necessary to verify employees and/or contractors and services provided during a disaster.

[6] For additional information, please reference the DHS/All – 026 Personal Identity Verification Management System SORN (74 FR 30301, June 25, 2009) www.dhs.gov/privacy.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

This project is an information technology project designed to serve all federal executive agencies and leverage the capabilities implemented as a requirement imposed by HSPD-12, FIPS-201, and P.L. 110-53. The system provides for a uniform process and technology to validate electronically those required to respond to disaster scenarios using a FIPS-201 compliant or FIPS-201 interoperable credential. NIST governs and invokes the technology by cryptology testing conducted by NIST-approved labs and testing done to vendor components by GSA approved labs. Mitigation of risk is provided by the establishment of the specific roles that determine who receives access to the system, the authentication method required to attain access, and the specific scope of that access.

9.2 What stage of development is the system in and what project development lifecycle was used?

The F/ERO Repository is in place and has the ability to be populated with 100K F/ERO designations at the present time. It is hosted in a secure facility in which a Department of Defense (DOD) F/ERO Repository is located that serves 90K DOD F/ERO designations located in the National Capital Region (NCR). The facility hosts more than one HSPD-12 issuing infrastructure used by several federal agencies to issue FIPS-201 compliant credentials. To that end, C&As conducted by several agencies have been satisfactorily conducted at this hosting facility. The hosting facility also administers PKI credentials issued throughout the federal government and is approved as a shared service provider under FPKI common policy approved by the FBCA Policy Authority.

More than 15 exercises and demonstrations across multi-jurisdictions coordinated by FEMA NCR over the past 3 years, confirms the concept of validating FIPS-201 credentials as the basis to grant authorization at an incident response scene. After Action Reports are available for all of the exercises and demonstrations and the results have are publicly endorsed by the administration for DHS/FEMA and DHS/Screening Coordination Office. The NIMS credentialing standard defines the validation of FIPS-201 credentials for access to an incident scene and is part of the testimony provided to Congress as to the status of responding to Title IV of P.L. 110-53 by FEMA Policy in Nov 2007.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

This system does not employ technology that may raise privacy concerns.

Responsible Officials

Kenneth Wall
National Capital Region Coordination
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A: ESF and NIPP Tables

ESF 1	Transportation
ESF 2	Communications
ESF 3	Public Works and Engineering
ESF 4	Firefighting
ESF 5	Emergency Management
ESF 6	Mass Care, Emergency Assistance, Housing and Human Services
ESF 7	Logistics Management and Resource Support
ESF 8	Public Health and Medical Services
ESF 9	Search and Rescue
ESF 10	Oil and Hazardous Materials Response
ESF 11	Agriculture and Natural Resources
ESF 12	Energy
ESF 13	Public Safety and Security
ESF 14	Long-Term Community Recovery
ESF 15	External Affairs

Sector 1	Agriculture and Food
Sector 2	Banking and Finance
Sector 3	Chemical
Sector 4	Commercial Facilities
Sector 5	Dams
Sector 6	Defense Industrial Base
Sector 7	Emergency Services
Sector 8	Energy
Sector 9	Government Facilities
Sector 10	Information Technology
Sector 11	National Monuments and Icons
Sector 12	Nuclear Reactors, Materials and Waste
Sector 13	Postal and Shipping
Sector 14	Public Health and Healthcare
Sector 15	Communications
Sector 16	Transportation Systems
Sector 17	Water
Sector 18	Critical Manufacturing

Appendix B – Agencies providing information to the F/ERO Repository

- General Services Administration
- Social Security Administration
- Small Business Administration
- Department of Homeland Security
- Department of Labor
- Department of Education
- Executive Office of the President
- Environmental Protection Agency
- National Credit Union Administration
- Veterans Affairs
- National Aeronautics and Space Administration
- Department of Defense
- Federal Aviation & Administration
- Federal Housing Financial Board
- Federal Trade Commission
- Health and Human Services
- Housing and Urban Development
- International Broadcasting Bureau
- Department of State
- Nuclear Regulatory Commission
- National Science Foundation