Privacy Impact Assessment
for the

DHS Physical Access Control Systems

DHS/ALL/PIA-039(a)

July 19, 2017

Contact Point
Richard McComb
Chief Security Officer
Department of Homeland Security
(202) 447-5010

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

Abstract

Department of Homeland Security (DHS) Physical Access Control Systems (PACS) support a range of functions related to managing physical access by individuals to DHS Headquarters (HQ) facilities. PACS are comprised of four major functions: visitor management, physical access control, intrusion detection, and video surveillance. PACS contain personally identifiable information (PII) from DHS employees, DHS contractors, and members of the public that access or attempt to access DHS HQ facilities. This Privacy Impact Assessment (PIA) Update addresses the two instances of PACS currently in operation within DHS HQ: the Headquarters Physical Access Control System (HQ PACS) and the St. Elizabeths Physical Access Control Systems (St. Es PACS). DHS is updating and replacing the previous PACS PIA, published on June 9, 2011, to broaden its scope beyond HQ PACS to also cover St. Es PACS. DHS will update this PIA further as more PACS are added to DHS HQ's physical security architecture. DHS will also publish a separate PIA for any PACS that differ substantially or that raise distinct privacy risks from those covered by this PIA Update.

Overview

Physical Access Control Systems (PACS) support the Department of Homeland Security (DHS) Office of the Chief Security Officer (OCSO) and the DHS Federal Protective Service (FPS) with facility access and intrusion detection at DHS Headquarters (HQ) facilities. PACS are comprised of a suite of applications that operate electronic security boundaries and alarms at each DHS facility. The boundaries and alarms are designed to prevent and deter individuals from reaching DHS personnel and assets to which they could pose a security risk. OCSO and FPS operate and maintain PACS as part of their larger mission to implement security policies, programs, and standards to protect and safeguard DHS personnel, property, facilities, and information.

Two PACS currently operate within DHS HQ and are covered by this Privacy Impact Assessment (PIA): Headquarters Physical Access Control System (HQ PACS) and St. Elizabeths Physical Access Control Systems (St. Es PACS):

HQ PACS

HQ PACS is a single system that supports physical security operations at DHS's Nebraska Avenue Complex (NAC) and 24 smaller DHS HQ facilities. OCSO uses the system to support its visitor management functions at the NAC, as well as its physical access control, intrusion detection, and video surveillance functions at all 25 DHS HQ facilities. HQ PACS also serves as a repository for all employee and visitor personally identifiable information (PII) required for authorizing and monitoring physical access at the NAC.

Users and Administrators

HQ 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. This form elicits the following PII:

- Full name (first, middle initial, and last);
- Phone number;
- Email address; and
- Employment position.

The user access request form includes a Privacy Notice listing the authorities DHS 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 the system 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, as described below.

St. Es PACS

St. Es PACS consists of three separate but partially integrated systems that support physical security operations at the St. Elizabeths campus in Southeast Washington, D.C. (St. Es). FPS authorizes and controls physical access at St. Es using individual authentication via card readers and accounting of card transactions. FPS also uses area intrusion detection and alerting mechanisms to conduct its physical boundary protection activities. FPS conducts both of these activities on a single St. Es PACS system dedicated to its physical access control and intrusion detection functions. A separate St. Es PACS system manages FPS's visitor management function and a third manages its video surveillance function.

Users and Administrators

St. Es PACS users and administrators are required to log in to a single system to execute FPS's physical access control and intrusion detection functions. Login to this system requires insertion of the employee's personal identity verification (PIV) card, a process already covered under a separate PIA.[1] In addition to logging in with their PIV cards, administrators of this system must enter a unique password as two-factor authentication security before exercising their administrator privileges. All PII required for setting up an account in the St. Es PACS physical access control and intrusion detection system is also taken directly from the user's or

[1] *See* DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System (PIV/IDMS), *available at* https://www.dhs.gov/privacy.

administrator's PIV card.

A separate system operates the St. Es PACS visitor management function. To log in to this system, both users and administrators must use their PIV cards and a unique personal identification number (PIN). FPS requires the PIN as an extra layer of security for its visitor management system because that system allows searches by Social Security number (SSN).

PACS Functions

PACS support 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.[2] This PIA Update covers collection and handling of PII for the other three functions.

1. Visitor Management (NAC and St. Es only):

DHS HQ's visitor management function authorizes and records entry and exit of visitors requiring temporary access to the NAC and St. Es. The visitor management function at the 24 other HQ PACS facilities are managed by non-DHS facility management personnel and thus are not covered by this PIA.

Visitor management at the NAC and St. Es is governed by DHS Instruction Manual 121-01-011-01, *Visitor Management for DHS Headquarters and DHS Component Headquarters Facilities.*[3] Per this guidance, OCSO distinguishes between four categories of visitors for purposes of screening:

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

The type of PII collected and the handling of that PII depends upon which of these categories a prospective visitor falls.

[2] DHS/ALL/PIA-042 Closed Circuit Television (CCTV) (July 18, 2012), *available at* https://www.dhs.gov/privacy.
[3] This instruction manual establishes procedures and program responsibilities to ensure a consistent level of visitor access control within DHS HQ as well as visitor management guidance and requirements for protecting DHS personnel and resources.

Current DHS Employees

Current DHS employees, both federal employees and contractors, in possession of a valid DHS-issued PIV card, are not subject to visitor screening to access the NAC and St. Es. DHS HQ employees visiting the NAC automatically have access rights to the facility coded onto their PIV cards. DHS employees visiting secure areas of St. Es must have their PIV cards coded for access by FPS personnel prior to entry. All collection and handling of PII associated with acquiring and maintaining DHS PIV cards is already covered under a separate PIA.[4]

Non-DHS U.S. Government Employees

U.S. Government personnel employed at federal agencies other than DHS are also exempted from visitor screening requirements at the NAC and St. Es unless specific direction is given by OCSO or FPS leadership. To access any DHS HQ facility, visitors falling under this category must present a valid employee identification card issued by their employing agency and an on-site DHS-employed sponsor must confirm the visit. The visitor's first and last name, agency of employment, and armed status[5] is 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.

Non-Federal Employees (U.S. Citizens)

U.S. citizens not employed by the U.S. Government who intend to visit the NAC or St. Es are subject to a background check using the National Crime Information Center (NCIC) system. NCIC is a computerized database that provides ready access to law enforcement agencies for making inquiries about an individual's criminal history. [6] The information generated from NCIC forms the basis for OCSO and FPS personnel to determine whether to grant access to a prospective visitor. The U.S. Federal Bureau of Investigations (FBI) administers NCIC and therefore all PII entered into NCIC as part of the visitor management screening process is transmitted to that agency. The FBI protects all records in NCIC from unauthorized access through various administrative, physical, and technical safeguards. These include restricting access to those with a "need-to-know" to perform their official duties and using locks, alarm devices, passwords, and encrypted data communications as appropriate.

OCSO and FPS collect PII from prospective visitors using DHS Form 11000-13, *Visitor Processing Information.* This form elicits the following PII required to screen U.S. citizens through NCIC:

[4] *See* DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System (PIV/IDMS), *available at* https://www.dhs.gov/privacy.
[5] Armed status refers to whether the visitor will be carrying a firearm onto the DHS facility.
[6] For more information about NCIC, *see* https://www.fbi.gov/services/cjis/ncic.

- Full name (first, middle, and last);
- SSN;
- Date of birth (DOB);
- Gender;
- Place of employment (name of company or local, state, federal, or foreign agency/post); and
- Armed status.

Form 11000-13 additionally requires the following PII from prospective visitors who intend to park vehicles at the NAC or St. Es: [7]

- Vehicle make;
- Vehicle model;
- Vehicle color;
- Vehicle tag number; and
- State of registration.

As with non-DHS U.S. Government employees, all prospective visitors falling under the non-federal U.S. citizen category must be sponsored by an on-site DHS employee who serves as OCSO's or FPS's primary point of contact during the screening process. Sponsors initiate the screening process for non-federal U.S. citizens by contacting the visitor management office to communicate their intention to host one or more visitors. The visitor management office responds by emailing the sponsor two one-page information handouts, one tailored to visitors and one tailored to the sponsors themselves.

The sponsor handout instructs sponsors to provide the visitor handout to each visitor they intend to host. Additionally, the sponsor handout explains that visitors can choose to share their PII with the sponsor so that the sponsor can complete Form 11000-13 on their behalf, or they can provide their PII directly to the visitor management office by arriving at least 30 minutes prior to their scheduled visit. The handout also instructs sponsors to send all 11000-13 forms they complete on behalf of visitors to the visitor management office via a password-protected email sent from a DHS account; and it further instructs sponsors to destroy all PII collected from the visitors as soon as the email is sent.[8] The sponsor handout explains too that the decision to grant or deny access to

[7] As with visitor management, parking management at DHS HQ facilities other than the NAC and St. Es are managed by non-DHS entities.
[8] The sponsor handout instructs sponsors to permanently delete any PII collected or recorded electronically and to shred any PII collected or recorded in hardcopy.

a visitor may not occur until shortly before the scheduled visit if the visitor chooses to provide the PII directly to the visitor management office.

The visitor handout and the Form 11000-13 both contain a Privacy Notice that states the proper authorities for collecting the information requested; the purpose of the information collection; how DHS will share information outside of the Department; 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 DHS HQ facilities. Like the sponsor handout, the visitor handout explains that visitors who are uncomfortable providing their PII to their sponsor may provide it directly to the visitor management office by arriving at least 30 minutes prior to their scheduled visit. The visitor handout further explains that emailing PII to the sponsor from anything other than a password-protected DHS account is not a secure practice and could result in a data breach. The handout provides contact information for the visitor management office as well in the event the visitor would like to seek access to his or her PII or redress for inaccurate PII.

OCSO and FPS use the information provided on Form 11000-13 to run a background check through NCIC to verify there are no outstanding warrants or criminal activities indicating a risk to the Department.[9] OCSO or FPS 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 the denial, he or she may do so by contacting the visitor management office using contact information listed on the one-page instruction sheet provided to the visitor by the sponsor.

OCSO and FPS generally require email submission of a separate Form 11000-13 for each visit to the NAC or St. Es. However, if the prospective visitor is reluctant to submit PII that was already provided for prior visits, he or she can contact the visitor management office to request that his or her record be retrieved using the last four digits of his or her SSN.

PACS visitor records contain the following information for U.S. Citizens:

- Full name (first, middle, and last);
- SSN (if issued);
- Date of birth (DOB);
- Gender;

[9] The FBI provides OCSO and FPS personnel with NCIC user accounts after appropriate training and certification to remove any risk that PII could be intercepted during transmission through a system-to-system interface.

- Status entry specifying visitor as non-federal employee U.S. citizen; and
- Date or date range of approved visit.

Visitor records are maintained for a period of five years from the date of the most recent visit, after which they are destroyed and cannot be recovered.

Foreign National Visitors

Foreign nationals who intend to visit the NAC or St. Es are also subject to the NCIC screening process. For foreign national visitors, Form 11000-13 elicits the following PII:

- Full name (first, middle, and last);
- SSN (if issued);
- Passport/Visa/Diplomatic ID
- Date of birth (DOB);
- Gender;
- Place of employment (name of company or local, state, federal, or foreign agency/post); and
- Armed status.

As with non-DHS U.S. Government employees and non-federal U.S. citizens, foreign nationals must be sponsored by an on-site DHS employee. Again, the sponsor ensures Form 11000-13 is completed and emailed to the appropriate visitor management office unless the prospective visitor is reluctant to share PII with the sponsor, in which case the visitor may provide it directly by arriving at the visitor management office at least 30 minutes prior to his or her scheduled visit. Visitor management personnel then follow the same policies and procedures described above for non-federal U.S. Citizens.

PACS visitor records contain the following information for foreign nationals:

- Full name (first, middle, and last);
- SSN (if issued);
- Passport/Visa/Diplomatic ID (if held)
- Date of birth (DOB);
- Gender;
- Place of employment (name of company or local, state, federal or foreign agency/post);
- Armed status;

- Country of citizenship; and
- Date or date range of approved visit.

As with all other categories of visitors, records for foreign nationals are available to OCSO and FPS personnel for up to five years after the visitor's most recent entry through a security boundary at the NAC or St. Es.

OCSO and FPS also use the Foreign Access Management System (FAMS) to screen all prospective visitors to DHS HQ 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 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 already covered under a separate PIA.[10]

2. Physical Access Control

DHS HQ's physical access control function regulates access to DHS HQ facilities. Most facilities control access through security guards or smart card readers. The smart card readers translate a unique code on an employee's PIV card or other approved credential to verify authorization to access a given space. OCSO and FPS 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.[11]

The only PII collected as part of the physical access control function other than that collected by card readers or recorded during PIV card issuance is from PACS users and administrators when setting up their system accounts, as discussed below.

3. Intrusion Detection

DHS HQ's intrusion detection function allows OCSO and FPS to identify and monitor the unauthorized intrusion of persons or devices into secure spaces at all DHS HQ facilities. It generally consists of sensors, lights, and other mechanisms used by OCSO and FPS to ascertain 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

[10] *See* DHS/ALL/PIA-048(a) Foreign Access Management System (FAMS), *available at* https://www.dhs.gov/privacy.
[11] *For information regarding how personal identifiers are stored and made retrievable on DHS PIV Cards, see* DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System (PIV/IDMS), *available at* https://www.dhs.gov/privacy.

power failures. The only PII collected as part of the intrusion detection function is from PACS users and administrators when setting up their system accounts, as discussed below.

4. Video Surveillance

DHS HQ's video surveillance function is covered in its entirety by a separate PIA.[12]

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 to protect the buildings, grounds, and property owned, occupied, or secured by the Federal Government, and the persons on the property. Per this statutory authority, The Department issued *DHS Directive 121-01*, *Office of the Chief Security Officer,* which delegates to the DHS Chief Security Officer the authorities and responsibilities for the performance of security functions within the Department. DHS regulations issued pursuant to this delegation and directly relevant to DHS HQ programs supported by PACS include:

- DHS Instruction 121-01-002, *Issuance and Control of DHS Badges* – establishes DHS procedures regarding the issuance, use, display, control, and accountability of DHS badges.
- DHS Instruction 121-01-008, *Issuance and Control of the Department of Homeland Security Credentials* – establishes DHS procedures regarding the issuance, use, display, control, and accountability of DHS credentials.
- DHS Instruction Manual 121-01-010-01, *Physical Security* – establishes physical security program guidance and requirements for protecting DHS real property and persons on the property. Specifically, the manual covers facility security risk assessments, application of the risk management process in the identification and allocation of resources, development and use of facility security plans, and use of performance measures in assessing the effectiveness of physical security programs.
- DHS Instruction Manual 121-01-011-01, *Visitor Management for DHS Headquarters and DHS Component Headquarters Facilities* – establishes visitor management guidance and requirements for protecting DHS personnel and resources. Specifically, the manual covers management of visitor access into DHS HQ and DHS Component facilities according to visitor category, methods for identifying individuals, and by maintaining "Do Not Admit" lists.

[12] DHS/ALL/PIA-042 Closed Circuit Television (CCTV) (July 18, 2012), *available at* https://www.dhs.gov/privacy.

All PII entered or stored within PACS is provided voluntarily by prospective visitors to DHS HQ facilities or from PACS users and administrators.[13]

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 published in the *Federal Register* and available on the DHS Privacy Office website:[14]

- *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 DHS information technology and access to classified facilities, as well as visitor security and management.[15]
- *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 DHS.[16]
- *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 DHS.[17]
- *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.[18]

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

Yes. The Authority to Operate (ATO) for HQ PACS expired on September 29, 2016. A System Security Plan for HQ PACS was completed on March 27, 2017, as part of efforts to reaccredit the system. The HQ PACS Federal Information Security Management Act (FISMA) ID

[13] However, failure to provide the PII may result in no action taken on visitor requests or inability to log in to PACS.
[14] www.dhs.gov/privacy
[15] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).
[16] DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010).
[17] DHS/ALL-025 Law Enforcement Authority in Support of the Protection on Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, 75 FR 5614 (February 3, 2010).
[18] DHS/All-026 Personal Identity Verification Management System of Records, 74 FR 30301 (June 25, 2009).

is DHQ-03433-MAJ-03433.

The ATO for St Es PACS expired on July 16, 2016. A System Security Plan for St. Es PACS was completed on February 15, 2017, as part of efforts to reaccredit the system. The FISMA ID is DHQ-06725-GSS-06725.

Both systems will receive renewed ATOs upon 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) 18, *Security and Protective Services Records* and by GRS 3.2, *Information System Security Records*.

DHS retains records of PII from visitors in accordance with GRS 18, item 17, *Visitor Control Files*. Per this guidance, PII is destroyed five years after most recent entry or five years after the date it was submitted, as appropriate.

DHS 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.

OCSO is working with DHS's PRA Program Management Office to address clearance requirements.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

PACS use PII collected from individuals requiring access to DHS HQ facilities and secure spaces to confirm their identity and determine their access eligibility. PII is entered into NAC PACS and St. Es PACS by OCSO and FPS visitor management personnel, respectively.

As discussed in a separate PIA covering DHS's PIV card program,[19] the following data

[19] DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System (PIV/IDMS) (October 20, 2015), *available at* https://www.dhs.gov/publication/personal-identity-verification.

elements are collected from DHS employee PIV cards and entered into PACS at time of PIV card issuance:

- Name (first, middle, last);
- Date of birth (DOB);
- Agency (e.g., DHS);
- Organization affiliation (e.g., FEMA);
- Employee affiliation (employee or contractor);
- Facial image;[20]
- Security clearance type;
- Email contact;
- User principal name (Microsoft account Name);
- PIV Card Identifiers (FASC-N string/GUID string);[21]
- Electronic Data Interchange Person Identifier (EDIPI); and
- PKI Public Key Certificate Data.

The following information is collected from non-DHS federal employee visitors upon entry into the NAC or St. Es:

- Name (first, middle, last);
- Agency of employment;
- Armed status;
- Vehicle information (if applicable);
    - Vehicle make;
    - Vehicle model;
    - Vehicle color;
    - Vehicle tag number; and

[20] Although DHS collects facial images of its employees during issuance of PIV cards, it does not currently employ facial recognition technology. DHS will further update this PIA if any PACS adopts facial recognition technology.
[21] Federal Agency Smart Credential Numbers (FASC-N) and Globally Unique Identifiers (GUID) consist of a series of numbers that are programmed onto PIV cards and that serve as unique identifiers for those cards. PACS card readers collect FASC-N from DHS and other federally-issued PIV cards, whereas GUID are collected from any readable PIV cards issued by non-federal entities.

- State where vehicle is registered.

The following information is collected from U.S. citizens not employed by the U.S. Government, and it is shared with the FBI via NCIC to verify that they are suitable for access as visitors:

- Full name (first, middle, and last);
- SSN;
- DOB;
- Employer name;
- Vehicle information (if applicable);
  - Vehicle make;
  - Vehicle model;
  - Vehicle color;
  - Vehicle tag number; and
  - State where vehicle registered.

The following information about U.S. citizens is entered into PACS when their visitor records are created:

- Full name (first, middle, and last);
- SSN (if issued);
- DOB;
- Gender;
- Status as non-federal employee U.S. citizen; and
- Date or date range of approved visit.

The following information is collected from foreign nationals, and it is shared with the FBI via NCIC to verify that they are suitable for access as visitors:

- Full name (first, middle, and last);
- Social Security number (if issued);
- Passport/Visa/Diplomatic ID (if held)
- DOB;

- Gender;
- Place of employment; and
- Armed status.

The following information about foreign nationals is entered into PACS when their visitor records are created:

- Full name (first, middle, and last);
- SSN (if issued);
- Passport/Visa/Diplomatic ID (if held)
- DOB;
- Gender;
- Place of employment (name of company or local, state, federal, or foreign agency/post); and
- Armed status;
- Country of citizenship; and
- Date or date range of approved visit.

The following information is collected by card readers from DHS employees who cross physical security boundaries at the NAC and St. Es, and it is stored in an entry log maintained in PACS:

- Full name (first, middle, and last);
- PIV card number; and
- Date, time, and location of entry

The type of PII collected from PACS users and administrators depends on which system they are using. HQ PACS users and administrators provide their first and last names, middle initial, phone number, email address, and position title when their system accounts are established. A unique username and a password is then required to log in to that system. St Es PACS users log in to FPS's physical access control and intrusion detection system using only their PIV cards, while administrators of this system log in using both a PIV card and a unique password. Users of the St Es PACS visitor management system log in using a PIV card and a PIN.

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

For visitor management, the source of PACS information is DHS Form 11000-13, *Visitor Processing Information* and the results of the NCIC screening process.

For PACS operation, the source of information is provided by users or administrators when setting up their system accounts and during login.

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 do not use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Generally, an on-site DHS-employed sponsor collects PII directly from visitors and completes and emails Form 11000-13 containing all visitor PII required for NCIC screening and visitor processing. However, if visitors are reluctant to share their PII with the sponsor, they are notified via a one-page handout that they may arrive at the visitor management office at least 30 minutes prior to their scheduled visit to provide the PII directly. OCSO and FPS do not investigate sponsors or visitors to determine if the information they provide is accurate. However, if the sponsor or visitor provides inaccurate information, any records stored in NCIC related to that information will refer to some individual other than the visitor. [22] In these cases, if the visitor is informed of a denial of access, the visitor may contact the visitor management office at the phone number or email listed on the visitor handout to validate whether the information submitted was correct. If it was not, the visitor will be provided an opportunity to provide the correct information.

PII required for operating PACS is provided by users and administrators when setting up their system accounts. Users and administrators may contact the system service desk to modify their PII or to reset their unique passwords or PINs.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

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

Mitigation: OCSO and FPS mitigate this risk by limiting access to the visitor management

[22] NCIC only stores information about individuals with criminal records. Therefore, the system will only generate results if the inaccurate PII that is entered into NCIC relates to an individual with a documented history of criminal activity.

module within PACS to only those with job duties that involve visitor management responsibilities. Similarly, PII from users and administrators is only available to a limited number of other system administrators.

Privacy Risk: There is a risk that visitor management personnel will collect more PII than is needed to conduct required visitor management functions.

Mitigation: PII collected via Form 11000-13 is the minimum required to screen prospective visitors through NCIC and to create visitor records that make the visitors easily identifiable and locatable in the event of a security incident. Although these forms are generally collected for each visit to the NAC or St. Es, visitors may inform the visitor management office that they have previously provided the requested PII and request that their PII be retrieved from the existing record using the last four digits of their SSN.

Privacy Risk: There is a risk that visitor management personnel from different DHS HQ facilities will duplicate collection of PII.

Mitigation: This risk is not currently mitigated. Visitor management personnel at the NAC and St. Es report to different DHS organizations and currently operate on different visitor management systems.[23] An effort is currently underway to partially integrate the two visitor management systems so that records can be shared between the NAC and St. Es.

Privacy Risk: There is a risk that DHS will make a decision to deny access to a prospective visitor based on the submission of inaccurate information.

Mitigation: This risk cannot be fully mitigated. Access to DHS facilities is a privilege, and if the visitor is denied access based on submission of PII pertaining to someone else that has a criminal record, that information will have been 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 visitor management office at contact information provided on the visitor handout. In these cases, if OCSO or FPS provide a reason for the denial that does not reflect the individual's actual history, OCSO or FPS will validate that the PII previously provided for the NCIC screening was accurate. If it was not, OCSO or FPS will run the background check again using the correct PII assuming the visitor would still like access to the NAC or St. Es.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

PACS use PII to authenticate the identity of federal employees, DHS contractor employees,

[23] The visitor management function at the NAC is managed by OCSO and the visitor management function at St. Es is managed by FPS.

and visitors who have entry authorization. OCSO and FPS use this information to verify the identity of individuals and, in the event of an emergency, to contact individuals. PACS also contain information on visitor vehicles so they can be identified in the event of a parking-related incident.

Additionally, DHS collects PII in the form of first and last names, middle initials, phone numbers, email addresses, and position description from PACS users and administrators when setting up their system accounts.

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 do 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?

Yes. In addition to OCSO and FPS, the Office of the Chief Information Officer (OCIO) provides IT system support, routine maintenance, and information security services.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk associated with individuals gaining 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 DHS 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. 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 formed the basis for both PACS systems obtaining a system security certification in accordance with the Office of Management and Budget (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 DHS domain account and requires that the user be logged in to a DHS Intranet-accessible computer. Furthermore, user accounts are individually approved by the Chief of OCSO's Physical

Security Services Branch for HQ PACS and by FPS's Risk Management Branch Chief for St. Es PACS. 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.[24]

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

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 DHS HQ facilities. Additionally, the handout explains that visitors who are uncomfortable providing their PII to their sponsor may provide it to the visitor's management office in person at least 30 minutes prior to their scheduled visit. Furthermore, the handout provides contact information for the visitor management 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 visitor management office, he or she is again provided with a Privacy Notice on Form 11000-13, *Visitor Processing Information*. Additionally, DHS will continue to provide notice to the public through this PIA and through the SORNs listed in 1.2 of this PIA Update.

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 DHS will use this information to determine if access may be granted. Failure to provide PII may result in a determination to deny access to DHS HQ facilities since it will be impossible to conduct the required background check through NCIC. This information is provided to visitors by their sponsors via a one page handout and is also included in the Privacy Notice contained on Form 11000-13, *Visitor Processing Information.*

HQ PACS users and administrators also provide PII when their system accounts are established. Again, failure to do so may result in no action being taken on establishing their accounts.

[24] Currently, the audit log is only reviewed in the course of ad hoc investigations or on suspicion of wrongdoing.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals providing information to DHS do not have notice that their PII will be stored in PACS.

Mitigation: This risk is partially mitigated by publication of this PIA Update, which serves as an additional notice as well as a further explanation regarding the way DHS receives and manages PACS data. Notice is also provided through the DHS Facility and Perimeter Access Control and Visitor Management SORN.[25]

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

DHS retains records of PII collected from visitors, as well as information collected about visitor automobiles parked at DHS facilities, in accordance with GRS 18, item 17, *Visitor Control Files*. Per this guidance, PII is destroyed 5 years after the visitor's most recent entry into a DHS HQ facility or five years after the date the visitor submitted it, as appropriate. This information is collected in case the visitor or his or her vehicle needs to be located due to a security incident that occurs while the visitor is on the premises.

DHS retains records of PII collected from users and administrators when setting up their PACS accounts 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. This information is collected in case a user or administrator needs to be identified or located due to an IT security incident involving PACS.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the completed and emailed DHS Form 11000-13, *Visitor Processing Information,* will be retained on an individual computer longer than necessary to accomplish a legitimate purpose or inconsistently with the records schedule.

Mitigation: This risk is partially mitigated. The visitor management office notifies sponsors via the sponsor handout that they are required to destroy all visitor PII immediately upon providing it to the visitor management office. DHS also reminds PACS users through policy and training that they must follow the applicable retention schedules for visitor control files regardless of where they are stored.

[25] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (Feb 3, 2010).

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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

Yes. Visitor management information 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 the NAC and St. Es with NCIC user accounts to remove any risk that data could be intercepted during transmission through a system-to-system interface. OCSO and FPS 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 and FPS only share PACS-related information outside of DHS in accordance with a routine use defined in the Facility and Perimeter Access Control and Visitor Management SORN noted in 1.2.[26] Specifically, OCSO and FPS visitor management personnel share PII with the FBI in order to conduct a criminal background check on prospective visitors to the NAC and St. Es to determine whether they could pose a security risk to DHS personnel and assets. Routine use H of the Facility and Perimeter Access Control and Visitor Management SORN 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 and FPS'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 and FPS during the course of screening prospective visitors through NCIC in accordance routine uses defined in the FBI's NCIC SORN.[27]

[26] DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records.
[27] *See* 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 provide the means to record all disclosures of PII to the FBI 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. PACS visitor records serve in lieu of DHS-191, release of Information Subject to the Privacy Act, because record entries of NCIC adjudication already document the release of information to other agencies.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that individuals authorized to access PACS will conduct unauthorized activities such as extracting and sharing information with unauthorized recipients.

Mitigation: OCSO and FPS have 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 DHS domain account and requires that the user be logged in to a DHS Intranet accessible computer. These user accounts are individually approved by OCSO or FPS. Furthermore, all users complete DHS 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.

Privacy Risk: There is a risk that PII on Form 11000-13 will be intercepted in transit when it is emailed from the sponsor to the visitor management office.

Mitigation: OCSO and FPS will not accept PII via email that is not password-protected and sent from a DHS account. This direction to sponsors is included on the sponsor handout.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress, which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Visitors who are U.S. citizens, lawful permanent residents, or covered by the Judicial

Redress Act, [28] may submit a Privacy Act (PA) request to gain access to their PII. Additionally, all visitors, regardless of citizenship status, may submit a Freedom of Information Act (FOIA) request for access to their PII. Furthermore, all visitors may contact the OCSO Customer Service Center at 202-447-5010 or by email at officeofsecurity@hq.dhs.gov; or they may contact the FPS Customer Service Center at 202-372-8990 or by email at CHQ-Visitor@hq.dhs.gov; for information about any PII about them that is maintained in PACS. This information is communicated to visitors in a one-page instruction sheet provided by their sponsors prior to PII collection.

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,[29] may submit a Privacy Act (PA) request to correct their PII. Once information is submitted to OCSO or FPS for entry into PACS, the individual who submitted it may contact OCSO or FPS directly. All visitors may also contact the OCSO Customer Service Center at 202-447-5010 or by email at officeofsecurity@hq.dhs.gov; or they may contact the FPS Customer Service Center at 202-372-8990 or by email at CHQ-Visitor@hq.dhs.gov; for information about any PII about them that is maintained in PACS. This information is communicated to visitors in a one-page instruction sheet provided by their sponsors prior to PII collection.

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

If an individual would like to make changes to enhance the accuracy of information in PACS, he or she may contact OCSO through its Customer Service Center at 202-447-5010 or by email at officeofsecurity@hq.dhs.gov; or he or she may contact the FPS Customer Service Center at 202-372-8990 or by email at CHQ-Visitor@hq.dhs.gov. PACS notifies individuals of the procedures for correcting their information in a one-page instruction sheet distributed to them by their sponsors prior to PII collection and through this PIA Update and the associated SORNs listed in 1.2.

7.4 Privacy Impact Analysis: Related to Redress

There is a low privacy risk that visitor management personnel will inappropriately divulge information related to visitors that are denied access to DHS HQ facilities seeking redress. PACS provides individuals multiple opportunities during and after the completion of the process to correct information by contacting OCSO or FPS using contact information provided on the visitor

[28] 5 U.S.C. § 552a note.
[29] Id.

handout. To mitigate risks associated with redress, OCSO and FPS personnel are trained not to divulge to anyone without an official need-to-know the fact of a denied visitor's supplementation, the contents of the supplementary information, or the fact that a denial prompted the visitor's right of redress.

Section 8.0 Auditing and Accountability

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

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

PACS are 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 and FPS visitor management personnel only accept transmission of PII via email when it is password-protected and sent from a DHS account. Furthermore, visitors are notified in a one-page visitor handout that emailing PII to sponsors from other than a password-protected DHS account is not a secure practice and could result in a data breach.

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 DHS employees and assigned contractor staff receive 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 or FPS leadership. All users must complete computer security training and must be properly vetted for access to DHS 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. [30]

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 establish 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.

Responsible Officials

Johnathan Swinton
Acting Branch Chief, Physical Security Services
Office of the Chief Security Officer
Department of Homeland Security

Virgil "Ted" Veyera
Branch Chief, Risk Management Branch
Federal Protective Service
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

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

[30] The different roles correspond to the four functions discussed in this PIA: visitor management, physical access control, intrusion detection, and video surveillance. For example, personnel whose duties are limited to visitor management would not have access to data or processes within PACS related to the other three functions.