Privacy Impact Assessment
for the

Physical Access Control System

DHS/ALL – 039

June 9, 2011

Contact Point
David S. Coven
Chief, Access Control Branch
Office of the Chief Security Officer
Department of Homeland Security
(202) 282-8742

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS), Office of the Chief Security Officer (OCSO), Physical Access Control Division (PHYSD) operates the Physical Access Control System (PACS). PACS is a security technology integration application suite used to control and manage physical access devices, intrusion detection, and video surveillance at DHS Headquarters (HQ) facilities in the National Capital Region (NCR), primarily the Nebraska Avenue Complex (NAC). This PIA will focus exclusively on the physical access control and intrusion detection functions within PACS. The video surveillance function within PACS is covered by a separate PIA and can be found at www.dhs.gov/privacy. PACS provides advanced access control, alarm monitoring, digital video,[1] intrusion detection, and employee, visitor, and parking management.

PACS allows authorized security personnel to simultaneously manage and monitor multiple entry points from a single, centralized location. The OCSO has conducted this Privacy Impact Assessment (PIA) to analyze the personally identifiable information (PII) that PACS collects, uses, and maintains. To the extent that other Departmental components use a system(s) that operates in the same way as PACS and will follow the rules outlined in this PIA, that system will be covered by this PIA and listed as part of an update to this PIA appendix.

Overview

PACS operates access control and intrusion detection functions at DHS HQ facilities in the NCR, primarily the NAC, and is comprised of a suite of applications which serve as a mechanism for the management of electronic access points and alarms. PACS produces automated transactional reports, documenting what activity took place, where and when.

PACS applications used at DHS HQ facilities in the NCR, primarily the NAC, are divided into four areas: A) identification for access; B) visitor management; C) parking permit management; D) alarm monitoring and intrusion detection. All four applications and processes operate independently at the direction of the PACS Administrator.

A) Identification – PACS requires an individual's PII so it can authorize physical access to DHS facilities. PACS sensors read the information on an individual's Personal Identity Verification (PIV)[2] card to verify if the individual is authorized access.

B) Visitor Management – Visitors and construction and service contractors[3] who have not been issued a PIV card must be identified before being granted access. This is accomplished by having the individual provide the information requested on DHS Form 11000-13 "Visitor Process Information." OCSO personnel enter the information on the form into the PACS visitor management function. This information is then used to conduct a search of the National Crime Information Center (NCIC) to determine if there are any criminal records or outstanding arrest warrants for the individual. The results of the NCIC check are entered into PACS. If there is no disqualifying information, such as an

[1] See NAC CCTV PIA at www.dhs.gov/privacy.
[2] See PIVMS PIA and SORN at www.dhs.gov/privacy.
[3] The facilities for which visitor information is maintained in PACS are: The Nebraska Avenue Complex, Plumb Island, the S&T office in Arlington, VA, and the Saint Elizabeths complex.

outstanding arrest warrant, the visitor is cleared for access. Access requests by foreign visitors[4] (non-U.S. citizens and non-Legal Permanent Residents) are processed through the DHS Foreign National Visitor Management System (FNVMS).[5]

C) Parking Permit Management – The Office of the Chief Administrative Officer (OCAO) uses PACS to issue and track parking permits for the NAC. OCAO personnel access PACS to determine if an individual is eligible to receive a parking permit. Once determined to be eligible, the individual must submit General Services Administration (GSA) Parking Application, Form 2941. Upon issuance of the parking permit, OCAO personnel enter into PACS the name and e-mail address of the permit holder, the permit number and type, issue date, and expiration date.

D) Alarm Monitoring and Intrusion Detection – The PACS alarm monitoring application allows OCSO personnel to monitor the Intrusion Detection System (IDS). A record is created in PACS of all IDS alarm activations or other issues, such as communication and power failures for example. The IDS in PACS consists of sensors, lights, and other mechanisms through which OCSO can detect the unauthorized intrusion of persons or devices. The only PII collected by the PACS IDS suite is the first and last name of the individual authorized to turn the alarm system on and off and the corresponding PIN number which the individual inputs into the alarm keypad to activate or deactivate the alarm.

To the extent that other Departmental components use a system(s) that operates in the same way as PACS and will follow the rules outlined in this PIA, that system will be covered by this PIA and listed as part of an update to this PIA appendix.

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?

The Chief Security Officer is responsible for developing and implementing security policies, programs, and standards to protect and safeguard the Department's personnel, property, facilities, and information. To do this, the OCSO and PHYSD have established access control policies designed to limit access to authorized individuals. In order to know if an individual is authorized access, the identity of the individual must be established. OCSO PHYSD does this by obtaining PII related to the individual and then conducting appropriate checks of records maintained by DHS and other U.S. government agencies. Authorities associated with protecting federal property and information include:

- 5 U.S.C. § 301, "Government Organization and Employees;"
- Executive Order 12977, "Interagency Security Committee;"

[4] The following information on foreign visitors to the NAC is maintained in PACS: Name, date of birth, and passport or visa number.
[5] See FNVMS PIA at www.dhs.gov/privacy.

- Executive Order 13286, "Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security;"
- Presidential Decision Directive 12, "Security Awareness and Reporting of Foreign Contacts;"
- Homeland Security Presidential Directive-7, "Critical Infrastructure Identification, Prioritization and Protection;"
- National Infrastructure Protection Plan, "Government Facilities Sector, Sector-Specific Plan;"
- Interagency Security Committee Standard, "Physical Security Criteria for Federal Facilities," April 12, 2010; and
- Federal Property Regulations, July 2002.

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

The following DHS SORNs apply:

- DHS/ALL – 024 Facility Access Control and Visitor Management, February 3, 2010, 75 FR 5609.
- DHS/ALL – 023 Personnel Security Management Systems of Records, February 23, 2010, 75 FR 8088.
- DHS/ALL – 026 Personal Identity Verification Management System, June 25, 2009, 74 FR 30301.

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 November 17, 2009, and a security certification authorizing the Authority to Operate (ATO) was granted on March 22, 2010, by the DHS Information Systems Security Manager Certifying Official. The ATO will expire on March 21, 2013. The PACS Federal Information Security Management Act (FISMA) ID is DHQ-03433-MAJ-03433.

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

DHS adheres to NARA General Records Schedule (GRS) 18, Security and Protective Services Records, items 20 through 25 for the retention schedule of personnel security clearance records.

In consultation with the DHS Records Officer, access control paper records are destroyed within 60 days of being scanned into the Access Control Program Office secured drive. The DHS visitor management paper records are destroyed not later than 60 days after the information is entered into PACS. Currently, parking program paper

records are stored under lock and key in NAC Building 2. During the transition to the new parking program, new records are stored under lock and key in NAC Building 7. Only designated parking or facilities personnel have access to documents in either location. Within 60 days after the information is entered into the parking portion of PACS, the paper records are destroyed. Alarm monitoring and intrusion detection incident longs are maintained for two years after final entry and then destroyed.

1.5 If the information is covered by the Paperwork Reduction 0.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 the 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 uses PII collected from individuals requiring access to confirm the identity of the individual and determine their access eligibility. PII is entered into PACS by OCSO personnel assigned to PHYSD or OCAO.

The following data is collected and entered into PACS to identify individuals authorized to access DHS HQ facilities in the NCR, primarily the NAC:

- Name;
- Social Security Number;
- Date of Birth;
- Gender;
- Home Address;
- Employee Type (e.g., Federal, Contractor, Detailee);
- Component;
- Home Agency or Company (if Detailee);
- Work Location;
- PIV Card – Number and Type; and
- PIV Card - Activation Date, Deactivation Date, and Pin Number.

The following information is collected for visitor management purposes and is used to verify the person entering the facility is suitable for access and does not have an outstanding arrest warrant or pose a threat to individuals:

U.S. Citizen Visitors

- Name;
- Social Security Number;
- Access Level (how frequently the visitor accesses the facility);
- Expiration of the Visit Authorization;
- Date of Birth;
- Gender;
- Visitor Type;
- Visitor's Home Agency or Company;
- Visit Type;
- DHS Point of Contact and Telephone Number;
- Office/Area Visited;
- Service Contractor Vehicle Information treated as separate visitor;
- If not service contract vehicle, vehicle information is listed in the visitor record:
  a. License number;
  b. Make of Vehicle;
  c. Model; and
  d. Color.
- Comments;
- Parking Pass Information categories;
- NCIC Completed Date; and
- Results of NCIC Check.

Foreign Visitors

- Name;
- Date of Birth;
- Country; and
- Passport or Visa Number.

The following information is collected by OCAO facilities management personnel and is used to issue parking permits. The information is also used by OCAO facilities management personnel to notify the individual in the event of an accident, emergency, or if their vehicle needs to be moved:

- Name;
- Vehicle Information (Make, Model, Color Year);
- Vehicle License Number and State of Registration;
- Parking Permit Number and Permit Issuance and Expiration Date;
- Permit Holder's PIV Card Type; and
- Permit Holder's e-mail address.

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

For facility access purposes, the sources of PACS information are the individual's PIV card and DHS Form 11000-14, Identification Access Card Control Request.

For visitor management purposes, the source of PACS information is DHS Form 11000-13, Visitor Processing Information and information provided by foreign national visitors.

The information source for NAC parking permits is General Services Administration (GSA) Form 2941.

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

PACS does not use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The information collected on DHS personnel and contractor employees is verified against information contained in the OCSO Integrated Security Management System (ISMS).[6] Information provided by visitors or parking permit applicants will not be confirmed unless a situation develops that would cause OCSO to question the accuracy of the information. Checks conducted on visitors are based upon the information provided by the visitor. DHS does not investigate the visitor to determine if the information provided by the visitor is valid.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk associated with the accuracy of data included in the PACS. Although most of the PII data is generated by the individual, it is possible that data associated with individuals with the same name or similar names could be inaccurately entered.

Mitigation: To address potential occurrences of data being inaccurately entered the following mitigation strategies are used: Electronic data collection tools are used to the greatest extent possible and SSN is used to increase accuracy of subject identification.

[6] See ISMS PIA at www.dhs.gov/privacy.

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 uses PII in order to authenticate the identity of federal employees, DHS contractor employees, and visitors who are authorized entry. OCSO uses this information to verify the identity of individuals and, in the event of an emergency, contact the individual. PACS also contains information on vehicles for which a permanent parking permit has been issued or a daily permit for a vehicle carrying a visitor to the NAC.

The IDS function within PACS monitors activity within sensitive or classified areas and records the name and pin number of the individual who activates or deactivates an alarm.

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.

PII in PACS is used to manage access control, physical access devices, and intrusion detection at facilities. There are no in-build data analysis functions to identify patterns or new areas of concern.

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

Only OCSO, OCAO, and the Office of the Chief Information Officer (OCIO) have assigned roles and responsibilities in PACS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk associated with the handling of PII. Privacy risks associated with the handling of PII occur when data is extracted from the system and the individual using the data improperly distributes or stores the data.

Privacy Risk: There is also a privacy risk associate with the system security concern of an "insider threat" where an individual authorized access to the system conducts unauthorized activities, such as attempting to access information for which they do not have permission.

Mitigation: To address both of these risks the following controls and mitigation strategies are in place:

Handling of PII

- Access to information is granted on a "need to know" basis;
- Access to PACS requires a DHS domain account and requires that the user be logged into a DHS Intranet accessible computer;
- PACS user accounts are individually approved by the Chief of the PHYSD;
- All users have received DHS computer security training and have been vetted and/or cleared for access to sensitive, and/or classified information;
- Access to PACS is role-based and users of the system have access to a limited subset of data based on the concept of least privilege/limited access; and
- Write capability, which is limited to a few roles, is tracked and audited.

System Security

- When information is stored as an attachment on the server, file access will be restricted by file permissions to prevent access by those without an appropriate requirement for access;
- All automated data processing equipment supporting the application environment is located in a DHS data center;
- Specific security roles have been defined and implemented within the application to control access to information;
- A system security certification was performed and obtained in accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources; and
- Network access to the application is made via a Secure Sockets Layer (SSL) connection to the ISMS environment.

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.

Individuals are provided notice at the time of collection by a Privacy Act Notice on the bottom of the information collection form. The Privacy Act Notice explains the reasons for collecting information, the consequences of failing to provide the requested information, and how the information is used. The collection, maintenance, and disclosure of information complies with the Privacy Act as noted in DHS/ALL – 023 Personnel Security Management, January 16, 2009, 74 FR 3084; DHS/ALL – 024 Facility and Perimeter Access Control and Visitor Management, January 16, 2009, 74 FR 3081; and DHS/ALL – 026 Personal Identity Verification Management System, September 25, 2009, 74 FR 30301.

Visitors to the NAC must agree with the Privacy Act Statement provided at the time the visitor is processed for access to the NAC.

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

Employees and contractor employees who opt not to provide information will not be granted access to DHS facilities since PACS will not have the ability to manage the electronic access points and alarms through which they must pass.

Visitors are advised that access control procedures require the submission of their PII. They are also advised that DHS will use this information to determine if access may be granted and that failure to furnish the requested information may delay or prevent their access.

4.3 Privacy Impact Analysis: Related to Notice

Information collected in association with the DHS PIV card, and used to manage access control within PACS, is completed in accordance with federal personnel security standards and requirements.

Visitors and foreign national visitors from whom data is collected may use a representative, (e.g., Executive Assistant or Embassy staff) to provide the data. Accordingly, there is a risk that the representative may not convey the Privacy Act Notice explaining why DHS is requesting the information and how the information will be used and stored. This PIA 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 DHS/ALL – 024 Facility and Perimeter Access Control and Visitor Management, January 16, 2009, 74 FR 3081.

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 personnel and security records relating to individuals are retained and disposed of in accordance with GRS 18, item 22a and 22c, as approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of the employee, whichever is first. The index to personnel security case files are destroyed with the related case.

Visitor records are retained in accordance with GRS 18, Item 17 and are destroyed five years after final entry or five years after the date of the document, as appropriate.

Where records are used as evidence in an investigation or in an administrative, litigation, or other proceeding, the records will be retained until final disposition of the investigation or proceeding.

5.2 Privacy Impact Analysis: Related to Retention

Risks associated with the retention and disposal of records collected in PACS are minimal. Risk is present when information for PACS is provided on paper form by the applicant. The risk is mitigated by security procedures in handling the data and destroying the files in accordance with the GRS.

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.

Information contained in PACS for access management purposes is not shared outside of DHS as part of the normal agency operations.

Visitor management information is shared outside PACS as part of normal operations for conducting record checks on the individual with other U.S. government agencies. The U.S. government agency to which the information is sent uses the information to search its records for information about the individual. Each agency maintains its records in accordance with its privacy policies. Some record checks are conducted with U.S. government agencies that maintain national security systems consistent with the requirements of Executive Order 12333, as amended, "United States Intelligence Activities."

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

Routine uses of records in PACS associated with visitors accessing DHS facilities are addressed in DHS/ALL – 023 Personnel Security Management, January 16, 2009, 74 FR 3084; DHS/ALL – 024 Facility and Perimeter Access Control and Visitor Management, January 16, 2009, 74 FR 3081; and DHS/ALL – 026 Personal Identity Verification Management System, September 25, 2009, 74 FR 30301.

6.3 Does the project place limitations on re-dissemination?

No limitations are placed on re-dissemination of information within DHS as long

as there is an official need to know.

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

PACS contains a field which maintains a record of the type of check conducted on the visitor as well as the agency with which it was conducted.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: As discussed in Section 3.4, there is the potential for an individual authorized to access the system to conduct unauthorized activities such as attempting to access information or extracting and sharing information for which they do not have permission.

Mitigation: To address this risk the following controls are in place:

- 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 and/or distribution of personnel security data to avoid accidental, inappropriate, or unauthorized use of the data;
- Access to information is granted on a "need to know" basis;
- Access to FNVMS requires a DHS domain account and requires that the user be logged into a DHS Intranet accessible computer;
- FNVMS user accounts are individually approved by OCSO and the Chief of ISID;
- All users have received DHS computer security training and have been vetted and/or cleared for access to privacy, sensitive, and/or classified information;
- Access to FNVMS is role-based and users of the system have access to a limited subset of data based on the concept of least privilege/limited access; and
- Write capability is limited to a few roles and is tracked and audited.

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?

Once data is submitted to OCSO for entry in PACS the individual who submitted the information must contact OCSO directly or submit a Privacy Act (PA) or Freedom of Information Act (FOIA) request to gain access to their PII and request that it be corrected. Individuals have the ability to address and provide updated information. OCSO may be contacted through its Customer Service Center at 202-447-5010 or by email at officeofsecurity@hq.dhs.gov.

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

OCSO will make changes to employee and contractor employee PACS records as long as the information is consistent with information ISMS. Changes will be made to visitor records if the change requested can be verified.

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

Instructions are provided on the respective form for making changes or updates to data that may be necessary after original submission. If an individual needs to make changes to enhance the accuracy of the information, the individual may contact OCSO through its Customer Service Center at 202-447-5010 or by email at officeofsecurity@hq.dhs.gov.

7.4 Privacy Impact Analysis: Related to Redress

Information contained in PACS may be corrected by contacting OCSO through its Customer Service Center at 202-447-5010 or by email at officeofsecurity@hq.dhs.gov or through redress procedures afforded under the PA and FOIA.

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?

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 through use of access control lists. As such, PACS users may only input, update, and delete records or fields to which they are authorized to have access and a need-to-know, as prescribed by the application user manual and system administration procedures.

Additionally, access control software on PACS prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.

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, and have undergone necessary suitability investigations and/or received security

clearances for access to classified 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 the OCSO PHYSD, Access Control Branch Chief, and authorized by the Chief of the Systems Security Division. All users must have received DHS computer security training and have been vetted for access to DHS IT systems or for access to classified national security information. Furthermore, access to PACS is role-based and users of the system have access to a limited 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 (ISAs). DHS 4300A, Sensitive System Handbook, September 2008, establishes this requirement for 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 entity/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

David S. Coven
Branch Chief, Access Control Operations
Office of the Chief Security Officer
Department of Homeland Security
(202) 282-8742

Approval Signature

Final signed version on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security