Privacy Impact Assessment
for the

Electronic Fingerprint System (EFS)

DHS/FEMA/PIA-034(a)

January 8, 2015

Contact Point
J'son Tyson
Section Chief
Identity, Credential, and Access Management
Office of the Chief Security Officer
Federal Emergency Management Agency
(202) 646-1898

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

Abstract

The Federal Emergency Management Agency (FEMA) Office of the Chief Security Officer (OSCO) is updating and replacing the DHS/FEMA/PIA-034 Electronic Fingerprint System (EFS) Privacy Impact Assessment (PIA), dated September 24, 2013. FEMA OCSO uses the EFS as part of the security suitability, clearance, and badging process for FEMA employees, contractors, and affiliates. FEMA is conducting a PIA because EFS collects personally identifiable information (PII) and now uses National Protection and Programs Directorate (NPPD), Office of Biometric Identity Management's (OBIM) Automated Biometric Identification System (IDENT) to store fingerprints as a part of background investigations.

Overview

As required by law, FEMA conducts background investigations of employees, contractors, and affiliates to ensure that these individuals meet established suitability and security standards. This includes conducting the suitability, clearance, and badging process for FEMA Permanent Fulltime (PFT) Employees, Temporary Fulltime (TFT) Employees, Cadres of On-Call Response Employees (CORE), Reserve Employees, contractors, individuals from volunteer organizations, and federal, state, local, and tribal partners working in furtherance of FEMA's mission. As part of this process, a fingerprint-based criminal history records check is required. To execute this check, FEMA obtains electronic fingerprints and other PII as required by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division (CJIS) to complete the investigation through its Integrated Automated Fingerprint Identification System (IAFIS).

FEMA OCSO uses the EFS to accomplish this process in a more efficient manner by automating the previous manual, paper, process by leveraging FEMA OCIO infrastructure to send and receive biometric data. FEMA has worked exclusively with FBI CJIS to use IAFIS and the Office of Personnel Management (OPM) for credentialing services. FEMA automates, streamlines, and reduces the time required to conduct background investigations to support staffing decisions by leveraging the IDENT system by using EFS. When using EFS, applicant records are no longer uploaded manually for investigation review; they are submitted electronically over DHS's *OneNet* network. This reduces process time from days to hours. In addition, there is no longer a need for manual entry of investigation result data; all result data is automated. This reduces the risk of human error and greatly improves process time.

In general, the background check process conducted by FEMA OCSO mirrors the process conducted by DHS OCSO as a whole, as described in DHS/ALL/PIA-014.[1] This includes the suitability, clearance, and badging process for all FEMA categories of individuals

[1] For more information please see the DHS/ALL/PIA-014 Personal Identity Verification, *available at*, http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_dhs_piv_august2012.pdf.

mentioned above, including individuals from state, local, and tribal entities, as well as volunteer organizations that go through the security process for issuance of a Personal Identity Verification (PIV) card. Some individuals from volunteer organizations may require access to FEMA IT systems for the purposes of coordinating resources in a disaster scenario. These specific volunteers would be issued PIV cards and are considered contractors to FEMA. For general information on the security suitability, clearance, and badging process at DHS, please refer to DHS/ALL/Personal Identity Verification (PIV)/PIA-014(b), August 23, 2012. Specifically, this PIA covers FEMA's use of EFS and its interactions with the IDENT system, which is different from DHS OCSO's current biometric vetting program.

This PIA documents the transition from FEMA OSCO's use of FBI CJIS's IAFIS to FEMA OCSO's use of IDENT through the IDENT/IAFIS Interoperability.[2] The IDENT/IAFIS Interoperability enables the two systems to seamlessly connect, communicate, and exchange information. As part of the new security suitability, clearance, and badging process, information that FEMA OSCO transmits to IDENT is also enrolled into the database. However, access to this information is restricted to only FEMA users.[3]

FEMA performed this transition in compliance with the DHS Memorandum signed by the Chief Information Officer (CIO) and the Screening Coordination Office (SCO), which stated, "all DHS programs requiring the collection and use of fingerprints to vet individuals shall use the target biometric service as defined by the Homeland Security (HS) Enterprise Architecture." FEMA is now going to be a user of the identity services provided by IDENT. FEMA underwent this transition to streamline biometric, and associated biographic, background checks from both IDENT and IAFIS for the purposes of credentialing all FEMA applicants.

EFS Process

FEMA OCSO uses the EFS as part of the security suitability, clearance, and badging process for all applicants and potential hires including: PFTs; TFTs; COREs; Reserve Employees; contractors; volunteer organizations; and federal, state, local, and tribal partners working in furtherance of FEMA's mission.

In the initial phases of the applicant suitability process, an applicant first provides proper identification as outlined on the I-9 Form, "List of Acceptable Documents."[4] Once the applicant's identity is verified, his or her PII and ten-fingerprint biometrics are collected by the

[2] More information about Biometric Interoperability between the U.S. Department of Homeland Security and the U.S. Department of Justice is found in the DHS/NPPD/PIA-007(b) Biometric Interoperability between DHS and DOJ, *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_visit_update-b.pdf.
[3] For more information on the IDENT system and enrollment, please refer to DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System (IDENT), *available at*, http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013.pdf.
[4] I-9 Form, "List of Acceptable Documents." An entire list of acceptable documents can be found on page 9 of the following document, *available at*, http://www.uscis.gov/files/form/i-9.pdf.

secure Universal Registration Client (URC) station to initiate the personnel security and suitability processes.[5] This station is connected to the secure DHS *OneNet* Network and requires proper security credentials for access. Access to the URC is only granted to FEMA's trained security officials. Once applicant data is collected and identity verified the security official capturing the information submits the encrypted data to the FEMA Fingerprint Store and Forward (FPSF) server.

The FPSF server then transmits the data in a secure IDENT Exchange Message (IXM) format over DHS *OneNet* to the IDENT database. IDENT enrolls the FEMA biometric data as a new record if there is not an existing record. If there is an existing record, the FEMA record will be added as an encounter. IDENT vets the data against its existing OBIM Watchlist and internal DHS law enforcement information, and also forwards the FEMA data to the FBI's IAFIS to search for matches with national criminal records and rap sheet data. FEMA uses this information to perform periodic re-investigations (every 5 to 10 years depending on clearance requirements) and continuous vetting.[6]

CJIS sends the results back to OBIM, and OBIM consolidates the results from the FBI and IDENT's own checks. OBIM then returns the consolidated vetting report back to FEMA for processing. Results are returned to FEMA within 24 hours. Personnel security specialists review the results in DHS's Integrated Security Management System (ISMS) and determine whether the applicant meets suitability requirements after the IDENT/IAFIS result message is returned to FEMA from OBIM. The FPSF server decodes the encrypted return message and FEMA personnel security representatives review the full criminal history results via a web interface to ISMS, as the results are automatically generated into this system from the FPSF server. ISMS is a web-based case management tool designed to support the lifecycle of the DHS personnel security process.[7]

Once FEMA OSCO obtains the criminal history and background check results from IDENT and IAFIS, FEMA also coordinates with OPM to conduct credit checks to supplement

---

[5] FEMA collects biometric and PII from prospective employees, contractors, and other affiliates from fixed locations as well as field locations. FEMA deploys fingerprinting units to various field locations in order to screen these individuals, including joint field offices or other designated locations set up during a disaster. All fingerprinting units connect with the centralized FPSF server. Applicant data is captured on the fingerprinting unit and transmitted and saved to the FPSF server and is automatically deleted from the fingerprinting unit.

[6] Continuous vetting, also known as "Continuous Evaluation" is a new requirement to increase the frequency of suitability investigations described in the SUITABILITY AND SECURITY PROCESSES REVIEW: *REPORT TO THE PRESIDENT* (February 2014), *available at*, http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf. "This Review found that the current reinvestigation practices do not adequately reevaluate or appropriately mitigate risk within the security and suitability population. Lengthy periods between reinvestigations do not provide sufficient means to discover derogatory information that develops following the initial adjudication. Furthermore, resource constraints lead agencies to conduct fewer than the required number of reinvestigations."

[7] For more information on ISMS, please see DHS/ALL/PIA-038 Integrated Security Management System, *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_isms.pdf.

the background check information for consideration during the suitability process. FEMA sends the criminal history results to OPM's investigative server via EFS, which alerts OPM to conduct a credit check on the individual. OPM then sends credit check results back to FEMA via EFS. Previously, this was a manual process and OPM and FEMA sent the information through the mail. The credit check process is an entirely separate EFS transaction from the IDENT/IAFIS transaction. The OPM credit check is consistent with current security procedures and standards and is covered by the DHS/ALL/PIA-014 and the System of Records Notices (SORN) listed below in Section 1.2.

Evaluating and Mitigating PII Risks and Vulnerabilities

FEMA has resolved known vulnerabilities by automating previously manual processes. For example, FEMA's previous fingerprint capture process required FEMA security managers to export applicant data to compact discs (CD). FEMA has eliminated this PII vulnerability with the new EFS. In addition, FEMA previously stored PII on the URC, which was then manually deleted by the security manager. With the new EFS, PII is not stored on the capture station, therefore further protecting PII.

Existing EFS automation has also been enhanced. The URC now uses a card reader to capture applicant data automatically from a driver's license, rather than manually entering the license information into the system. This improves process time and decreases manual entry. The new EFS also automatically sends results to ISMS instead of the previous manual data entry process.

All FEMA background check biometrics are enrolled in IDENT. FEMA completed the Data Business Filtering Form required of all IDENT users that establishes access restrictions and filtering rules within IDENT for each user. FEMA restricts access to data within IDENT to only FEMA users. This is also memorialized in the Information Sharing Agreement (ISA), in the Data Access Request Analysis (DARA), and in the Data Business Filtering Rules. FEMA manages and provides IDENT with a list of FEMA personnel that are authorized to access FEMA data within IDENT. FEMA is a member of the IDENT Capability Working Group which meets monthly to discuss the Department's use of IDENT and any related issues. Only FEMA users can access the information provided by FEMA in IDENT; no other IDENT users can access or search this information.

OBIM restricts the sharing of IDENT data with users through the Data Access Security Controls. These controls allow data owner organizations to control what data is shared and who is granted access to the data. For more information on IDENT, please refer to the DHS/NPPD/USVISIT-002 PIA.[8]

[8] DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System (IDENT), *available at,* http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013.pdf.

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?

- 44 U.S.C. § 3544, "Federal Agency Responsibilities;"[9]
- 5 C.F.R. Part 731, "Suitability;"[10]
- 5 C.F.R. Part 732, "National Security Positions;"[11]
- 32 C.F.R. Part 147.24, "The National Agency Check;"[12]
- Executive Order 10450, "Security Requirements for Government Employment;"[13]
- Executive Order 12968, "Access to Classified Information;"[14]
- Homeland Security Presidential Directive-12 (HSPD-12);[15]
- DHS Delegation 12000, "Delegation for Security Operations Within the Department of Homeland Security;"[16]
- DHS Directive 121-01, "Chief Security Officer;"[17] and
- DHS Instruction 121-01-007, "The Department of Homeland Security Personnel Security and Suitability Program."[18]

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

---

[9] 44 U.S.C. § 3544, *available at*, http://www.gpo.gov/fdsys/pkg/USCODE-2008-title44/pdf/USCODE-2008-title44-chap35-subchapIII-sec3544.pdf.
[10] 5 C.F.R. Part 731, *available at*, http://www.gpo.gov/fdsys/pkg/CFR-2012-title5-vol2/pdf/CFR-2012-title5-vol2-part731.pdf.
[11] 5 C.F.R. Part 732, *available at*, http://www.gpo.gov/fdsys/pkg/CFR-2012-title5-vol2/pdf/CFR-2012-title5-vol2-part732.pdf.
[12] 32 C.F.R. § 147.24, *available at*, http://www.gpo.gov/fdsys/pkg/CFR-1999-title32-vol1/pdf/CFR-1999-title32-vol1-sec147-24.pdf.
[13] Executive Order 10450, *available at*, http://www.archives.gov/federal-register/codification/executive-order/10450.html.
[14] Executive Order 12968, *available at*, http://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf.
[15] Homeland Security Presidential Directive 12 (HSPD-12), *available at*, http://www.dhs.gov/homeland-security-presidential-directive-12#1.
[16] DHS Delegation 12000, *available at*, http://www.dhs.gov/xlibrary/assets/foia/mgmt_instruction_112_03_001_issuing_delegations_of_authority.pdf
[17] DHS Directive 121-01, *available at*, https://www.dhs.gov/xlibrary/assets/foia/mgmt_dir_121_01_office_of_the_chief_security_officer.6.30.08.pdf.
[18] DHS Instruction 121-01-007, *available at*, https://www.dhs.gov/xlibrary/assets/foia/instruction-121-01-007-personnel-suitability-and-security-program.pdf.

The following DHS-wide SORNs, under the authority of the DHS OCSO, cover the information collection associated with the security background checks:

- DHS/ALL-023 DHS Personnel Security Management SORN[19] and
- DHS/ALL-026 Personal Identity Verification Management System SORN.[20]

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

The EFS Security Plan (SP) was developed as part of the initial Certification and Accreditation (C&A) Package. The initial C&A effort was completed September 2013 and the Authority to Operate (ATO) was granted in the 4th Quarter of Fiscal Year 2013.

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

FEMA retains the personnel security clearance records in accordance with NARA General Records Schedule (GRS) 18, Security and Protective Services Records, items 20 through 25.

The IDENT database itself retains biometric and biographic data in accordance with Records Schedule Number DAA-0563-2013-001.

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 collection of information from federal employees and contractors does not fall under the purview of PRA. FEMA/OCSO is working with the PRA program management office to address PRA requirements related to the collection of information from members of the public.

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.

[19] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088, (February 23, 2010), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.
[20] DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301, (June 25, 2009), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2009-06-25/html/E9-14905.htm.

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

FEMA OSCO collects and enters the following information into EFS to initiate the background investigation process:

- Applicant Name (First, Middle Initial, Last, & Suffix);
- Applicant Fingerprints;
- Social Security number (SSN);
- Place of Birth;
- Date of Birth;
- Gender;
- Race;
- Height;
- Weight;
- Eye Color;
- Hair Color;
- Complete Residential Address (Street, City, State, Zip Code, and Country);
- Employing Government Agency, if any; and
- Address of Government Agency, if any.

Once the information is transmitted and searched against the IDENT database, IDENT enrolls the information into the system as a new entry.

The following datasets are searched in IDENT, via IAFIS. The match results are returned to FEMA:

- FBI-Known or Appropriately Suspected Terrorist;
- Wants/Warrants;
- FBI/Identification for Firearms Sales;
- FBI-Sex Offender Registry;
- Gang Member;
- Deported Felon;
- Department of Defense (DoD) Lookout;
- Wanted by Interpol;
- Smuggler/Removed Alien;
- Aliens;
- Drugs;
- Final Order (an order to an illegal alien to leave the country); and
- Pending Removal status (pending deportation).

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

There are three sources of information in EFS: the individual being screened, FBI's IAFIS system, and IDENT. FEMA OCSO collects information directly from a current or prospective federal hire, a federal employee, a contractor, or other affiliates, including state, tribal, and local partners, and individuals from volunteer organizations. FEMA collects the information via paper and electronic media. The applicant provides two forms of identification per the I-9 in order for FEMA to verify identity. All biometric data is captured directly from the individual at the capture station by an electronic fingerprint scanner. The applicant's information is then saved to the FPSF server and transmitted to and searched against, and then enrolled into the IDENT databases.

IAFIS data is maintained by the FBI. IAFIS is a national fingerprint and criminal history system that responds to requests 24 hours a day, 365 days a year to help local, state, and federal partners solve and prevent crime and catch criminals and terrorists. IAFIS provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses.

IDENT data comes from DHS, collected by, or in cooperation with DHS and its components and may contain information collected by other federal, state, local, tribal, foreign, and international agencies. IDENT is a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context.

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.

Applicants are given the opportunity to check their information for accuracy prior to submitting it to FEMA. The accuracy of applicant data is also visually checked against the identification documents provided by the applicant as the first step in the fingerprinting process. The applicant is also fingerprinted and the data he or she provides is confirmed through IAFIS and IDENT. FEMA security officials identify and address any discrepancies or inaccuracies in the original information provided from the applicant during the adjudication process. If the FEMA security officials identify inaccurate or inconsistent information, FEMA OSCO will contact IDENT via EFS within 72 business hours to update or correct the inaccurate FEMA information enrolled in IDENT.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that inaccurate information may have an adverse effect on the suitability status of an applicant.

Mitigation: This risk is mitigated by allowing applicants to review their applications prior to submission. Additionally, the FEMA OCSO Personnel Security Division (PSD) checks and cross references the information received from OPM and the FBI criminal history report to identify any discrepancies in the information. If during the review of this information, the PSD notices inaccurate information or discrepancies between the two sources, and requires further clarification, the PSD will notify the applicant and request supporting or clarifying documentation. For example, if the PSD identifies that the applicant has different SSNs and addresses listed on the credit history report and criminal history report for the same period of time, the PSD will contact the applicant for clarification. The applicant is then given the opportunity to provide supporting or clarifying documentation to explain the discrepancy (e.g., he or she was a victim of identity theft and has documentation to support this and explain the discrepancy). Furthermore, FEMA OSCO contacts the IDENT System Administrators to correct any inaccurate or incorrect information provided by FEMA in IDENT within 72 business hours from notification. More information about the process for correcting inaccurate or incorrect information can be found in the DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) PIA.[21]

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.

FEMA OCSO uses the biometric data and PII collected as part of the security suitability, clearance, and badging process. All data collected (including SSN), is required by IAFIS and OBIM to ensure proper identification and verification of each applicant. The biometric data and PII are entered into IDENT and IAFIS and searched against the databases for possible hits or matches. FEMA OCSO then uses the search results from IDENT and IAFIS to determine the individual's suitability.

IDENT enrolls the FEMA biometric data as a new record if there is not an existing record. If there is an existing record, the FEMA record will be added as an encounter. IDENT vets the data against its existing OBIM Watchlist and internal DHS law enforcement information, and also forwards the FEMA data to the FBI's IAFIS to search for matches with

[21] DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System (IDENT), *available at*, http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013.pdf.

national criminal records and rap sheet data. FEMA uses this information to perform periodic re-investigations (every 5 to 10 years depending on clearance requirements) and continuous vetting. Only FEMA users can access and search the FEMA data that is enrolled in IDENT; no other IDENT users can access or search this information.

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, FEMA does not use technology to search IDENT for patterns or general terms. Queries are specific to the applicant and only needed for the purpose of the individual's personal background investigation.

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

No. Although data is sent between DHS components (FEMA to NPPD/OBIM via DHS *OneNet*), all users of EFS are within FEMA. There are no other components with assigned roles or responsibilities within the system.

Only FEMA users of IDENT can access and search data provided by FEMA to IDENT. Other IDENT users cannot access or search that data. This information is memorialized in the ISA, in the DARA, and in the Data Business Filtering Rules.

FEMA may only share information with other DHS components that have an authorized need to know for the information. Any information sharing must be consistent with the original purpose of collection and the SORNs in 1.2.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that FEMA suitability information may be used within IDENT for unauthorized purposes, or for reasons that are inconsistent with the original purpose of collection.

Mitigation: IDENT and EFS personnel will regularly analyze their respective audit logs to detect and track unusual or suspicious activities across the connection that might indicate intrusions or internal misuse. FEMA completed the Data Business Filtering Form required of all IDENT users that establishes access restrictions and filtering rules within IDENT for each user. FEMA restricts access to data within IDENT to only FEMA users. This is also memorialized in the ISA, in the DARA, and in the Data Business Filtering Rules. FEMA manages and provides IDENT with a list of FEMA personnel that are authorized to access FEMA data within IDENT. FEMA is a member of the IDENT Capability Working Group that meets monthly to discuss the

Department's use of IDENT and any related issues. Only FEMA users can access the information provided by FEMA in IDENT; no other IDENT users can access or search this information.

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

Mitigation: IDENT and EFS users, including system administrators, are required to protect and use data in accordance with the policies, standards, and regulations specified for each system. All system users must read and sign their agency's "Rules of Behavior" statement and comply with DHS and U.S. Government security requirements.

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.

EFS provides FEMA applicants a notice required by the Privacy Act, 5 U.S.C. § 552a(e)(3), which can be found in Appendix A. All applicants must read and sign a separate Privacy Act notice form. This Privacy Act notice form is provided in both paper and electronic format. The notice states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used.

This PIA and the SORNs listed in 1.2 also serve as notice for information collection. Additionally, all FEMA badging offices display posters with Privacy Act notices to further notify applicants about the collection of information.

FEMA applicants, using an electronic signature process, confirm the presentation of and agree with the Privacy Act Statement, and voluntarily participate in the fingerprinting process and submit to a name-based background check appropriate to job requirements.

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

Individuals are notified of the uses of their information prior to collection. The individual gives consent to the uses of his or her information by confirming and agreeing with the Privacy Act Statement. All applicants must provide information in order to be considered for employment at FEMA. Provision of information is voluntary; however, if an individual declines to provide information, FEMA will not be able to conduct sufficient background check and the individual will not be considered for employment.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that FEMA employees will not be aware that their information and biometrics will be recurrently vetted as part of the new Continuous Evaluation process.

Mitigation: FEMA employees receive notice from FEMA, at the time of collection, of the uses of their information within IDENT. Additionally, temporary and/or non-FEMA employees also receive notice by way of this PIA.

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.

Records relating to applicants are retained and disposed of in accordance with General Records Schedule 18, item 20 through 25, approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable. This retention period is required for FEMA to conduct periodic re-investigations and perform continuous vetting to compare any findings to the original submission. OCSO removes any information pertaining to individuals not selected for employment from the EFS server on an annual basis. FEMA OSCO contacts IDENT System Administrators to delete the corresponding information from IDENT.

Investigative reports and related documents created or received by FEMA for use in making security/suitability determinations are placed in inactive files after notification of death, separation, or transfer of employee, or expiration of contract relationship. In accordance with NARA Authority N1-311-94-1, Item 1, inactive files are cut off semi-annually and transferred to Federal Record Centers (FRC), and destroyed 15 years after cutoff.

Investigative reports and related documents created or received by FEMA for use in making security/suitability determinations that result in substantially actionable issue(s), adverse adjudication, or debarment are placed in inactive files after notification of death, separation, or transfer of employee, or expiration of contract relationship. In accordance with NARA Authority N1-311-94-1, Item 2, inactive files are cut off semi-annually and transferred to FRC, and destroyed 25 years after cutoff.

Data is retained on the FPSF server for a minimum period of 3 years, not to exceed 7 years.

In accordance with NARA Authority DAA-0563-2013-0001, IDENT records are retained for persons encountered who are no match to the watch list for 1 year; persons whom are a near match but turn out to be cleared for 7 years; and persons who are direct matches to the watch list

are retained for 99 years or 7 years from date of death.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that applicant information is retained longer than required, which may increase the likelihood of an unauthorized disclosure of information.

Mitigation: This risk is mitigated by retaining the information in accordance with the approved NARA retention schedules and only for a period necessary for FEMA OCSO to conduct periodic re-investigations and perform continuous vetting to compare any findings to the original submission. A Designated System Administrator is responsible for deleting or archiving information in accordance with the retention schedules. The Designated System Administrator will review all data on an annual basis. Also, security controls are in place to ensure that information is protected during this time.

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.

EFS sends data to the FBI and OPM for the purpose of conducting suitability and security background investigations of applicants, employees, and contractors. This includes FEMA PFT Employees, TFT Employees, CORE, Reserve Employees, contractors, individuals from volunteer organizations, and federal, state, local, and tribal partners working in furtherance of FEMA's mission.

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

The purpose of DHS/ALL-023 DHS Personnel Security Management SORN and DHS/ALL-026 Personal Identity Verification Management System SORN is to collect and maintain biographic and fingerprint information of employees in order to determine suitability, and issue clearances and badging. Primary external sharing is with law enforcement-type entities via routine uses published in DHS/ALL-023 DHS Personnel Security Management SORN and DHS/ALL-026 Personal Identity Verification Management System SORN. These outside entities receive PII from FEMA and in turn provides any relevant data to assist FEMA in making a determination about an individual's suitability.

For example, FEMA shares names and fingerprint information of employees with the

FBI, which then provides FEMA with information as to whether the employees have committed any disqualifying crimes. The FBI is able to retrieve this data based on the information FEMA provides. Without first sharing with the FBI, FEMA would be unable to meet this requirement by law.

FEMA also shares data related to the fingerprints with other appropriate federal, state, local, tribal, foreign, or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual and to an individual's prospective or current employer to the extent necessary to determine employment eligibility.

Thus, the sharing is compatible with the purpose of collecting the fingerprint information.

6.3 Does the project place limitations on re-dissemination?

Yes, external agencies are strictly prohibited from sharing the information provided by EFS outside the descriptions in this PIA. Users understand and acknowledge these limitations when they sign the EFS Rules of Behavior.[22] The EFS System Owner receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the Rules of Behavior, before authorizing access to information and the information system.

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

As identified in the SORNs listed in 1.2, requests for records from FEMA/OCSO are made to the FEMA Disclosure Office, which maintains the accounting of what records were disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be disclosed or inappropriately shared with unauthorized entities.

Mitigation: This risk is mitigated by only disclosing information pursuant to the routine uses of the SORNs listed in 1.2. FEMA has a Memorandum of Understanding (MOU) in place with OPM to ensure that there are formal procedures in place to secure and protect FEMA employee and contractor data. OPM is required by the MOU with FEMA and also by government-wide security standards to ensure that any information it receives or transmits is transmitted to a party that has a need to know and that the receiving party has adequate security measures in place.

[22] EFS Rules of Behavior state that information from EFS, including biometrics, fingerprint results, audit logs, and paper reports are not to be used, copied, or disseminated outside of the requirements of this PIA and applicable SORNs.

Privacy Risk: There is a risk of unauthorized disclosure of information during electronic capture/transmission of fingerprints from EFS to OPM.

Mitigation: To mitigate the risk of unauthorized disclosure when transmitting data electronically, DHS and OPM have taken appropriate measures to ensure that unauthorized disclosure during transmission does not occur, such as trusted Virtual Protected Network (VPN) tunnels, data encryption, and additional security measures.

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?

Individuals may directly correct basic information such as address and phone number at any time after the clearance process is completed. Individuals can provide updated information to FEMA OSCO who will then make the appropriate changes. This is completed through the FHR Navigator with manager approval of each change. During the clearance process individuals may not alter their information. They may inform the FEMA OCSO of a change in their information, but cannot directly access it.

Individuals 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. When seeking records about yourself from this system of records your request must conform with the Privacy Act regulation set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746m, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the DHS Chief Privacy Officer and Chief Freedom of Information Act Officer, www.dhs.gov, or 1-866-431-0486.

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

Once the information provided by the applicant during the pre-enrollment and enrollment processes has been verified and authenticated, changes to the database would occur for a name change or for additional information provided through adjudication procedures. Individuals may directly correct basic information such as address and phone number at any time after the

clearance process is completed. FEMA OSCO deletes the information pertaining to nonselected individuals from the EFS server on an annual basis.

On an as-needed basis, but no less than monthly, FEMA OSCO will contact IDENT system administrators to correct inaccurate information provided by FEMA and to delete information of nonselected individuals from IDENT. For more information on how information is maintained in IDENT, please refer to the DHS/NPPD/USVISIT-002 PIA.

Furthermore, the SORNs listed in Section 1.2 and this PIA also provide notice on how individuals can access and correct their information.

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

Individuals are informed in writing and given an opportunity to explain, refute, or deny the information in their background check. If during this process, FEMA identifies any discrepancies in the information (e.g., inaccurate information, adverse information), FEMA contacts the individual and provides the individual an opportunity to provide mitigating or clarifying documentation. If the adverse information is appropriately mitigated, then he or she is approved in writing for suitability or security clearance in addition to being eligible for clearance. Additionally, during the enter-on-duty process and before receiving clearance, the form used for issuance of the actual card contains notice reminding the employee or contractor of the ability to access information as well as notice of the uses of the collection.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that inaccurate information may be used to make a determination on an individual's suitability.

Mitigation: To mitigate this risk, the individual is afforded his or her rights as outlined in the law and DHS policies prior to FEMA OCSO making a determination on an individual's suitability for employment or ineligibility for a clearance based on adverse information obtained in his or her background investigation (including criminal history and credit checks). For example, an individual is given the opportunity to clarify or provide supporting or mitigating documentation for any discrepancies found in the credit history report and criminal history reports.

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?

FEMA OCSO ensures access to employee information is both restricted and controlled. EFS uses a separation of access capabilities based on user roles and an internal audit process. FEMA OCSO established audit logs and regularly verifies them to minimize the possibility of a breach. FEMA OCSO also relies on automated tools to indicate when information may have been misused.

FEMA OCSO has a plan in place to immediately respond to a breach, should it occur. Self-audits, third-party audits, and reviews by the Office of Inspector General or Government Accountability Office can be performed as needed or as required by law. Attempts to access sensitive data are recorded for forensic purposes if an unauthorized individual attempts to access the information contained within the system.

FEMA restricts access to FEMA data within IDENT to only FEMA users. This is memorialized in the ISA, in the DARA, and in the Data Business Filtering Rules. FEMA provides IDENT with a list of FEMA personnel that are authorized to access FEMA data within IDENT. IDENT employs its own security measures based on these requirements. IDENT also provides audit trail capabilities in order to monitor, log, and analyze system transactions, as well as actions and system accesses of authorized IDENT users. FEMA is a member of the IDENT Capability Working Group that meets monthly to discuss the Department's use of IDENT and any related issues.

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

FEMA employees (including EFS users and administrators) and contractors are required to complete annual privacy and security training. If any FEMA employee fails to complete the required annual training, access to FEMA networks and facilities is denied until mandatory training requirements are fulfilled. FEMA OCSO implemented strict guidelines, and enforces adherence for its employees as it pertains to protecting personal and sensitive employee information.

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

Authorized FEMA OCSO personnel or contractors (pursuant to an appropriate routine use) who handle the operations and maintenance of the system will have position-specific access to the system to support the primary system function, as well as to troubleshoot technical system issues encountered on a day-to-day basis. All assigned FEMA employees and contractor staff receive appropriate privacy and security training and have any necessary background investigations and/or security clearances for access to sensitive, private, or classified information and secured facilities. FEMA ensures this through legal agreements with its contractors and

enforcement of internal procedures with all DHS entities involved in processing the background checks. Additionally, robust standard operation procedures and system user manuals describe user roles, responsibilities, and access privileges.

OBIM has documented standard operating procedures to determine which user may access the IDENT system. In particular, individuals with system access must hold a DHS security clearance, must have a need to know the information based on their job responsibilities, and must participate in security and privacy training. Also, access to specific data is predetermined; the data provider decides who may have access to the data it provides. In this case, FEMA only allows FEMA users to access FEMA data.

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?

FEMA's process for reviewing and approving MOUs and ISAs involve FEMA's IT Security Branch, FEMA Privacy Officer, and the Office of Chief Counsel, and appropriate authorities from the other agency/organization to the agreement. FEMA reviews these agreements on an annual basis and reviews appropriate security documents for any newly identified risks. FEMA mitigates any newly identified risks between the partnering agencies in accordance with applicable laws.

Responsible Officials

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

Approval Signature

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix A: Privacy Act Notice

PRIVACY ACT INFORMATION

Authority: Executive Order 9397, Executive Order 10450, section 2 and 3, Executive Order 12958, and Executive Order 12968, the Robert T. Stafford Relief and Emergency Assistance Act, P.L. 93-288, as amended (42 U.S.C. § 5149)(b) authorizes the collection of information including the Social Security Numbers (SSN).

Purpose: The information is required for the purpose of hiring and employment, including background checks. Such personally identifiable information (PII) is required before each individual can be hired and granted access to agency-controlled facilities, computers, databases, and other agency systems.

Disclosure: Furnishing this information, including SSN, is not mandatory; however, failure to do so may impede the processing of each individual's application for employment. In addition, failure to provide complete PII may impede the processing of each individual's application for employment.

Routine Uses: Any disclosure or sharing of information is done in accordance with the Routine Uses outlined in DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN.