Privacy Impact Assessment
for the

FEMA Physical Access Control Systems

DHS/FEMA/PIA-051

April 20, 2018

Contact Point

J'son Tyson
Chief, Identity Credential & Access Management
Federal Emergency Management Agency
(202) 641-1686

Reviewing Official

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency's (FEMA) Office of the Chief Security Officer (OSCO) owns and operates the Physical Access Control System (PACS). PACS supports a range of functions related to managing physical access by individuals to FEMA facilities. PACS allows authorized security personnel to simultaneously manage and monitor multiple entry points from a single, centralized location. FEMA is conducting this PIA to analyze the personally identifiable information (PII) that PACS collects, uses, and maintains.

Overview

PACS is a single suite of applications that supports physical security operations at all FEMA facilities. These include permanent (e.g., FEMA Headquarters, Regional Offices), temporary (Joint Field Offices and Disaster Readiness Centers (DRC)), and transient (Disaster Survivor Assistance centers and Mobile DRCs) facilities. FEMA OCSO uses the system to support four major functions: visitor management, physical access control, intrusion detection, and video surveillance. PACS functions may vary based on the type of facility; however, all facilities have the intrusion detection function. PACS users are OCSO and DHS Federal Protective Service (FPS) personnel who operate and maintain PACS as part of their larger mission to implement security policies, programs, and standards to protect and safeguard personnel, property, facilities, and information.

PACS hosts a suite of applications that operate electronic security boundaries and alarms at each FEMA facility. The boundaries and alarms are designed to prevent and deter individuals from reaching FEMA personnel and assets to which they could pose a security risk. PACS also serves as a repository for all employee and visitor PII required for authorizing and monitoring physical access to FEMA facilities.

PACS Functions

PACS supports four major functions: 1) visitor management; 2) physical access control; 3) intrusion detection; and 4) video surveillance. Applications and processes supporting each function operate independently at the direction of PACS administrators. The video surveillance function relies on Closed-Circuit Television (CCTV) and is therefore covered by a separate PIA specifically dedicated to CCTV.[1] This PIA covers collection and handling of PII for the other three functions.

[1] DHS/ALL/PIA-042 Closed Circuit Television (CCTV) (July 18, 2012), *available at* https://www.dhs.gov/publication/dhs-all-pia-042-cctv-systems-0.

Visitor Management

The FEMA PACS visitor management function automates and coordinates the visitor screening process within OCSO, and authorizes and records entry and exit of visitors requiring access to FEMA facilities. Visitor management is governed by DHS Instruction Manual 121-01-011-01, Visitor Management for DHS Headquarters and DHS Component Headquarters Facilities, FEMA 121-1 Personal Identity Verification Guidance, FEMA Directive 121-3 Facility Access, and FEMA 121-3-1 Credential and Access Reference. Per this guidance, OCSO distinguishes between four categories of individuals for purposes of screening:

- Current FEMA Employees and Contractors;
- Non-FEMA U.S. Government Employees;
- Non-Federal Employee U.S. Citizens; and
- Foreign National Visitors.

FEMA OSCO defines a visitor as any individual requesting access to a FEMA business facility; this may include FEMA employees and contractors who are requesting access to facilities other than their assigned workplace. The type of PII collected and use of that PII varies by category of visitor, as detailed below.

Current FEMA Employees

In general, Current FEMA employees and contractors in possession of a valid DHS-issued Personal Identity Verification (PIV) card are not subject to additional visitor screening in order to access most FEMA facilities. All collection and use of PII associated with acquiring and maintaining DHS PIV cards is covered under a separate PIA.[2]

Certain FEMA facilities are designated as high security and require current FEMA employees and contractors to fill out FEMA Form 649-0-1-2, Facility Access Request. This form requests the information that was originally collected for PIV card/FEMA Access Card issuance, and additionally collects work and mobile phone numbers, employer name, work location, supervisor name, supervisor phone number, and driver's license state and number. This information is collected in order to run an additional background check through the National Crime Information Center (NCIC).[3] NCIC is a computerized database administered by the U.S. Federal Bureau of Investigation (FBI) that provides ready access to law enforcement agencies for making inquiries about an individual's criminal history. This check verifies that individual does not have any outstanding warrants for criminal activities indicating a risk to the Department.

[2] DHS/ALL/PIA-014(e), Personal Identity Verification/Identity Management System (May 18, 2007), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall014-pividms-may2017.pdf.
[3] For more information about NCIC, *see* https://www.fbi.gov/services/cjis/ncic.

Additionally, during disaster support operations, FEMA hires individuals from the affected area to assist with disaster recovery. These individuals, considered FEMA employees, require physical access to FEMA facilities but do not always require access to the FEMA information technology (IT) network. In these situations, FEMA issues the employee a FEMA Access Card for use with PACS. The information collected from these individuals is the same as the information collected for issuing employee PIV cards, and for the period of their employment they are considered FEMA employees.

Non-FEMA U.S. Government Employees

U.S. Government employees and contractors employed at federal agencies other than FEMA, including other DHS components, are considered visitors. However, such individuals are exempt from visitor screening requirements at all FEMA facilities, unless specific direction is given by OCSO to the contrary. To access any FEMA facility, visitors falling under this category must present a valid employee identification card issued by their employing agency and an on-site FEMA-employed sponsor must attest that the visitor requires access to the FEMA facility by submitting a visitor request form. The visitor's first and last name, agency of employment, and authorized armed status[4] on official duty are recorded in PACS as well as the first and last name of the sponsor. This information may be provided in advance or, if no notice of the visit is given, at time of entry.

Occasionally, other federal agencies require access to FEMA facilities as a part of their response to a security event. In these cases, FEMA can program an agency's law enforcement credentials to be accepted by PACS for unescorted access. The information collected from individuals in these circumstances by FEMA is the same as other non-FEMA U.S. Government employees. After the security event has been resolved, access is revoked and the record is retained in accordance with the PACS retention schedule.

Non-Federal Employees (U.S. Citizens)

U.S. citizens who are not employed by the U.S. Government and who intend to visit a FEMA facility for official FEMA business are subject to a background check using the NCIC system. These individuals include state and local government officials and members of the first responder community attending training at a FEMA facility. For the purpose of this PIA, this does not include disaster survivors seeking access to a temporary FEMA location established during a presidentially declared disaster to apply for assistance, such as the DRCs. Such disaster locations are accessible to the public without requiring any visitor screening or background check processes.

As with non-FEMA U.S. Government employees, all prospective visitors falling under the non-federal U.S. citizen category must be sponsored by an on-site FEMA employee who serves as

[4] Armed status refers to whether the visitor will be carrying a firearm onto the DHS facility.

OCSO's primary point of contact during the screening process. Sponsors initiate the screening process for non-federal U.S. citizens by contacting the FEMA Access Control office to communicate their intention to host one or more visitors.

To begin the screening process, FEMA OCSO collects PII from prospective visitors using FEMA Form 649-0-1-2, Facility Access Request. PII collected on this form includes full name, Social Security number (SSN), date of birth, driver's license number and state issued, place of birth, citizenship status (i.e., U.S. citizen, Y/N), gender, and place of employment in order to initiate and conduct the background check through NCIC. OCSO uses the data on Form 649-0-1-2 to create a record in PACS, and to run a background check through NCIC. This check verifies that individual does not have any outstanding warrants for criminal activities indicating a risk to the Department.

OCSO then grants or denies access based on the information provided by NCIC. The determination to grant or deny access is communicated back to the sponsor and recorded in the visitor management module of the PACS along with the date the NCIC search was conducted. Only the determination itself is communicated to the sponsor and recorded in the PACS. The basis for the determination is neither recorded nor shared. If the visitor applicant would like to discuss the reasons for a denial of access to a facility, he or she may do so by contacting the FEMA Access Control Office using contact information listed on the two-page instruction sheet provided to the visitor by the sponsor.

Foreign National Visitors (Non-U.S. Citizens)

Foreign visitors (including U.S. Lawful Permanent Residents) to FEMA facilities are also subject to the NCIC screening process, and as with non-FEMA U.S. Government employees and non-federal U.S. citizens, foreign nationals must be sponsored by an on-site FEMA employee. These individuals include foreign government, foreign emergency/crisis managers, and any person who does not have U.S. citizenship. Non-U.S. citizens who intend to visit a FEMA facility are asked to complete DHS Form 11055 at least 30 days prior to their visit. This form should be submitted to the visitor's point of contact at FEMA. Two forms of identification that include a photo (e.g. diplomatic identification, alien registration card, passport, government identification) should be presented at the time of the visit.

In addition to using NCIC for background screening, OCSO will also use the Foreign Access Management System (FAMS)[5] to screen all prospective visitors to FEMA facilities who are not U.S. citizens. While NCIC screenings of foreign visitors disclose only information related to criminal activities that occur within U.S. jurisdiction, FAMS screenings rely on information collected by the U.S intelligence community regarding any activities of concern that occurred

[5] DHS/ALL/PIA-048(b), Foreign Access Management System (April 10, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-all048-fams-april2017.pdf.

outside of the United States. None of the information collected or displayed by FAMS is connected to PACS systems or processes, and all collection and handling of PII associated with screening foreign nationals through FAMS is covered under a separate PIA.[6] PACS stores the visitor's approval or denial of entry based on the response from FAMS.

To grant access to foreign visitors and verify identity, FEMA makes a photocopy of the documents listed in section 2.1. These documents are added to the visitor record and maintained for a period of five years from the date of the most recent visit, after which they are destroyed and cannot be recovered.

Physical Access Control

The physical access control function of PACS regulates access to the majority of FEMA facilities. This function is in place at all permanent facilities. Temporary and transient facilities may or may not have this function. Most facilities control access through security guards and/or smart card readers. The smart card readers translate a unique code on an employee's PIV card or other approved credential (e.g., FEMA Facility Access card or law enforcement credential) to verify if the individual has authorization to access a given space. The code is linked to the individual's record within PACS. OCSO can code the credentials for swipe access to the facilities themselves and also to more secure areas within the facilities. Every time an employee crosses a physical security boundary using a PIV card, the card reader at that location collects the employee's full name, PIV card number, and the time, date, and location of entry and logs the information in PACS.[7]

Intrusion Detection

The FEMA intrusion detection function allows OCSO and FPS to identify and monitor the unauthorized intrusion of persons or devices into secure spaces at all FEMA facilities. It generally consists of sensors, lights, and other mechanisms (e.g., annunciation alarms) used by OCSO and FPS to ascertain physical presence and track unauthorized persons who cross or attempt to cross security boundaries. Records are created in PACS of all alarm activations and certain other issues, such as communications and power failures. No PII from individuals is collected as part of the intrusion detection function.

Video Surveillance

FEMA deploys a number of Closed Circuit Television (CCTV) systems throughout the agency. FEMA's CCTV systems are used to obtain real-time and recorded visual information in and around federal worksites and facilities to aid in crime prevention and criminal prosecution,

[6] *Id.*
[7] For information regarding how personal identifiers are stored and made retrievable on DHS PIV Cards, *see* DHS/ALL/PIA-014(c) Personal Identity Verification Management System (October 20, 2015), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-update-dhs-all-014-c-oct-2015.pdf.

enhance officer safety, secure physical access, promote cost savings, and assist in terrorism investigation or terrorism prevention. These systems have the ability to capture images of people, license plates, and any other visual information within range of the cameras. FEMA's video surveillance function is covered in its entirety by a separate PIA.[8]

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?

DHS has legal authority under 40 U.S.C § 1315[9] to protect the buildings, grounds, and property owned, occupied, or secured by the Federal Government, and the persons on the property.

DHS Instruction Manual 121-01-011-01, Revision 00, Visitor Management for DHS Headquarters and DHS Component Headquarters Facilities, establishes procedures and program responsibilities in accordance with Department of Homeland Security (DHS) Directive 121-01, Chief Security Officer and DHS Delegation 12000, Security Operations within the Department of Homeland Security**.**

FEMA Directive 121-1, Personal Identity Verification Guidance, establishes the policy and procedures for FEMA preparation, issuance, use, and disposition of DHS PIV cards for all eligible FEMA employees and qualified contractors as required by Homeland Security Presidential Directive 12 (HSPD-12).

FEMA Directive 121-3, Facility and Access, establishes the policy for entering and exiting FEMA facilities.

FEMA Directive 121-3-1, Credential and Access Reference, establishes FEMA policies and procedures to govern the issuance, use, and destruction of all types of FEMA badges and credentials, and how they are used to gain physical access to FEMA facilities.

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

The information in PACS is collected, used, disseminated, and maintained in a manner consistent with the purposes, categories of records, routine uses, and retention periods described in the following Department-wide SORNs:

---

[8] DHS/ALL/PIA-042 Closed Circuit Television (CCTV) (July 18, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/PIA%20DHS%20CCTV%2020160222.pdf.

[9] *See* 40 U.S.C. § 1315 - Law enforcement authority of Secretary of Homeland Security for protection of public property, *available at* https://www.law.cornell.edu/uscode/text/40/1315.

- DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records allows for the collection of records related to the Department's facility and perimeter access control, including access to FEMA information technology and access to classified facilities, as well as visitor security and management.[10]
- DHS/ALL-023 Personnel Security Management System of Records allows for the collection of information related to background investigations and adjudications as well as other activities relating to personnel security management responsibilities at FEMA.[11]
- DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records allows for the collection of reports documenting the results of law enforcement activities in support of the protection of property owned, occupied, or secured by FEMA.[12]
- DHS/ALL-026 Personal Identity Verification Management System of Records allows for the collection of PII data elements necessary to identify individuals and perform background or other investigations on those individuals to determine their suitability for access to federally controlled facilities.[13]

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

A System Security Plan for PACS was completed on July 11, 2017, and a security certification authorizing the Authority to Operate (ATO) was granted on September 11, 2017, by the DHS Information Systems Security Manager Certifying Official. The ATO will expire on September 11, 2018. The PACS Federal Information Security Management Act (FISMA) ID is FEM-03703-MAJ-03703.

A new ATO will be issued upon the completion of this PIA.

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

Yes. PII retained by PACS is covered by NARA General Records Schedule (GRS) 5.6, *Security Records* and by GRS 3.2, *Information System Security Records*.

For areas under maximum security, FEMA retains records of PII from visitors in accordance with GRS 5.6, item 110, meaning records are temporary and are destroyed when 5

[10] DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management, 74 FR 42578 (August 24, 2009).
[11] DHS/ALL-023 Personnel Security Management, 75 FR 8088 (October 1, 2009).
[12] DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security, 82 FR 27274 (June 14, 2017).
[13] DHS/ALL-26 Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

years old, but longer retention is authorized for business use. For other areas, records are retained in accordance with GRS 5.6, item 111, meaning records are temporary and are destroyed when 2 years old but longer retention is authorized for business use.

FEMA retains records from PACS users and administrators in accordance with GRS 3.2, item 031, *System Access Records.* Per this guidance, PII is destroyed six years after a password is altered or a user account is terminated.

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.

FEMA uses Office of Management and Budget (OMB) Control Number 1660-NW75; FEMA Form 649-0-1-2 to collect PII from prospective visitors for the purpose of visitor screening, and also for granting FEMA employees and contractors access to high security areas.

Section 2.0 Characterization of the Information

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

FEMA collects information from anyone accessing a facility where PACS is deployed. This includes FEMA employees, contractors, and visitors.

The information below is collected from the DHS Identity Management System (IDMS)[14] when the FEMA employees or contractors are issued a PIV card, and is entered into PACS at the time of PIV card issuance. IDMS automatically sends the information below to FEMA PACS any time FEMA personnel receives a new PIV card. This information is stored as a part of the PACS profile for PIV card holders:

- Name (first, middle, last);
- Date of birth;
- Agency (e.g., FEMA);
- Organization affiliation (e.g., FEMA);
- Employee affiliation (employee or contractor);
- Facial image;
- Security clearance type;

[14] DHS/ALL/PIA-014(e) Personal Identity Verification/Identity Management System (May 18, 2007), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall014-pividms-may2017.pdf.

- Email contact;
- User principal name (Microsoft account name);
- PIV Card Identifiers;
- Citizenship status;
- Electronic Data Interchange Person Identifier (EDIPI); and
- Public Key Infrastructure Public Key Certificate Data.

The additional information below is collected when a FEMA employee, contractor or non-FEMA employee requests access to a high-security facility:

- Work and mobile phone numbers;
- Employer name;
- Work location;
- Supervisor name;
- Supervisor phone number; and
- Driver's license state and number.

The information below is collected from U.S. Government employees and contractors requesting a visit to a FEMA facility:

- Full name;
- Agency;
- Armed status; and
- Full name of sponsor.

For non-U.S. government employees, PACS collects one of the following identification documents for visitor (temporary) access to FEMA facilities:

- Driver's license state and number;
- Passport number;
- Border Crossing Card (Form DSP-150);
- Department of Homeland Security "Trusted Traveler" Cards (Global Entry, NEXUS, SENTRI, FAST);
- U.S. Certificate of Naturalization or Certificate of Citizenship (Form N-550);
- U.S. Permanent Resident Card (Form I-551); and
- Native American Tribal Photo ID.

The information below is collected from non-U.S. government employees and used to create a record in PACS and perform a background check in NCIC:

- Full name;
- Address;

- SSN;
- Date of birth;
- Driver's license state and number;
- Place of birth;
- Citizenship status;
- Gender; and
- Place of employment.

In addition to the PII collected as part of the physical access control function by card readers or recorded during PIV card issuance, PII of PACS application users and administrators is also collected when system accounts are initially set up, as discussed below.

PACS users and administrators are required to complete a user account request form in order to set up or make changes to their system accounts. Only FEMA OCSO personnel may have access to be a user or administrator of PACS. This form requests the following PII in order to create a PACS account:

- Full name (first, middle initial, and last);
- Phone number;
- Email address;
- FEMA Enterprise Network (FEN) User Name; and
- Employment position.

The user access request form includes a Privacy Notice listing the authorities FEMA uses to collect the PII, the purpose for which the PII is requested, and routine uses for the PII. It also contains a disclosure statement explaining that failure to provide the PII may result in a denial of access to PACS.

Users log in to PACS with a unique username and a password that must be changed every 90 days. This is true regardless of which of the four PACS functions users intend to execute.

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

Generally, an on-site FEMA-employed sponsor collects PII directly from visitors and completes FEMA Form 649-0-1-2 Facility Access Form with all visitor PII required for screening and visitor processing. If visitors are reluctant to share their PII with the sponsor, they may arrive at the visitor management office at least 30 minutes prior to their scheduled visit to provide the PII directly.

Additionally, OCSO receives an "approve entry" or "disapprove entry" reply from NCIC in response to a background request. This background request is sent via PACS for all non-FEMA visitors to FEMA facilities.

FEMA PACS users complete a user account form when requesting access to the system. For FEMA employees and contractors, IDMS will make data available to PACS for data synchronization and access control. PACS has a connection to IDMS, and the connection is used to capture information from PIV card holders to create records in PACS. The IDMS automatically sends the information outlined in section 2.1 to the FEMA PACS any time FEMA personnel receive a new PIV card

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. PACS does not use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

In general, FEMA receives information directly from the visitor via their sponsor. FEMA staff validate identification documents (e.g., driver's license) presented at the time of the visit to verify identity and ensure the accuracy of the information on record. OCSO does not investigate sponsors or visitors to determine if the information they provide is accurate. If a visitor is informed of a denial of access, the visitor may contact the FEMA Access Control Office to validate whether the information submitted was correct. If it was not, the visitor will be provided an opportunity to provide the correct information.

For FEMA employees and contractors, PACS receives all data from IDMS as part of the application and onboarding process. Employees and contractors provide their information directly to FEMA during these processes. During the initiation of the background check process, employees and contractors have an opportunity to correct any inaccurate information that may have been provided. FEMA employee and contractor information is also verified during the background check process. FEMA assumes the information on the PIV card to be accurate upon issuance of the card.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Visitor management personnel may collect more PII than is needed to conduct required visitor management functions.

Mitigation: PII collected via FEMA Form 649-0-1-2 Facility Access Request, including SSNs, is the minimum required to screen prospective visitors through NCIC and to create visitor

records that make the visitors easily and uniquely identifiable and record their last known location in the event of a security incident. Although these forms are generally collected for each visit to FEMA facilities, visitors may inform the FEMA Access Control Office that they have previously provided the requested PII and request that their PII be retrieved from the existing record using their full legal name.

Privacy Risk: FEMA may make a decision to deny access to a prospective visitor based on the submission of inaccurate information.

Mitigation: This risk cannot be fully mitigated. If the visitor is denied access based on submission of PII that may be linked to another person (with the same name) that has a criminal record, any follow up or clarifying information would be supplied by the visitors themselves or by their sponsors. If visitors who are denied access would like to discuss the reasons for the denial, they may contact the FEMA Access Control office. In these cases, if OCSO provides a reason for the denial that does not reflect the individual's actual history, OCSO will validate that the PII previously provided for the NCIC screening was accurate. If it was not, OCSO will run the background check again using the correct PII, if the visitor would still like access to FEMA facilities.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

PACS uses PII and one of the approved identity documents to authenticate the identity of federal employees, FEMA contractors and employees, and visitors who have entry authorization.

OCSO and FPS use this information as well as information collected on visitor forms to verify the identity of individuals and to conduct background checks.

Additionally, FEMA collects the following PII when setting up their system accounts: first and last names, middle initials, phone numbers, email addresses, FEMA user name, and position description from PACS users and administrators.

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. PACS does not conduct searches, queries, or analyses in electronic databases to discover predictive patterns or anomalies.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information could be used in a manner inconsistent with the purpose of the collection.

Mitigation: FEMA mitigates this risk by limiting PACS user permissions to a level appropriate for their everyday duties. In addition, PACS administrators monitor all transactions using daily transaction reports. If any anomalies are discovered, the administrator reports the transaction to the system owner for investigation. Finally, FEMA OCSO provides role-specific user training that includes proper use of PACS and the information collected.

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.

Visitors are provided notice by their sponsors via a Privacy Act Statement present on the Facility Access Request form that contains the proper authorities for collecting the PII, the purpose of the information collection, routine uses of the information, and a disclosure statement explaining that visitors are not required to provide their PII, but that failure to do so may result in a denial of access to FEMA facilities. Additionally, visitors are provided with a two-page handout that includes general information about visiting a FEMA facility and contact information for the Access Control office in the event the visitor would like to seek access or redress.

Additionally, FEMA will continue to provide notice to the public through this PIA and through the SORNs listed in section 1.2 of this PIA.

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

The submission of PII is voluntary. Visitors are advised that access control procedures require the submission of their PII and that FEMA will use this information to determine if access may be granted. Failure to provide PII may result in a determination to deny access to FEMA facilities since it will be impossible to conduct the required background check through NCIC. This information is provided to visitors by their sponsors via the Privacy Notice contained on FEMA Form 649-0-1-2 Facility Access Request. FEMA employees and contractors who refuse to provide

their information for access control purposes may be denied access to certain facilities or IT networks.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals providing information to FEMA may not have notice that their PII will be stored in PACS.

Mitigation: This risk is mitigated by publication of this PIA, which serves as an additional notice as well as an explanation regarding the way FEMA receives and manages PACS data. Notice is also provided through the FEMA Facility Access Request, which includes a Privacy Act Statement.

Section 5.0 Data Retention by the project

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

FEMA retains records of PII from visitors of high security areas in accordance with GRS 5.6, item 110. Per this guidance, PII when 5 years old, but longer retention is authorized for business use.

FEMA retains records of PII from visitors of all other areas in accordance with GRS 5.6, item 111. Per this guidance PII is destroyed when 2 years old, but longer retention is authorized for business use.

FEMA retains records from PACS users and administrators in accordance with GRS 3.2, item 031, System Access Records. Per this guidance, PII is destroyed six years after a password is altered or a user account is terminated.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: The completed FEMA Form 649-0-1-2 Facility Access Request may be retained longer than necessary to accomplish a legitimate purpose or inconsistently with the records schedule.

Mitigation: FEMA's process uses NARA-approved retention schedules to retain and eventually dispose of the data. In addition, FEMA leverages training and documentation, such as standard operating procedures, to inform FEMA users of proper record retention standards.

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.

Yes. Visitor management information is shared with the FBI for the purpose of screening FEMA employees requesting access to high security areas and visitors that are not employed by the U.S. Government through NCIC. The FBI provides visitor management personnel at FEMA facilities with NCIC user accounts to remove any risk that data could be intercepted during transmission through a system-to-system interface. OCSO personnel are required to complete training and obtain a certification prior to receiving an NCIC user account to ensure they understand relevant operational and security requirements.

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

OCSO only shares PACS-related information outside of DHS in accordance with Routine Use H as defined in the Facility and Perimeter Access Control and Visitor Management SORN[15] noted in 1.2. Specifically, OCSO Access Control Office personnel share PII with the FBI in order to conduct a criminal background check on prospective visitors to FEMA facilities to determine whether they could pose a security risk to FEMA personnel and assets. Routine Use H allows sharing of information with other federal agencies if the information is relevant and necessary to a DHS decision concerning the issuance of a grant or other benefit, and when disclosure is appropriate to the proper performance of the official duties of the person making the request. OCSO's external sharing with the FBI is compatible with this routine use because the PII is shared by visitor management personnel in the course of performing official duties related to determining whether to grant prospective visitors the benefit of access to DHS facilities.

6.3 Does the project place limitations on re-dissemination?

Yes. The FBI only re-disseminates PII obtained from OCSO during the course of screening prospective visitors through NCIC in accordance with the routine uses defined in the FBI's NCIC SORN.[16]

[15] DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management, 74 FR 42578 (August 24, 2009).
[16] FBI-001 National Crime Information Center (NCIC) 64 FR 52343 (September 28, 1999).

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

PACS provides the means to record all disclosures of PII to the FBI that are required to screen visitor applicants through NCIC. Every time an NCIC search is conducted, the date and time of the search is recorded in the visitor's record. Thus, each adjudication of visitor access recorded in PACS is essentially documentation of information sharing with the FBI.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Individuals authorized to access PACS may conduct unauthorized activities such as extracting and sharing information with unauthorized recipients.

Mitigation: OCSO has established numerous controls to address this risk. For example, a data/report request form must be completed, signed, and approved by the requester, requester's manager, and their Division Chief prior to the creation or distribution of personnel security data to avoid accidental, inappropriate, or unauthorized use of the data. Access to information is then only granted on a need-to-know basis. Additionally, access to PACS requires a FEMA domain account and requires that the user be logged in to a FEMA Intranet-accessible computer. These user accounts are individually approved by OCSO. Furthermore, all users complete FEMA computer security training and are vetted and cleared for access to privacy-sensitive and classified information. Access is also role-based and users of the system only have access to a limited subset of data based on the concept of least privilege/limited access.

Section 7.0 Redress

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

Visitors who are U.S. citizens, lawful permanent residents, or covered by the Judicial Redress Act, may submit a Privacy Act (PA) request to access their PII. Requests for PA-protected information must be made in writing, and clearly marked as a "Privacy Act Request." The name of the requester, the nature of the records sought, and the required verification of identity must be clearly indicated.

Additionally, all individuals, regardless of citizenship, may seek access to the records maintained by PACS by submitting a Freedom of Information Act (FOIA) request. FOIA requests must be made in writing, and clearly marked as a "FOIA Request". The name of the requester, and the nature of the records sought must be clearly indicated.

PA and FOIA requests should be sent to:

FEMA Information Management Division
Chief, Disclosure Branch
500 C Street, S.W., Mailstop 3172
Washington, D.C. 20472

Lastly, all visitors, regardless of citizenship status, may contact the FEMA Access Control Office at (202) 646-3012 or via email at FEMAAccessControl@fema.dhs.gov for information about any PII about them that is maintained in PACS. If the visitor was attempting to access Mount Weather (MW), they may contact the MW Access Control Office at (540) 542-2081 or via email at FEMA-MW-AreaA-Access@fema.dhs.gov.

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

Visitors have the ability to address inaccuracies in PACS and provide updated information. Visitors who are U.S. citizens, lawful permanent residents, or covered by the Judicial Redress Act, may submit a Privacy Act (PA) request to correct their PII, via the following address:

FEMA Information Management Division
Chief, Disclosure Branch – Attn: PA Amendment Request
500 C Street, S.W., Mailstop 3172
Washington, D.C. 20472.

Once information is submitted to OCSO for entry into PACS, the individual who submitted it may contact OCSO directly. All visitors, regardless of citizenship status, may also contact the FEMA OCSO Access Control Office at (202) 646-3012 via email at FEMAAccessControl@fema.dhs.gov; or if they visited MW, they may contact the MW Access Control Office at (540) 542-2081via email at FEMA-MW-AreaA-Access@fema.dhs.gov; for information about any PII about them that is maintained in PACS.

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

FEMA OCSO notifies individuals of the procedures for correcting their through this PIA and the associated SORNs listed in 1.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A privacy risk associated with this system is that individuals will be unaware of the redress process.

Mitigation: This privacy risk is mitigated because FEMA provides notice of redress procedures to individuals who wish to amend their information within PACS via this PIA and the

SORNs referenced in section 1.2. FEMA OCSO also provides a two-page instruction to FEMA employees and contractors during PII collection, and to visitors via their sponsor, that contains contact information for OCSO.

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?

PACS is safeguarded in accordance with applicable rules, such as those contained in the Department's automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising stored information. Additionally, OCSO visitor management personnel only accept transmission of PII via email when it is password-protected and sent from a FEMA account.

PII maintained in PACS is visible only to authorized users with a need-to-know based on their official duties. All PACS user access is based on pre-defined system owner and management authorized job roles and official duties. These roles and policies are enforced using access control lists. PACS users may only input, update, or delete records or fields to which they are authorized as prescribed by the application user manual and system administration procedures.

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

All FEMA employees and assigned contractor staff complete privacy and security training. PACS users have also undergone necessary suitability investigations and received security clearances for access to sensitive national security information and facilities. Additionally, standard operating procedures and system user manuals describe in detail user responsibilities and training requirements.

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

PACS user accounts are individually approved by OCSO. All users must complete computer security training and must be properly vetted for access to FEMA IT systems and sensitive national security information. Furthermore, access to PACS is role-based, and users of the system have their access limited to a subset of data based on the concept of least privilege/limited access.

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?

PACS establishes data sharing agreements with external entities using Interconnection Security Agreements (ISA). DHS 4300A, Sensitive System Handbook, establishes this requirement for all DHS systems. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same Designated Accrediting Authority (DAA). The ISA documents the security protections that must operate on interconnected systems to ensure that transmissions between systems permit only acceptable transactions. The ISA includes descriptive, technical, procedural, and planning information. It also formalizes the security understanding between the authorities responsible for the electronic connection between the systems. The DAA for each organization is responsible for reviewing and signing the ISA.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: PACS users may be able to access PII in the system that they do not need in the performance of their duties.

Mitigation: OCSO mitigates this risk by limiting access to the visitor management module within PACS to only those whose job duties involve visitor management responsibilities. Similarly, PII from users and administrators is only available to a limited number of other system administrators.

Privacy Risk: Individuals may gain unauthorized access to information in PACS.

Mitigation: Numerous system security controls are in place to prevent access by unauthorized individuals to sensitive information in PACS. For example, specific security roles have been defined and implemented within the application to control access to information. Additionally, all automated data processing equipment supporting the application environment is located in a secure data center. Furthermore, when information is stored as an attachment on a server, file access is restricted by file permissions to prevent those without an appropriate need for accessing the file. Also, network access to the application is made via a Secure Sockets Layer (SSL) connection to the PACS environment. These and other system security controls form the basis for all PACS systems obtaining a system security certification in accordance with OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.

Policy controls have also been established in PACS regarding handling of PII. For example, access to information is only granted on a need-to-know basis. Additionally, access to PACS requires a FEMA domain account and requires that the user be logged in to a FEMA Intranet-accessible computer. Furthermore, user accounts are individually approved by the FEMA Chief,

Identity Credential and Access Management Branch, within OCSO. Access to PACS is role-based and users of the systems have access to a limited subset of data based on their particular job duties. Lastly, PACS contain an audit history log that details what information was accessed, which users accessed it, and when it was queried from the system.

Responsible Officials

William H. Holzerland
Senior Director for Information Management
Office of the Chief Administrative Officer
Federal Emergency Management Agency

Approval Signature

[Original, signed copy complete and on file with the DHS Privacy Office]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security