Privacy Impact Assessment
for the

Authentication and Provisioning Services (APS)

DHS/FEMA/PIA-031

August 6, 2013

Contact Point
Tina Wallace-Fincher
Information Technology Security Branch
FEMA Information Technology
(202) 646-4605

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

Abstract

The Federal Emergency Management Agency (FEMA), Mission Support, Office of the Chief Information Officer (OCIO) manages and operates the Authentication and Provisioning Services (APS) system. APS is FEMA's enterprise platform system that provides identification, authentication, account management, and Active Directory account provisioning to internal and external users, through Microsoft Active Directory Servers. FEMA is conducting this PIA because APS collects, uses, maintains, and retrieves personally identifiable information (PII) about employees; contractors; members of the public; and federal, state, local, and tribal government officials.

Overview

The FEMA OCIO manages APS. APS is the standardized, configurable, and comprehensive security gateway and interface to FEMA applications and systems. APS provides authentication services for FEMA using Microsoft Active Directory Servers. APS provides a number of services for both internal and external users. Internal users are classified as FEMA employees and contractors. External users are members of the public who have registered with FEMA to request disaster assistance and federal, state, local, and tribal government officials assisting with disaster response efforts.

The Homeland Security Presidential Directive-8 (HSPD-8): National Preparedness (December 17, 2003) authorizes FEMA to establish policies that strengthen preparedness and prevent and respond to major disasters and other emergencies. This authority includes establishing mechanisms for improved delivery of federal preparedness assistance. APS collects and uses information on individuals in order to grant and control access to FEMA systems and applications. APS is comprised of three components: Active Directory, Network Access Control System (NACS), and FEMA Access Management System (FAMS), all of which provide services and capabilities to control access to FEMA's internal and external systems and applications, based on user role.

- APS Active Directory is the application used for internal user account creation, management, and Group Policy settings to allow FEMA employees and contractors (internal users) access to authorized FEMA resources and applications. It establishes username, password, and Group Policy settings for each user and allows access to FEMA resources (i.e., services, applications, and systems). FEMA must create users and add them to a Group in the APS Active Directory to grant any internal user access to FEMA resources. The Operations Group creates a user by extracting the user's information from the applicable subsystem, either NACS or the Automated Deployment Database (ADD). Once this process is complete, a user account and profile is established. Establishment of this account allows access to specific, authorized FEMA applications. APS Active Directory shares username, Group Policy information, and account status with APS NACS. All other data (the non-sensitive PII) is kept within the Active Directory logs for seven years.
- APS NACS provides authentication access for internal users (i.e., FEMA employees and contractors) through password expiration tracking and establishing minimum password requirements for the system. Password expiration tracking is derived from DHS Sensitive

Systems Policy (4300A), password management requirements. APS NACS keeps track of annual security training and informs internal users when annual security training is needed. APS NACS shares password expiration information with APS Active Directory in an effort to ensure compliance with annual training requirements and maintain control of access to FEMA resources.

- APS FAMS specifically grants external users (members of the public who have registered with FEMA to request disaster assistance and federal, state, local, and tribal government officials) access during a disaster or national emergency. It grants the individual a username and password within public-facing FEMA systems. It does not share account information with APS Active Directory or APS NACS, as these are strictly used for internal user purposes. FAMS is set up to only allow access within known and declared disaster areas. This means that disaster survivors submit their personal information to create an account. Based upon the address they enter, authorized local officials (federal, state, local, and tribal officials supporting disaster response efforts) review the submitted information to ensure access is necessary. The following applications and source systems use FAMS for authentication from members of the public:
    - Disaster Assistance Improvement Program (DAIP)[1];
    - National Shelter System (NSS);
    - Individual Assistance Program Support System (IAPSS)[2]; and
    - Direct Assistance Replacement Assistance Consideration (DARAC).

Sources of APS Data

APS provides authentication and role-based access to both internal and external users of FEMA's information technology systems. FEMA employee PII is collected from the Automated Deployment Database (ADD) system, a FEMA system that is external to the APS boundary. FEMA contractor PII is collected from the designated Contracting Officer's Representative (COR). External user PII (members of the public who registered for disaster assistance and federal, state, local, and tribal officials supporting the disaster response effort) is collected from public-facing FEMA source systems that are external to the APS boundary. Information maintained in APS is covered by the Department of Homeland Security/ALL-004 General Information Technology Access Account Records System of Records Notice (SORN)[3] and retained in accordance with the records retention schedule pursuant to NARA Authority N1-311-89-5, Item 1.

APS allows internal users to initiate, track, and expedite the process of providing aid to other federal agencies, state, local, and tribal governments in response to a pre-incident emergency declaration or post-disaster declaration under the Stafford Act. FEMA uses the information collected from external

[1] See, DHS/FEMA/PIA-012(a) - Disaster Assistance Improvement Plan (DAIP), available at http://www.dhs.gov/privacy-documents-fema.
[2] IAPSS is an upgrade to the National Emergency Management Information System – Individual Assistance (NEMIS-IA) Web-based and Client-based modules. For more information on NEMIS-IA, please see DHS/FEMA/PIA-027, June 29, 2012.
[3] See, DHS/ALL-004, 77 FR 70,792 (Nov. 27, 2012) http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

users to match and verify against presidentially declared disaster areas. Currently, there are approximately 19,702 internal users and 2.5 million external users. The number of internal users can grow substantially depending on the level of disaster assistance necessary (e.g., during Hurricane Katrina, internal users grew to be more than 50,000.) This number includes personnel, such as: FEMA Permanent Full Time Employees (PFT), Temporary Full Time Employees (TFT), FEMA Reservists, Cadre of On-call Response Employees (CORE), the FEMA Corps, and DHS Surge Capacity Force (SCF) programs.

Typical Transaction for APS Internal Users:

As part of the FEMA on-boarding process, OCIO APS administrators establish user profiles for new FEMA employees and contractors upon receipt of request from FEMA's Office of the Chief Component Human Capital Officer (OCCHCO), a designated supervisor, or COR. The APS administrator accesses ADD to verify FEMA employee information such as full name, social security number (SSN), and address. ADD is not part of APS; it is the designated system authorized to hold sensitive PII for FEMA employees. FEMA collects the information maintained in ADD during the hiring process. However, SSNs are not stored in APS. The designated COR provides FEMA contractor information (i.e., full name, address, FEMA office location, contractor company name) to the APS administrator, who then populates APS. FEMA uses a third-party identity proofing (IdP) service for identity verification of FEMA contractors. SSNs for contractors are not collected or stored within APS.

Through an automated process, APS extracts the FEMA employee's ID number, full name, and office location from ADD and places it in the APS staff table. The APS staff table is a temporary table that the APS administrators use to house the extracted PII from ADD. The staff table contains only PII that is necessary to create an account within APS. Once this information has been entered and approved, APS creates a system generated unique identifier known as a USER ID. The USER ID is the primary key that is recognized throughout the staff tables when trying to locate or reference an individual. The user's full name is used for display purposes when queries are run on staff tables to ensure accuracy. As previously mentioned, the APS system does not collect or store SSNs for FEMA internal users. However, SSNs of FEMA employees are verified via ADD as added security for the authentication process. This is done through a secure SSL encrypted connection to ADD. The information is discarded after use and is not stored within the APS boundary. The information that is stored within APS for internal users includes: full name, user name, office location, work location, office and cell phone numbers, company, job title, and FEMA email address.

Once APS assigns the USER ID and a temporary password, the user may access the FEMA network, and ultimately FEMA's resources, services, and systems, as appropriate. The user's data access is controlled through an Oracle database and application security mechanisms[4].

[4] Oracle grants access to data based upon a person's designated role. These roles are assigned specific "rights" (e.g., read-only, modify, delete). The access rights granted are based upon the internal user's position, role, and job responsibilities. A FEMA official, usually the user's supervisor or the COR grants user roles. When the user first logs in, he or she must complete the annual security training and change the temporary password to meet FEMA requirements.

Typical Transaction for External APS Users:

FEMA collects external user information for APS through the FEMA internet interface (FAMS) via https://portal.fema.gov/famsVuWeb/home. FAMS is setup to allow access only within known/declared disaster areas. Through this process, FEMA collects the following PII data: first and last name, home address, email address phone number, SSN, and mother's maiden name. Though SSNs are collected at the source system level, SSNs are not transferred into APS. With web-based applications, FEMA uses web-based interface integration with the IdP, which facilitates identity proofing by asking questions that only the specific registrant/user would know. It uses a four question quiz and publicly-available information about the user from the past 10 years. Access is not provided if the questions are not answered correctly. Once the applicant/user completes the registration process, the application is reviewed by a FEMA "Gatekeeper" or approver (federal, state, local, and/or tribal officials under FEMA oversight), who is assigned during disasters. The "Gatekeepers" have the capability to assign, approve, and remove access rights to users. For a more detailed description of DAIP and the identity verification process, please see DHS/FEMA/PIA-012(a) - Disaster Assistance Improvement Plan (DAIP) at www.dhs.gov/privacy.

Federal, state, local, and tribal government officials assigned to support disaster efforts log into disasterassistance.gov to establish a FEMA user account. Through this process, FEMA collects the following PII data elements: first and last name, home address, phone number, office address, position title, organization, and email address. FEMA's web-based interface integration with the IdP as described above, occurs. Once the user completes the application process, his or her application is reviewed by a FEMA APS Administrator, who will assign user rights based on the individual user's roles in disaster response efforts.

Upon approval, the external user/disaster applicant receives a notifying email, which directs him or her to a web URL to create a user name and password for login to the appropriate application. Once a user logs in, icons will appear so that the user can choose the application he or she needs to access, based on the user roles assigned. The user does not receive any other access to internal information other than what is provided by the web-based interface and the specific permissions granted to him or her. The identity proofing process mitigates the risk of an unauthorized person gaining access. Authentication results are monitored by the FEMA Security Operations Center (SOC).

One of the major privacy risks associated with APS is that it relies on underlying source FEMA systems for data and may use inaccurate data. Since information is not collected directly from the internal user, he or she may be unaware of the proper procedure for seeking redress to correct, access, or amend his or her records within APS. This risk is mitigated as internal users can contact the FEMA Help Desk to request information be corrected or updated. External users can access and correct their personal information online via https://portal.fema.gov/famsVuWeb/home using the applicant's USER ID, password, system generated PIN, and authentication that was established during the application process. Also, both internal and external users can file a Privacy Act Record Amendment Request with FEMA to correct any personal information that they cannot correct at the source system level. Additional redress procedures can be found DHS/ALL-004 General Information Technology Access Account Records, 77 FR 70,792 (Nov. 27, 2012) and the various source system PIAs.

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?

APS was established to support the FEMA disaster management activities in accordance with Homeland Security Presidential Directive-8 (HSPD-8): National Preparedness; the National Preparedness Guidelines (Guidelines September 2007); and the Robert T. Stafford Disaster Relief and Emergency Assistance Act.

- *Homeland Security Presidential Directive-8: National Preparedness (HSPD-8)* delegates agencies to establish policies to strengthen the preparedness of the United States to prevent and respond to major disasters and other emergencies. This includes establishing mechanisms for improved delivery of federal preparedness assistance.

- *Presidential Policy Directive-8 (PPD-8): National Preparedness (PPD-8)* continues the aims of HSPD-8. It requires the involvement of everyone, not just the government, in a systematic effort to keep the nation safe from harm and resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics. This policy directive calls on federal departments and agencies to work with the whole community to develop a national preparedness goal and a series of frameworks and plans related to reaching the goal.

- *National Preparedness Guidelines* directs the Secretary of Homeland Security to develop a national domestic all-hazards preparedness goal and related preparedness tools.

- *Robert T. Stafford Disaster Relief and Emergency Assistance Act as amended,* 42 U.S.C. § 5121, Title II – Disaster Preparedness and Mitigation Assistance constitutes the statutory authority for most federal disaster response activities especially as they pertain to the FEMA assistance programs.

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

Information maintained in APS is covered by the DHS/ALL-004, General Information Technology Access Account Records, 77 FR 70,792 (Nov. 27, 2012).

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

APS had an active Authority to Operate (ATO) until July 15, 2013. A new package has been submitted and a renewal is expected.

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

FEMA retains the information in APS pursuant to NARA Authority N1-311-89-5, Item 1. These records are related to all users of APS. Specific data regarding the records are outlined in Section 2.1 below. The records are accessible on FEMA's server for 30 days, then recorded on backup tape and retained in a secure location for seven years. Additionally, audit logs are included within the records retention schedule. Audit logs capture a login record of when the user logs in and accesses resources, which include login time, USERID, and resources accessed through APS.

In accordance to FEMA's contract with the IdP, once it fulfills the purpose to provide identity proofing and authentication, the IdP may not use an individual/user's information for any other purpose nor may it retain user information.

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 PRA does not apply to APS because no information is collected directly from the public. APS receives information from source systems. Each source system is responsible for compliance with the PRA. Federal employee information within APS is not covered by the PRA, as it does not apply to federal employees.

Section 2.0 Characterization of the Information

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

The following information is collected and used for internal users (FEMA employees and contractors):

- Full Name;
- Home Address;
- Username;
- Work Phone Number;
- Work Cell Number;
- Office Location;
- Organization or Company Name; and

- FEMA Email address.

The following information is collected and used for external users (members of the public who have registered with FEMA to request disaster assistance; and federal, state, local, and tribal government officials):

- Full Name;
- Home Address;
- Username;
- Home Phone Number;
- Email address;
- Government Agency or Company Name (if applicable) and Address; and
- Position Title.

Note:

- The SSN is verified against existing information contained within ADD for the purpose of initial account creation only for FEMA employees. SSN is not stored within APS and is not used for non-FEMA internal users or external users.
- External user PII is not shared with any external organizations except the IdP for identity verification. The external user data is transmitted via 256 bit Secure Socket Layer (SSL) connection. The IdP system asks the user certain questions to verify identity such as old addresses or work addresses that only the person would know. The data used by the IdP is not stored within APS and neither is the data retained in any of the IdP systems.

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

Information is collected in APS via external and internal FEMA source systems. The primary external source systems are disasterassistance.gov, NSS, and DAIP; and the primary internal source system is ADD. As noted in Section 2.1, SSNs are verified against existing information contained (for FEMA employees only) within ADD, but are not stored within APS. Personal information is submitted through the IdP (for external users and FEMA contractors) for identification verification, but the IdP does not retain the information.

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

FEMA collects full name, address, telephone number, and/or government agency/company information (as appropriate) from disaster registrants, federal, state, local, and tribal officials, as well as

internal FEMA contractors. The information is sent for identity verification via a secure web service to the IdP, which then performs a query of its database of public records to determine if a person with these characteristics exists and returns a yes/no status. The IdP performs authentication by sending a four question quiz to the user to answer. The quiz and answers are then used to authenticate users. The IdP does not share the specific data it uses for authentication with FEMA nor does it store user information within its system or use the data for any other purpose.

2.4 Discuss how accuracy of the data is ensured.

FEMA ensures accuracy of data within APS in four primary ways: source systems, The IdP, and designated FEMA officials:

1) APS derives user information from FEMA source systems (i.e., ADD, disasterassistance.gov, DAIP, and NSS), which are outside of APS. Ensuring data accuracy of information obtained from source systems is primarily accomplished at the specific source system level. When user information is corrected within a source system, APS is automatically updated.

2) FEMA employee data (internal user's information) is verified against existing information contained within ADD. The employee provides this information directly during his or her hiring/on-boarding process.

3) FEMA uses the IdP for identification verification of external users and FEMA contractors.

4) The designated FEMA official verifies the accuracy of internal user (FEMA employees and contractors) information. Designated FEMA officials are usually the supervisors of FEMA employees and CORs for the contractors.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that information collected and maintained in APS may be inaccurate or erroneous.

Mitigation: APS mitigates this privacy risk through the user information verification process, whereby APS uses existing data within ADD to verify FEMA employee information and uses the IdP to verify the identity of external users and FEMA contractors (internal users). This risk is also mitigated through the redress process prescribed for each source system (i.e., disasterassistance.gov, NSS, DAIP, and ADD). Additionally, designated FEMA officials (supervisors of employees or CORs for contractors) verify internal user information. Internal users may also call the FEMA Help Desk to correct inaccurate information. External FAMS users can correct their information by logging into the website (www.disasterassistance.gov) or they may call 1-800-621-3362 to correct their information.

Privacy Risk: There is a privacy risk that the IdP inaccurately fails or passes an individual.

Mitigation: APS mitigates this privacy risk by setting up a manual review process for applicants who have received a "fail" flag. In order to mitigate the risk of inaccurate passing, APS has agreements with the IdP that guarantees the accuracy of the data. APS conducts routine reviews of the accuracy of data from the IdP. If the IdP inaccurately passes an applicant, the applicant is not able to access any status information without going through the identity authentication process. The manual review process verifies that the applicant actually needs access to the system by verifying the user's address with a known declared disaster area.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

APS is FEMA's standardized, configurable, and comprehensive security gateway and interface to FEMA applications and systems. APS collects PII from internal users (FEMA employees and contractors) and external users (members of the public registering for disaster assistance and federal, state, local, and tribal government officials assigned to support disaster response efforts) in order to grant user access to FEMA's network and ultimately its resources, systems, and services.

SSNs are not stored within APS. However, the SSNs of FEMA employees are verified against existing information within ADD. PII such as full name, home address, telephone numbers, government agency, and company information of external users and FEMA contractors are collected and submitted through the IdP for verification of identification. The data is not stored by the IdP.

Once the user's information is verified through the APS process, APS creates the usernames and assigns roles and access rights to the various FEMA source systems.

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.

APS does not conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

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

FEMA assigns roles and responsibilities to internal and external users. Internal users are FEMA employees and contractors. External users are members of the public requesting and/or registering for

disaster assistance as well as federal, state, local, and tribal government officials. There are no other components with assigned roles and responsibilities within APS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that information could be used for purposes other than that for which it was collected.

Mitigation: FEMA mitigates this privacy risk by limiting the collection of information to only that which is required to establish user account profiles. Access to APS is limited to only those with a "need to know" in order to perform their official duties. External users can only access information about themselves; therefore, there is no opportunity for external users to misuse information about another individual. Internal users must attend "Rules of Behavior" training and must agree not to use the information for other purposes. Rules of Behavior training is required annually by all internal users. Additionally, all internal users must sign a non-disclosure agreement before receiving access.

Section 4.0 Notice

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

FEMA provides notice of its collection of information for external users at FEMA's public facing website/source system located at http://www.disasterassistance.gov (which is hosted by DAIP). At the front page of the site, there is a link to the Privacy Act Statement that outlines the authority, purpose, and uses of the information. It also explains expectations for use of the government site. The user must agree before access is granted.

FEMA provides notice to internal users (FEMA employees and contractors) during the hiring/on-boarding process through Privacy Act Statements.

FEMA also provides notice by way of this published Privacy Impact Assessment and the SORNs mentioned in section 1.2.

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

FEMA provides internal users the opportunity to consent to or decline to provide information during the hiring/on-boarding process and external users the opportunity during the disaster assistance application process and the disaster response engagement process; all of which occur prior to the information collection by APS.

If an individual declines, APS will not establish a USERID nor allow the individual to access FEMA's network and critical systems. As a result, disaster registrants (external users) will not receive services during a disaster. Federal, state, local, and tribal government officials (external user) and internal

users (FEMA employees and contractors) will not have access to the FEMA systems necessary to perform their jobs functions.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that users will not receive notice at the time their information is collected.

Mitigation: FEMA mitigates this privacy risk by providing notice of collection of information in several ways including through Privacy Act Statements on the web and mobile sites. In addition, disaster registrants using the www.disasterassistance.gov website to apply for assistance must electronically accept the Privacy Act Statement before APS will collect their information as part of the application process. Lastly, notice is provided to users through the publication of this PIA and the listed SORNs in section 1.2.

Section 5.0 Data Retention by the project

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

FEMA retains the information in APS pursuant to NARA Authority N1-311-89-5, Item 1. These records are related to all users of APS. Specific data regarding the records are outlined in Section 2.1. Additionally, audit logs capturing when the user logs in and accesses FEMA resources, which include: login time, USERID, and resources accessed via APS are retained. The records are accessible on FEMA's server for 30 days, then recorded on back-up tape and retained in a secure FEMA location for seven years.

Sensitive PII (i.e., SSN) is verified against existing information in ADD upon initial user profile creation within APS. The SSN is not part of the logs that are retained within APS. The SSN is verified against the record within ADD using SSL encryption and discarded after verification and not stored within APS.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that APS will retain information longer than necessary.

Mitigation: APS stores user information and audit logs on back-up tape in a secure FEMA location that is only accessed by authorized personnel. After seven years, the tapes are completely erased prior to re-use or they are destroyed if the tapes are degraded beyond reuse. The information on the tapes is purged using NIST SP 800-88 process before destruction. APS leverages SOPs to establish and track destruction to ensure appropriate retention and destruction dates are met.

Section 6.0 Information Sharing

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

Information is only shared outside of DHS when external users' information (e.g., individuals requesting disaster assistance) is submitted to the IdP for the purpose of identity verification as explained in Section 2.3.

For the identity verification process, information is shared under routine use (H) of DHS/ALL 004- General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792. APS shares information because the IdP provides identity proofing and verification for all external users and internal FEMA contractors.

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

With the exception of using the IdP for identification verification as outlined in Section 2.3, APS does not share information outside of DHS as part of normal agency operations.

6.3 Does the project place limitations on re-dissemination?

With the exception of using the IdP for identification verification as outlined in Section 2.3, APS does not share information outside of DHS as part of normal agency operations. Information sharing takes place at the source systems (www.disasterassistance.gov, NSS, DAIP, and ADD) level, pursuant to published Routine Uses in the associated SORNs outlined in Section 1.2.

FEMA has a contract with the IdP that specifies the purpose and use of the data. The IdP does not store personal information provided by FEMA in its system, nor does it re-disseminate or share the information with any other entity.

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

APS does not share information outside of DHS as part of normal agency operations. Information sharing takes place at the source systems level. As identified in the SORNs in section 1.2, requests for records may be submitted to the FEMA Disclosure Office, pursuant to the Freedom of Information Act (FOIA) and the Privacy Act. The Disclosure Office maintains the accounting of what records are disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: FEMA mitigates the privacy risk by not sharing information in APS as part of normal agency operations; with the exception of using the IdP for identification verification. DHS-

FEMA has a contract with the IdP that specifies the purpose and use of the data. The IdP does not store personal information provided by FEMA in its system, nor does it re-disseminate or share the information with any other entity.

FEMA further mitigates the risk related to information sharing by requiring all users to complete security and privacy awareness training, which includes appropriate and inappropriate uses and disclosures of the information accessible to them as part of their official duties. User activity in the system is monitored and audited. If a user inappropriately uses or discloses information, he or she is subject to lose access and the disclosure will be referred to the appropriate internal investigation entities. Additionally, users are required to undergo system access recertification annually, which includes Rules of Behavior and privacy training.

Section 7.0 Redress

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

Records collected, maintained, and used within APS are derived from various FEMA source systems. APS users, both internal and external, can file a Privacy Act Record Amendment Request with FEMA to correct any personal information that cannot be corrected at the source system level. Internal users can also contact the FEMA Helpdesk to correct their information. External users can also access and correct their personal information online via https://portal.fema.gov/famsVuWeb/home using the USERID, password, system generated PIN, and authentication that was established during the account creation process.

As per the applicable SORN outlined in Section 1.2, written requests pursuant to the Privacy Act/Freedom of Information Act (FOIA) may be submitted to: FEMA Disclosure Officer, Records Management Division, 500 C Street, SW, Washington, DC 20472.

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

The procedures outlined in Section 7.1 above may be used to correct inaccurate data.

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

The SORNs listed in Section 1.2 and this PIA provides notice regarding how users can correct their information. External users (disaster applicants) may also login to https://portal.fema.gov/famsVuWeb/home to review and correct their information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that internal and external users will not know the proper procedure for providing redress to their personal information in APS; specifically because information in APS is derived from various source systems as opposed to directly from the individual.

.**Mitigation:** This privacy risk is mitigated as noted in Section 7.1 above. Additionally, the SORNs, this PIA, and the various source system PIAs provide information about the redress processes.

Section 8.0 Auditing and Accountability

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

FEMA ensures that the practices stated in this PIA are followed by leveraging SOPs, which are updated annually. In addition, relevant meetings, record retention schedules, and security measures promote adherence to the practices stated in this PIA. APS also has auditing and accountability capabilities. Audit logs capture login records of when users log in and access resources, which include login time, USERID, and resources accessed through APS. These audit logs are retained as an official record in accordance with the files plan and records retention schedule.

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

FEMA requires all APS users to take privacy awareness and information security awareness training annually, in accordance with the FEMA training guidelines. FEMA does not grant users access to the various FEMA system(s), via APS, until the privacy and security trainings are completed. An annual training conference is given to APS users, including FEMA staff, contractors, and federal, state, and local POCs. In addition to meeting the privacy awareness and information security awareness training requirements, FEMA requires all contract staff to adhere to the Privacy Act and confidentiality clauses per terms of their contracts with FEMA.

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

For all internal users, APS uses a role-based access control mechanism to control access to both data and functionality. APS implemented the security access controls in accordance with Group Policy Settings. This administers user roles and permissions based on organizational position, which are assigned and approved by the internal user's supervisor. All internal users must also read and sign the rules of behavior agreement.

External users, specifically disaster registrants, are granted access contingent upon their address being located in a known/declared disaster area. This means that disaster survivors submit their personal information to create an account. Based upon the address entered into the source system, authorized officials/gatekeepers (federal, state, local, and tribal officials under FEMA oversight) review the requests to validate that there is a declared disaster in the respective areas and that access is required. APS grants external users access to specified FEMA applications.

All users are added to a certain group in order to have specific authorized access. This ensures that users can gain access to their authorized applications, resources, and systems.

Access to data and specific system functions have been pre-defined for each user role. This is based on the principles of separation of duties and "authorized need to know." This policy pertains to all APS users, both internal and external.

FEMA assigns APS administrator "rights" to certain FEMA employees and contractors (internal users) with a "need to know" for the purpose of assisting with vetting and granting users access to FEMA's resources. Permissions and access rights differ among FEMA employees and contractors, other government officials, and disaster applicants. APS determines access rights for both internal and external users based upon position and role-based criteria.

APS keeps a login record of when users log in and access resources, which includes login time, USER ID, and which source systems were accessed through APS. There is an official DHS banner posted on the initial webpage and startup screen for each source system. The banner indicates that only authorized personnel can access the system. The record of access for external (FAMS) users is stored at the website/source system level. The FAMS account is used for authentication into all FEMA public-facing systems used for disasters. Internal user access is approved by the designated FEMA authority, which is usually the supervisor of the FEMA employee or the COR for the FEMA contractor.

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?

APS does not require information sharing agreements or MOUs since it does not share information outside of DHS as part of normal operations, with the exception of using the IdP for identification verification. FEMA has a contract with the IdP that specifies the purpose and use of the data. The IdP does not store personal information provided by FEMA in its system, nor does it re-disseminate or share the information with any other entity.

Responsible Officials

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

Approval Signature

Original signed and on file at the DHS Privacy Office.

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