Privacy Impact Assessment Update
for the

FEMA Physical Access Control Systems

DHS/FEMA/PIA-051(a)

June 22, 2020

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

Reviewing Official
Dena Kozanas
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 Privacy Impact Assessment (PIA) Update to provide notice and assess the privacy impacts of FEMA's use of PACS in ways not addressed in the original PIA, including the collection of additional PII; the expansion of unescorted access to State, Local, Tribal, and Territorial emergency managers; the use of new Facility Access Request forms; and the classified portion of PACS.

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 personally identifiable information (PII) required for authorizing and monitoring physical access to FEMA facilities.

Reason for the PIA Update

FEMA is publishing this PIA update to: (1) describe the collection of additional PII in order to comply with DHS direction related to criminal history record checks; (2) describe the expansion of unescorted access to State, Local, Tribal, and Territorial (SLTT) emergency managers; (3) document the rescission and replacement of FEMA Form 649-0-1-2, Facility Access Request; and (4) document the previously undocumented classified portion of PACS.

1. FEMA has modified PACS to comply with DHS requirements which direct all DHS components to conduct criminal history record checks on visitors to all its facilities.

Previously, FEMA only conducted these checks for visitors to high-security facilities. In addition to the information currently collected to provide access to all FEMA facilities, FEMA will collect and maintain a copy of a visitor's Driver's License, Passport, Tribal Card, or State Identification Card to perform the criminal history record check. FEMA may also generate and maintain a "do not admit" list for individuals that DHS or FEMA deem to pose a safety or security risk to personnel or property. This list will retain an individual's name and photographic image. The list is populated from OCSO, based on the results from the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC),[1] Terrorist Screening Database (TDSB), and Be On the Lookout's (BOLO) from other agencies. The list is maintained in PACS and distributed via password-protected email to facility entrance guards.

2. The original PIA describes FEMA's ability to program an agency's law enforcement credentials to be accepted by PACS for unescorted access. FEMA has expanded this capability to include the credentials of SLTT emergency managers. This does not change the type of PII collected from the credential;[2] however, FEMA will now collect this information from members of the public. Unescorted access will be granted to SLTT emergency managers so they can support response and recovery efforts during suspected and confirmed events. SLTT emergency manager access is a one-time event allowance and access will be disabled after the event concludes.

3. FEMA is making a modification to the method of collecting information from individuals requesting access to FEMA facilities. FEMA Form 649-0-1-2 has been rescinded and replaced with two forms. The forms have been split due to a need to place a higher classification on forms related to high security facilities.

   The first form is FEMA Form 123-3-1-3A. This form is used to grant access to all FEMA facilities, except those designated as high security. PII collected on this form includes full name, home and business phone numbers, Social Security number (SSN), date of birth (DOB), place of birth, citizenship status, alien registration number, gender, and place of employment. In the case of a visitor without a Personal Identification Verification (PIV) Common Access Card (CAC), this form also collects the full name, signature, and contact information of the FEMA employee who will be sponsoring (escorting) the visitor while in the facility.

[1] For more information about the FBI's NCIC, please see https://www.fbi.gov/file-repository/pia-ncic.pdf/view.
[2] Detailed in original PACS PIA, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-fema-051-pacs-april2018.pdf.

The second form is FEMA Form 123-3-1-3B. This form collects the same information and is used to grant access to high security FEMA facilities and becomes classified once it is filled out.

4. FEMA maintains a classified PACS system to protect the sensitive nature of the personnel accessing a specific high security location. This system works identically to the unclassified system.

Privacy Impact Analysis

Authorities and Other Requirements

DHS has legal authority under 40 U.S.C § 13159 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 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.

Characterization of the Information

In addition to the data elements identified in the original PIA, PACS receives and stores the following information:

From all visitors:

- Copy of the individual's Driver's License, Passport, Tribal Card, or State Identification (previously, only a copy of the Driver's License or State issued Identification for visitors to high-security facilities was collected)
- Alien Number, if applicable, and Phone Number

From SLTT emergency managers:

- Photograph retrieved from credentials (e.g., PIV card)

Uses of the Information

The previous PIA accurately describes how PACS uses information collected during the criminal history record check process. That process has been extended to include all SLTT individuals that will be granted unescorted access as described above.

FEMA may use the information within PACS to generate and maintain a "do not admit" list. This list will contain the name and photographic image of any individuals that DHS or FEMA deem to pose a safety or security risk to personnel or property.

Notice

Visitors are provided notice by their sponsors via a one-page handout prior to the collection of their PII. The handout includes a Privacy Notice containing 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.

The handout explains that visitors who are uncomfortable providing their PII to their sponsor may provide it to the FEMA OCSO Access Control office in person at least 30 minutes prior to their scheduled visit. Furthermore, the handout provides contact information for the Access Control office in the event the visitor would like to seek access or redress. Should the visitor decide to provide his or her PII in person at the Access Control office, he or she is again provided with a Privacy Notice on FEMA Form 649-0-1-2, Visitor Processing Information.

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

Data Retention by the project

The previous PIA accurately describes the data retention of PACS. The updates described in this document do not change the retention schedules or procedures.

Privacy Risk: There is a privacy risk that FEMA will retain the PII from the public for longer than is necessary to authorize access to a FEMA facility.

Mitigation: This risk is mitigated. FEMA retrieves the existing record of return visitors by their full legal name and automatically disables credentials from all personnel who do not access the facility within a year. Once the credentials are disabled, FEMA uses the NARA-approved retention schedules to retain and eventually dispose of the data. Records retained relating to access to areas designated by the Interagency Security Committee (ISC) as Facility Security Level V will be destroyed when 5 years old in accordance with NARA General Records Schedule (GRS) 5.6,

Item 110 and DAA-GRS-2017-0006-0014. Records retained relating to access to areas designated by the ISC as Facility Security Levels I-IV will be destroyed when 2 years old in accordance with NARA GRS 5.6, Item 111 and DAA-GRS-2017-0006-0015.

Information Sharing

Visitor management information to include members of the public is shared with the FBI for the purpose of screening 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.

Redress

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, whether due to non-admittance from a presence on the "do not admit" list or other visitor management issue.

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.

Privacy Risk: There is a privacy risk that an individual will not have the opportunity to contest a determination by PACS to not allow them to enter a FEMA facility.

Mitigation: This risk is mitigated. FEMA provides all visitors 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, this PIA provides notice that FEMA uses information from the FBI, Terrorist Screening Database (TDSB), and BOLOs from other agencies to create a "do not admit" list. Visitors may need to reach out to those agencies to correct any underlying information used by FEMA to create this list.

Auditing and Accountability

There are no changes to how PACS ensures the information is used in accordance with stated practices in this PIA update, nor have there been any changes related to privacy training since the original PIA publication.

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.

Responsible Official

William H. Holzerland
Senior Director for Information Management
Federal Emergency Management Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file with DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security