Privacy Impact Assessment Update
for the

Personal Identity Verification

June 18, 2009

Contact Point
Cynthia Sjoberg
Program Director, HSPD-12
Office of Security
Department of Homeland Security
(202) 447-3202

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

Abstract

The Department of Homeland Security (DHS) is updating the Personal Identity Verification (PIV) Privacy Impact Assessment (PIA) issued on October 13, 2006, to reflect changes in Departmental requirements identified through increased collaboration with the components during implementation planning and to include bringing the components online. Additionally, this update discusses the use of the Integrated Security Management System (ISMS) and a more robust, second-generation Identity Management System (IDMS), which replaces the PIV IDMS discussed in the previous PIA.

Introduction

Background

On October 13, 2006 the DHS Office of Security published a PIA detailing how the Department would implement Homeland Security Presidential Directive-12 (HSPD-12),[1] *Policy for a Common Identification Standard for Federal Employees and Contractors*. The PIA and accompanying System of Record Notice (SORN)[2] discussed the use of the following information technology (IT) systems Personnel Security Activities Management System (PSAMS) and the PIV IDMS.

In the previously published PIV PIA only certain DHS components had opted to utilize the Headquarters solution for HSPD-12 implementation[3]. Since that time all DHS components except the U.S. Coast Guard (USCG) have elected to adopt the Headquarters HSPD-12 solution. The following DHS components will now utilize the existing Headquarters process: Federal Law Enforcement Training Center (FLETC), Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), the Federal Emergency Management Agency (FEMA), and the U.S. Secret Service (USSS). Although the USCG has not yet elected to use the Headquarters solution, certain USCG employees may be issued HSPD-12 credentials through other components as duties require. The USCG may in the future elect to implement the Headquarters HSPD-12 solution. In the event this occurs, USCG will also meet the parameters of this PIA and this PIA will be updated to note such change in status.[4] All other DHS directorates, offices, and

---

[1] Personal Identity Verification PIA, October 13, 2006.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_hc_piv.pdf.
[2] Personal Identity Verification Management System, SORN, September 12, 2006.
http://edocket.access.gpo.gov/2006/E6-15044.htm
[3] For the purposes of this PIA, "Headquarters" refers to DHS programs, directorates, and offices other than the eight major DHS components (i.e. USCG, FLETC, TSA, CBP, USCIS, ICE, USSS, and FEMA).
[4] Similar to USCG, certain major programs within DHS components may interface with the Headquarters

programs will be administered by DHS Headquarters as discussed in the original PIA and as updated here.

An outcome of this process is the Department-wide utilization of the PIV infrastructure established by DHS Headquarters. As such, the PIV process at DHS will utilize updated consolidated enterprise-level IT systems that provide the Department with greater scalability and decreased processing times. Under the HSPD-12 implementation, and in preparation for all DHS components utilizing the Headquarters solution, PSAMS will ultimately no longer be utilized and will be replaced by the Integrated Security Management System (ISMS) and the second-generation Identity Management System (IDMS).[5] ISMS is an updated IT system to PSAMS and replaces the multiple security management systems currently in use across DHS. The next iteration of the IDMS will provide more robust identity management capabilities, which will allow the system to meet Department-wide operational needs. The policies and procedures previously discussed in the DHS IDMS PIA have not changed.

Process

The basic process for individuals to apply for and receive a card is as follows:

- The need for an employee/contractor (referred to as applicant) to receive an identification card is triggered, and the individual is sponsored by an appropriate employee or official. A new employee/contractor will complete the SF-85 form or equivalent, as required.
- Applicant's biometrics (fingerprints and photograph) are captured. The biometrics and the data in the SF-85 or equivalent are used to perform a background investigation that confirms the applicant meets suitability and credentialing requirements.
- After an adjudication indicating that the applicant has met suitability requirements, the executing security office will transfer the applicant's PIV data into the IDMS with an indicator noting approval for issuance of a DHS PIV card. Note that legacy personnel who have already met suitability requirements will be sponsored through simple data transfer from ISMS.
- Applicant verifies identity by providing two forms of government issued identification as required by FIPS 201.

---

solution independently of their controlling component. For example, the Verification Division of USCIS may interface directly with the HQ PIV systems instead of routing information through the USCIS systems. US VISIT (NPPD) may also interface in this manner. These programs are covered by this PIA.

[5] ISMS PIA, January 15, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_psams_isms.pdf.

- Applicant's biometrics (fingerprints and photograph) are captured a second time and matched against the biometrics already stored in the system to confirm the applicant's identity.
- The PIV card is produced.
- Applicant receives a new DHS PIV card.
- As applicable, the DHS PIV card and access privileges are revoked.

Although components may make individual adjustments to the process, they follow the same general process described above.

Reason for the PIA Update

This PIA update addresses changes to the Department's HSPD-12 infrastructure as a result of integrating the components previously not covered by the Headquarters solution. The changes are as follows:

- The replacement of the initial IDMS with second-generation IDMS,
- The eventual replacement of PSAMS with ISMS,[6]
- The categories of individuals for which information will be collected in the IDMS, ISMS, and CMS are expanded to include:
  - Emergency response officials,
  - Detailees from other agencies, and
  - Foreign nationals on assignment.

As stated above, components that will use both ISMS and the IDMS include Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigrations and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS). The U.S. Secret Service (USSS) and U.S. Coast Guard (USCG) may also use ISMS. The Transportation Security Administration (TSA) is developing a separate identity management vetted database and will only use the Department's IDMS.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

[6] ISMS PIA, January 15, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_psams_isms.pdf.

The categories of individuals for which information will be collected are expanded to include emergency response officials, detailees from other agencies, and foreign nationals on assignment that require long-term access to DHS facilities.

In order to support DHS components, the HSPD-12 solution also requires additional categories of records, specifically maiden name, mother's maiden name, date of birth, clearance level, identifying physical information, financial history, entry on duty date, expansion on what is included in an SF-85, SF-86, or equivalent documents (Questionnaire for Non-Sensitive Positions, Questionnaire for National Security Positions, respectively), and weapons bearer designation. These records are either new records in the PIV system or were erroneously excluded from the previous PIA and SORN. These records are consistent with records currently collected in support of previous credentialing processes prior to HSPD-12.

Uses of the System and the Information

The uses of the personally identifiable information collected for the PIV Program have not changed with this update. The information is used to verify identity and issue credentials throughout DHS and its components.

Retention

The retention schedules for the PIV Program have not changed with this update. Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). For security facilities, records of access are maintained for five years and then destroyed unless retained for specific, ongoing security investigations. For other facilities, records are maintained for two years and then destroyed. All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

Internal Sharing and Disclosure

Initially, components will not have a need to share HSPD-12 data with other components or internal systems. Each participating component directly enters the data into ISMS, which then populates the IDMS with the information necessary to produce the PIV card.[7] In the future cross-component information sharing may occur in cases such as employee transfer and name reconciliation (data integrity checks and audit).

[7] TSA plans to use a slightly different process for vetting employees. TSA information will not use the DHS ISMS system and will instead populate the IDMS with information directly from its own vetting system.

The PIV card will ultimately be used for physical access control (entry into DHS facilities) and logical access control (access to DHS systems and computers). When the upgraded physical and logical access controls systems are in place, information from the PIV card, such as unique identifiers and authentication information for physical and logical access privileges, can be shared with physical and logical access control systems across DHS.

All data transmitted internally is safeguarded in accordance with applicable rules and policies, including all applicable DHS policies. Strict controls are imposed to minimize the risk of compromising the information in transit. For more information on data protection, please see the "Safeguards" section of the DHS PIV SORN and its update.[8]

External Sharing and Disclosure

DHS may share limited personally identifiable information (name, email address, and duty office) with a contractor service used to schedule appointments for employees to receive their cards.

The only other change to external sharing is reflected in the updated SORN for the IDMS. The updated SORN includes an additional routine use for information sharing for the purposes of resolving and investigating incidents related to a data breach or identity theft.

Notice

DHS is issuing an updated SORN to reflect some changes made to the system of records. That notice will be published in the Federal Register when this PIA is posted on the DHS website.

Individual Access, Redress, and Correction

The processes for access, redress, and correction have not changed with this update.

Technical Access and Security

The implementation of the second-generation IDMS did not require any changes in processes or increase privacy risks. The controls discussed in the previous PIA are in use for the next generation of IDMS. This system has completed the C&A process to acquire its Authority to Operate (ATO), which was granted on June 23, 2008 for a period of 3 years. The 800-79 C&A was completed on June 16, 2008 for the original system. The C&A for the new system is expected to be completed June 1, 2009.

---

[8] Personal Identity Verification Management System, DHS-OS-2006-047, September 12, 2006, 71 FR 53697. The update will be published in the *Federal Register* on the day this PIA is published at www.dhs.gov/privacy.

Technology

The first-generation IDMS was an HSPD-12 compliant solution; however, when considering the volume of applicants that must be processed, and the volume of cards that must be produced, the original system was not equipped to meet the expected demands efficiently. The second-generation of IDMS provides the Department with more robust, scalable identity management capabilities, providing the system capacity necessary to handle periods of high processing volume and growth with the Department. The IDMS technology supports enterprise-level identity management and provides reduced processing times. Further, the second-generation IDMS accommodates the enterprise needs of the Department and makes it scalable to the components' usage. The system has the capability to deploy and establish enrollment and issuance workstations more efficiently. The IDMS interacts with the components' databases and provides solutions for using the DHS PIV card for logical and physical access. Additionally, PSAMS will be replaced with ISMS, a consolidated Department-wide security information system which is covered by a separate PIA.[9]

Responsible Official

Cynthia Sjoberg, Program Director, HSPD-12

Office of Security

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

[9]The ISMS PIA is available here:
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_psams_isms.pdf