Privacy Impact Assessment Update
for the
Personal Identity Verification
DHS/ALL/PIA-014(b)

August 23, 2012

Contact Point
Cynthia Sjoberg
Chief, Identity Management Division (IMD)
Office of the Chief Security Officer
Department of Homeland Security
(202) 245-1114

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

Abstract

The Department of Homeland Security (DHS) is updating the Personal Identity Verification (PIV) Privacy Impact Assessment (PIA) Update, issued on June 18, 2009, to reflect changes in Departmental requirements and enhanced interoperability with US-VISIT Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Integrated Automated Fingerprint Identification System (IAFIS), DHS Component Physical Access Control Systems (PACS), DHS Component Active Directories, as well as issuance of PIV compatible credentials to visitors to DHS.

Introduction

Background

On June 18, 2009, the DHS Office of the Chief Security Officer (OCSO) published a PIA update detailing how the Department was implementing Homeland Security Presidential Directive-12 (HSPD-12),[1] *Policy for a Common Identification Standard for Federal Employees and Contractors.* The PIA update and accompanying Systems of Record Notices (SORN)[2] discussed the use of the Integrated Security Management System (ISMS)[3] and the Identity Management System (IDMS).

The previously published PIV PIA update noted the DHS Components added to the enterprise IDMS, as well as new IDMS system functionalities added through change and configuration management. Continued collaboration with DHS Components ensures the enterprise IDMS meets the needs of Department partners, increases efficiency, and decreases cost through a reduction in redundancies and the interconnection of other enterprise systems.

Process

As a whole, the process for candidates applying for and receiving DHS PIV Cards remains unmodified from the last PIA update. However, this PIA Update is being conducted to

[1] DHS/PIA/ALL-014(a) Personal Identity Verification PIA Update, June 18, 2009, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_hc_piv.pdf.
[2] This PIA Update is covered by three DHS SORNs: DHS/ALL-023 - Department of Homeland Security Personnel Security Management (February 23, 2010), 75 FR 8088, available at http://edocket.access.gpo.gov/2010/2010-3362.htm, DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management (February 3, 2010), 75 FR 5609, available at http://edocket.access.gpo.gov/2010/2010-2206.htm, and DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System (June 25, 2009), 74 FR 30301, available at http://edocket.access.gpo.gov/2006/E6-15044.htm.
[3] For a detailed description of the Integrated Security Management System (ISMS) please see DHS/ALL/PIA-038 Integrated Security Management System (ISMS) Privacy Impact Assesment, March 22, 2011, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_isms.pdf.

detail the new interaction between the IDMS and DHS Component Active Directory and PACS, and the US-VISIT IDENT system.

Currently, when a potential new candidate (i.e., DHS employee or contractor) submits fingerprints as part of the personnel security and suitability processes and subsequent entry-on-duty, his or her fingerprints are collected twice. The first collection occurs during the personnel security and suitability processes. The second collection occurs when fingerprints are captured from a candidate at a DHS PIV Card Issuance Facility (PCIF) on their first day of employment to receive their PIV card. The fingerprints captured from this second collection are stored in IDMS, but a second search of IDENT and IAFIS does not occur.

The new interaction between IDMS and IDENT will allow for a more streamlined fingerprint collection process and search of IDENT and IAFIS to determine a candidate's suitability. Once a candidate submits his or her ten-fingerprint biometric for their personnel security and suitability processes, the information is stored and maintained within IDMS. Biometrics are then sent to IDENT and are used for search purposes only within IDENT and IAFIS. The new interaction between IDMS and IDENT does not result in the enrollment or storage of biometric information into IDENT. IDENT functionality is limited to a conduit to the IAFIS search only.[4]

Once IDENT receives and processes the information, it will then relay any additional information to the IDMS, providing further assurance to the Department that a candidate is suitable. Once a candidate receives a favorable suitability determination, the candidate will only need to perform a one-to-one (1:1) biometric authentication against information stored within the IDMS during the PIV card issuance process. Biometric information is deleted from IDENT following the "match" or "no match" returned to IDMS from IDENT and IAFIS. For additional information, the US-VISIT IDENT program currently has a PIA that addresses the IDENT data responsibilities.[5] The interaction between IDMS and IDENT does not result in the enrollment or

[4] The functionality of IDENT as a conduit to IAFIS for this purpose is covered by the DHS/USVISIT-0012 - DHS Automated Biometric Identification System (IDENT) SORN (June 5, 2007), 72 FR 31080, available at http://edocket.access.gpo.gov/2007/07-2781.htm. The *Categories of Individuals* within DHS/USVISIT-0012 include "Individuals whose biometrics are collected by, on behalf of, in support of, or in cooperation with DHS as part of a background check or security screening in connection with their hiring, retention, performance of a job function, or the issuance of a license or credential." External information sharing to IAFIS is permitted under Routine Use (B) "To appropriate federal, state, local tribal, foreign, or international government agencies charged with national security, law enforcement, immigration, intelligence, or other DHS mission-related functions in connection with the hiring or retention by such an agency of an employee, the issuance of a security clearance, the reporting of an investigation of that employee (but only if the System of Records in which the investigatory files are maintained allows such disclosure), the letting of a contract, or the issuance of a license, grant, loan, or other benefit by the requesting agency."

[5] DHS/NPPD/USVISIT/PIA-002(b) Enumeration Services of the Automated Biometric Identification System (IDENT) (May 25, 2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_enumeration.pdf.

storage of biometric information into IDENT. IDENT functionality is limited to a conduit to the IAFIS search only.

Once a candidate is deemed suitable for employment and requires a PIV card, information stored within the IDMS can be provided to a DHS Component Active Directory to enable smart card log-in, application access, and digitally signed and encrypted E-mail. Additionally, the IDMS can provide PIV card data to DHS Component PACS to streamline the physical access management process and improve security by providing PIV card status (e.g., card revoked or valid). The DHS OCSO is working with DHS Components to inter-connect both Active Directory and PACS with the IDMS.

Reason for the PIA Update

This PIA update addresses changes made to the Department's HSPD-12 infrastructure due to links with Component Active Directory connections, planned integration with DHS Component PACS and planned interconnection with the US-VISIT IDENT/CJIS IAFIS system. The changes are as follows:

- The planned Active Directory connections will synchronize candidate account information with data stored within the IDMS and on a candidate's PIV card. This is necessary to enable logical access and to ensure data accuracy.
- The planned interface between the IDMS and Component PACS will share data about new candidates and update the status of existing data for access control purposes.
- The planned US-VISIT IDENT/CJIS IAFIS connection provides an interface between the IDMS and IAFIS via IDENT so that relevant criminal history information about potential candidates (i.e., DHS employees and contractors) can be made available to ISMS and DHS Personnel Security (PERSEC) as part of the background investigation process. Through the existing connection, ISMS receives criminal history data from the IDMS.
- The DHS enterprise IDMS will store biographic and biometric information about visitors issued a PIV-compatible access card for identification and/or access to a DHS facility. A visitor is any individual attempting or requesting access to agency facilities that is not an employee, contractor, or primary affiliate of the agency.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

Visitors and any members of the public applying for a position within DHS will now have their biographic and biometric information collected in the IDMS. These new categories of individuals, while not covered under the and DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System, are covered by the DHS/ALL-023 - Department of Homeland Security Personnel Security Management SORN. DHS/ALL-023 allows the Department to collect information from Federal employees, applicants, excepted service federal employees, contractor employees, retired employees, and past employees providing support to DHS who require: (1) unescorted access to DHS-owned facilities, DHS-controlled facilities, DHS-secured facilities, or commercial facilities operating on behalf of DHS; (2) access to DHS information technology (IT) systems and the systems' data; or (3) access to national security information including classified information.

Visitors and members of the public are not issued a PIV card for entry into DHS facilities, unless they are consultants, volunteers engaged by DHS who require long-term access to Federally controlled facilities and information systems; Federal emergency response officials; foreign nationals on assignment; other Federal employees detailed or temporarily assigned to DHS in direct support of the DHS mission and who work in Federally controlled facilities or require access to Federal information technology systems; or individuals who require regular, ongoing access to agency facilities, information technology systems, or information classified in the interest of national security.[6]

Uses of the System and the Information

There have been no changes made to the use of personally identifiable information (PII) collected for the PIV program. The information is used to verify identity and issue credentials throughout DHS.

Retention

There have been no changes made to the retention schedules for the PIV program. Records relating to an individual's access are retained in accordance with General Records

[6] See *Categories of Individuals* under DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System (June 25, 2009), 74 FR 30301, available at http://edocket.access.gpo.gov/2006/E6-15044.htm.

Schedule 18, Item 17, which the National Archives and Records Administration (NARA) approved. For maximum security facilities, records of access are maintained for five years and then destroyed unless retained for specific, ongoing security investigations. For all other facilities, records are maintained for two years and then destroyed. All other employee records are retained and disposed of in accordance with General Records Schedule 18, item 22a, which NARA also approved. Records are destroyed upon notification of death or no later than five years after an employee leaves.

Internal Sharing and Disclosure

The DHS PIV Card will 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 DHS PIV Card, such as unique identifiers and authentication information for physical and logical access privileges, will be shared with physical and logical access control systems across the Department.

All data transmitted internally is safeguarded in accordance with applicable rules and policies, including all applicable DHS policies. Strict controls 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. Changes to the information shared by the IDMS are as follows:

1. US-VISIT IDENT/CJIS IAFIS connection streamlines and augments the security of DHS employee and contractor background investigation process. Table 1 provides information regarding the data exchanged for this connection.

Table 1: *IDMS and IDENT/CJIS IAFIS Data Attributes*

Data	Description & Contents	Creator	Recipient
Person Name	First, Middle, and Last Name, where applicable, of the individual's identity record.	IDMS	IDENT receives this information in order to perform searches and matches; IDMS does not enroll this information into IDENT. FBI IAFIS receives this information to perform a criminal history check; IAFIS only stores the data if there is existing derogatory criminal data.

Data	Description & Contents	Creator	Recipient
Fingerprint Biometric	Segmented ten finger biometric; formatted in IDENT IXM format	IDMS	IDENT receives this information in order to perform searches and matches; IDMS does not enroll this information into IDENT. FBI IAFIS receives this information to perform a criminal history check; IAFIS only stores the data if there is existing derogatory criminal data.
Social Security Number	Social Security Number	Received from ISMS via web interface	IDENT receives this information in order to perform searches and matches; IDMS does not enroll this information into IDENT. FBI IAFIS receives this information to perform a criminal history check; IAFIS only stores the data if there is existing derogatory criminal data.
Date of Birth	Date of Birth	Received from ISMS via web interface	IDENT receives this information in order to perform searches and matches; IDMS does not enroll this information into IDENT. FBI IAFIS receives this information to perform a criminal history check; IAFIS only stores the data if there is existing derogatory criminal data.
Originating Agency Identifier (ORI)	DHS Agency Organization Request Identifier (ORI) code is used for billing purposes	Provided by PERSEC and stored within IDMS	Data is provided by the IDMS via IDENT and associated within FBI IAFIS
Rap Sheet	FBI provides a criminal history data and rap sheet based on a biometric match	FBI IAFIS	Sent to ISMS via an IDENT and IDMS data connection

2. IDMS will make data available to DHS PACS for data synchronization and access control. Table 2 provides information regarding the data exchanged for this connection.

Table 2: *IDMS and PACS Data Attributes*

Data	Description & Contents	Owner	Stored in Component PACS
Card Holder Unique Identifier	Used to establish a unique identifier that associates an individual with his or her credential as well as provides information about the issuer of the credential Contains: agency code, card serial number, issuing system code, credential services/version, issue and expiration date, digital signature of the issuing system, and cryptographic information for data integrity Format compliant with FIPS 201-1 and NIST 800-73	IDMS	X
Person Name	The name associated with an individual that is used as part of the enrollment record into PACS	Received from ISMS via web interface	X
Component Affiliation	An individual's organizational affiliation that is used as part of the enrollment record into PACS	Received from ISMS via web interface	X
Facial Biometric	An applicant or user's facial biometric	IDMS	X
PIV Card Status	Status of an individuals' PIV card; *revoked or current*	DHS PKI	X
PIV Authentication Certificate	Used for electronic authentication Contains: person's name, organizational affiliation, issuer, validity period, usage, public keys and certificates, and other relevant cryptographic information * Reference "DHS PKI Certification Practices" statement for specific details.	DHS PKI	X

3. The IDMS will make data available to DHS Component Active Directories to enable logical access and for the purposes of data synchronization. Table 3 provides information regarding the data exchanged for this connection.

Table 3: *IDMS and Active Directory Data Attributes*

Data	Description & Contents	Owner	Stored in Component Active Directory
Electronic Data Interchange Personal Identifier (EDI-PI)	IDMS tracking number to ensure uniqueness of an individual's record A ten digit, randomly generated sequential numerical string Example: John Doe's EDI-PI = 1234567890	IDMS	X
User Principal Name (UPN)	Used for Microsoft Domain Authentication. Consists of EDI-PI @ [DHS Component Active Directory Domain].gov Example: 1234567890@hq.dhs.gov	IDMS	X
PIV Authentication Certificate	Used for electronic authentication Contains: person's name, organizational affiliation, issuer, validity period, usage, public keys and certificates, and other relevant cryptographic information * Reference "DHS PKI Certification Practices" statement for specific details.	DHS PKI	X
PIV Encryption Certificates	Used for electronic authentication Contains: person's name, organizational affiliation, issuer, validity period, usage, public keys and certificates, and other relevant cryptographic information * Reference "DHS PKI Certification Practices" statement for specific details.	DHS PKI	X

4. Visitors to the Department who receive PIV compatible access cards must have the information listed in Table 4 captured in the IDMS:

Table 4: *PIV Compatible Access Cards for Visitors*

Data	Description & Contents	Creator	Stored in IDMS	Stored on Card
Person Name	An individual's name that is used to establish a record within the IDMS and issue a PIV compatible visitor card	IDMS	X	X
Affiliation	Affiliation of the individual (e.g., Federal, Industry, Congress)	IDMS	X	X
Social Security Number	Individual's Social Security Number	IDMS	X	
Fingerprint Biometric	Individual's segmented 10 finger biometric Formatted in IDENT IXM format	IDMS	X	X
Facial Biometric	Individual's Facial Biometric	IDMS	X	X
Date of Birth	Individual's Date of Birth	Received from ISMS via web interface	X	
Contact number	Individual's Business Phone Number	Received from ISMS via web interface	X	
E-mail Address	Individual's Business e-mail address	IDMS	X	

External Sharing and Disclosure

This update has not made any changes to external sharing processes.

Notice

Background check applications and applications for credentials contain notices that discuss the purpose and use of a particular collection. In addition, notice is provided to individuals through the publication of this PIA Update, and the existing SORNs DHS/ALL-023 - Department of Homeland Security Personnel Security Management, February 23, 2010, 75 FR 8088, DHS/ALL-024 - Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, February 3, 2010, 75 FR 5609, and DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System, June 25, 2009, 74 FR 30301.

Individual Access, Redress, and Correction

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

Technical Access and Security

The continued implementation of the IDMS does not require any procedural changes, and does not present any increase in privacy risks. The controls discussed in the previous PIA are still applicable with the current IDMS. The IDMS completed the Security Authorization (SA) process to acquire its Authority to Operate (ATO) in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37-1, which the IDMS received on September 10, 2009 for a period of three (3) years. The SA and renewal of both ATO for the IDMS is expected no later than September 30, 2012.

Technology

The IDMS technology supports enterprise-level identity management and provides reduced processing times. The updates to the system allow for processes, including deploying and establishing enrollment issuance workstations (EIWS), to be more efficient. These updates, which interact with Component databases, also provide DHS Components with logical and physical access solutions using the DHS PIV Card. Furthermore, the new IDMS accommodates the enterprise needs of the Department and makes it scalable to the Components' usage.

Responsible Official

Cynthia Sjoberg, Chief, Identity Management Division (IMD)
Office of the Chief Security Officer (OCSO)
Department of Homeland Security (DHS)

Approval Signature

Original signed and on file at the DHS Privacy Office.

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