Privacy Impact Assessment Update
for the
Personal Identity Verification/Identity Management System (PIV/IDMS)

DHS/ALL/PIA-014(c)

October 20, 2015

Contact Point
David Colangelo
Office of the Chief Security Officer
(202) 447-5320

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security is updating the Personal Identity Verification (PIV) Privacy Impact Assessment (PIA), previously issued on August 23, 2012, to describe the new integration of the Identity Management System (IDMS) with other DHS security systems, issuance of new credentials for DHS facility visitors, implementation of Continuous Evaluation for certain DHS employees, and to document the PIA name change from Personal Identity Verification to Personal Identity Verification and Identity Management System (IDMS). DHS is conducting this PIA update because PIV/IDMS collects, maintains, and disseminates personally identifiable information (PII) about members of the public and DHS employees and contractors.

Overview

On August 23, 2012, DHS published a Privacy Impact Assessment (PIA) update[1] detailing how the Department implemented Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.[2] The PIA update and accompanying Systems of Record Notices (SORN)[3] discussed the use of the Integrated Security Management System (ISMS)[4] and the Identity Management System (IDMS). The process for candidates applying for and receiving DHS (Personal Identity Verification) PIV Cards remains unmodified from the August 2012 PIA Update.[5]

This PIA update details (1) the planned interaction between the PIV/IDMS system and the DHS Component Active Directories for logical and physical access; (2) issuance of temporary badges to DHS visitors; (3) integration and interconnections with the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT)[6] to enable Continuous

---

[1] DHS/PIA/ALL-014(b) Personal Identity Verification PIA Update, August 23, 2012, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_dhs_piv_august2012.pdf.
[2] 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.
[3] 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.
[4] For a detailed description of the Integrated Security Management System (ISMS) please see DHS/ALL/PIA-038 Integrated Security Management System (ISMS) Privacy Impact Assessment, March 22, 2011, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_isms.pdf.
[5] DHS/PIA/ALL-014(b) Personal Identity Verification PIA Update, August 23, 2012, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_dhs_piv_august2012.pdf.
[6] DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012), *available at* http://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

Evaluation (CE); (4) implementation of a scheduling tool connected to the IDMS; and (5) new sharing with DHS internal investigative organizations.

Reason for the PIA Update

DHS is updating this PIA to describe the following updates to the IDMS:

1) *Interaction between the IDMS and the DHS Component Active Directories for Improved Logical and Physical Access Control*

DHS is launching new system interfaces to support the various DHS Logical Access Contol Systems (LACS) and DHS Physical Access Control Systems (PACS), to provide a connection between IDMS and Active Directory. The DHS Trusted Identity Exchange (TIE)[7] provides a connection hub between IDMS and both LACS and PACS. This connection provides biographic, credential, and account information to improve the accuracy and timeliness of information used for access control decisions. Once a candidate is deemed suitable for employment and is issued a DHS PIV Card, certificate information stored within IDMS is provided to the candidate's assigned Component Active Directory.

For logical access, this connection will enable DHS employees and contractors to use their DHS PIV Cards to log-in to DHS networks and applications and to digitally sign and encrypt e-mail or electronic forms.[8] For physical access, IDMS provides DHS PIV Card data to DHS and Components to provision the cardholder for access to his or her respective building or location. This information is used to provision (or de-provision) cardholder access based on changes to his or her DHS PIV Card status (e.g., active, revoked, suspended).

2) *Issuance of temporary badges (i.e., alternative PIV cards) to DHS temporary employees, visitors, and individuals of partner programs and affiliates*

The Department lacks an enterprise wide and unified approach to policies, processes, and procedures to manage identity vetting, sponsorship, credentialing, and access management for temporary employees, visitors, and individuals of partner programs and affiliates that do not meet the PIV issuance requirements. Issuance of temporary badges to these personnel types at an enterprise-level is a necessity within the Department;[9] DHS Headquarters and Components

[7] DHS/ALL/PIA-050 DHS Trusted Identity Exchange (April 2, 2015), *available at* http://www.dhs.gov/publication/dhs-all-pia-050-dhs-trusted-identity-exchange.

[8] This information consists of the cardholder Microsoft User Principal Name (UPN), the PIV Authentication, Digital Signature, and Key Encryption certificates.

[9] OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, which called for federal agencies to implement Federal Information Processing Standard (FIPS) 201 for agency employees and contractors who work at agency facilities or have access to agency information systems in order to increase the security of federal facilities and information systems. This includes issuance of temporary badges to temporary employees and visitors.

currently issue temporary badges, but the temporary badge templates and access management capabilities are disjointed and not consistent across the Department.

Because of the interrelationship between identity management and access management, DHS is implementing standard temporary badge templates and guidance to provision the access capabilities associated with those templates. These templates will set the framework and processes to provide facility and logical access credentials across DHS for visitors and individuals serving in DHS partner programs and affiliates. The templates apply to all DHS organizations.

Although DHS Components may have visitor management programs that primarily focus on access management internal to their organization, the HSPD-12 Program Office unifies these efforts at a Department level using the PIV/IDMS to manage credentials and temporary badges used for facility and logical access across DHS for temporary employees and visitors to all organizations. This effort is intended to support a fully integrated set of processes used to improve the performance and efficiency of the Government by working to reduce costs, streamline processes, eliminate duplication, and create a leaner, smarter, and more efficient Department. These processes improve the experience of the temporary employee and visitor, increase public confidence, and demonstrate better stewardship of taxpayer dollars.

3) Integration and interconnections with IDENT

As part of the DHS enrollment into the Personnel Security CE process, this update covers the integration and expanded data connections between the OBIM IDENT and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Next Generation Identification (NGI) system.[10] These data connections will be used to verify the identity of persons associated with matters of national security. The DHS Office of the Chief Security Officer (OCSO) will obtain the following services from IDENT:

- **Identify Service (+External Identify):** The IDENT "identify service" will be used to enroll an applicant's (e.g., DHS employee or contractor) fingerprint biometrics and associated biographic data into IDENT in order to search both the FBI NGI gallery and IDENT to inform the personnel suitability process for employment or contract support. Upon a match, IDENT returns associated biographic encounter information as a result of an IDMS "identify service" request. IDENT also passes the FBI CJIS NGI biometrically matched Criminal Master File history in the form of a rap sheet as part of the "external identify" response.
- **Notification Services (Derogatory Information (DI) and Encounter):** Notification services will be activated for all DHS personnel requiring CE stored in the IDENT database. These services provide recurrent vetting by informing the

[10] For more information about the FBI CJIS NGI, *please visit* https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.

IDMS if the applicant is encountered by another IDENT user, the FBI, or if new DI is enrolled into IDENT. A notification provides only basic information to include an encounter identifier associated with the triggering event.

- **Retrieve Identity:** Upon notification of an encounter from the "notification service," the IDMS can retrieve detailed information by performing a "retrieve identity" request to IDENT. The retrieve identity provides detailed information such as date, location, and reason for the encounter.

4) IDMS scheduling tool

This update gives notice of the implementation of a scheduling tool connected to the IDMS. This scheduling tool allows personnel applying for federal or contract work with DHS to schedule an enrollment appointment at a DHS PIV Card Issuance Facility (PCIF). This tool will replace the current solution (TimeTrade). The benefit is that the IDMS pre-populates the locations for the enrollment stations into the scheduling tool to assist with coordinating the appointment for PIV enrollment and issuance.

5) New sharing with DHS internal investigative organizations

Sharing a sub-set of data elements with DHS internal investigative organizations for the purpose of investigating criminal acts or security violations within DHS-owned and leased facilities.

Privacy Impact Analysis

Authorities and Other Requirements

In addition to the authorities documented in the "Authority for maintenance of the system" sections of the DHS/ALL-023, DHS/ALL-024, and DHS/ALL-026 SORNs, the following authorities cover the OBIM IDENT to IDMS data interfaces: Civil Service Act of 1883, Section 2 – original authority; Pub. L. 82-298; Pub. L. 92-261; Pub. L. 93-579; and Pub L. 107-347. 5 U.S.C. §§ 1303, 1304, 3301, 7701; 22 U.S.C. §§ 1434, 2519, 2585; 32 U.S.C. § 686; 40 U.S.C. § 11302(e); 42 U.S.C. §§ 1874(c), 2165, 2455.[11]

[11] In addition, the following regulations, Executive Orders, and DHS Directives and Instructions provide authority for the PIV/IDMS. 5 C.F.R. Part 5; 5 C.F.R Part 731; 5 C.F.R. Part 732; 5 C.F.R. Part 736; 32 C.F.R. Part 147; Executive Orders 10422, 10450 (as amended by subsequent Executive Orders), 12968 and 13467. DHS Directives and Instructions: Management Directive 0810.1, The Office of Inspector General; Directive 121-01, Chief Security Officer (Revision 01), including Instruction 121-01-001, Instruction for the Office of the Chief Security Officer (Revision 00) and Instruction Manual 121-007-01, The DHS Personnel Security, Suitability, and Fitness Program (Revision 00); and Directive 121-03, Common Identification Standard for DHS Employees and Contractors (Revision 00).

Characterization of the Information

The data elements associated with the below sub-sections are located in Appendix A.

Logical and Physical Access Control updates:

The DHS TIE provides a connection hub between IDMS and Component Active Directory and applications to provision biographic, credential, and account information to support accurate and timely access control decisions. Once a candidate is deemed suitable for employment and is issued a DHS PIV Card, certificate information stored within IDMS is provided to selected DHS Component Active Directories to enable DHS PIV Card log-in to DHS networks and applications, and to digitally sign and encrypt e-mail or electronic forms.

DHS IDMS will also connect to Component PACS (either directly or through the TIE) to provide biographic, biometric (photograph), credential, and account information. This update improves the accuracy and timeliness of personnel data for physical access control decisions. Once a candidate is deemed suitable for employment and is issued a DHS PIV Card, PIV card and other person data stored within IDMS is provided to selected DHS Component electronic PACS to enable building access.

IDENT interconnection updates:

IDMS provides fingerprint and biographic data that is enrolled to conduct biometric searches of IDENT and criminal history checks of NGI; any future biometric matches whether IDENT or NGI, will be provided in real-time to IDMS for transmission to ISMS. These matches will then become encounters for CE. The PIV/IDMS forwards information requests from ISMS to IDENT and NGI to perform a fingerprint check. IDMS is not storing any additional or new information as a result of interconnection with IDENT or NGI. Data provided will reside in the IDENT IT system to support the database search for the identity associated with the request and to locate encounters found for the individual.

Active Directory updates:

The Component Active Directory may access IDMS to obtain objects necessary to support DHS PIV Card logon to the Component Windows domain(s). This information includes:

- Cardholder User Principal Name;
- PIV Authentication Certificate;
- PIV Digital Signature Certificate; and
- PIV Key Encryption Certificate.

The information sources are ISMS and the DHS Public Key Infrastructure (PKI). No information is received from commercial sources or publicly available data. The role of PIV/IDMS

is to make the information available to the Component to support Windows logon. The accuracy of the data has already been verified because the data is sourced from an authoritative trusted source.

Privacy Risk: There is a risk that adverse information uncovered via source checks listed above may be associated with the wrong individual.

Mitigation: This risk is mitigated by IDMS enhancements and changes to the IDMS processes outlined in this PIA update, and by existing personnel security adjudication procedures. OCSO's ability to verify an individual's identity and rule out any false positives will be enhanced by collecting fingerprints only once during the security process, and using both biometric and biographic, rather than only biographic information for criminal history checks. Furthermore, adverse information uncovered over the course of a background investigation is further evaluated to verify its accuracy and resolve any potential identity discrepancies.

Uses of the Information

On-Boarding and Continuous Evaluation

IDMS will integrate with the DHS IDENT IT system to perform recurring biometric checks, enabling CE for personnel meeting specific criteria (e.g., eligibility or access to Top Secret/Sensitive Compartmented Information) as determined by DHS personnel security.[12] If a candidate requires CE, the DHS or Component personnel security office will search the IDMS for an individual's record and submit a request for a fingerprint check to IDENT (listed in the "Characterization of the Information" section of this document). IDENT will perform a search of the IDENT database and will also send a biometric criminal history check to the FBI NGI system.[13] If a match exists within the IDENT or NGI database, IDENT will send the results to IDMS. IDMS will forward this data to ISMS for inclusion into the individual's personnel security records.

[12] OCSO uses IDENT as a service provider to for biometric checks with NGI. This information sharing is compatible with the purpose of DHS/ALL-023 Personnel Security Management System of Records and permissible under Routine Use H.

[13] The functionality of the IDENT IT system as a conduit to NGI for this purpose is also 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 covered by the system* 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 NGI 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."

Once IDMS is integrated with IDENT, IDMS will enroll personnel biographic and biometric information during on-boarding. Post-enrollment, biometric, and biometric data can then be used to perform biometric fingerprint checks through IDENT, issuance of the PIV credential, as well as lifecycle identity management during an individual's employment at DHS.

If a biometric background seach is needed, IDMS will send the individual's data to IDENT, IDENT will enroll and store the individual's biometrics into the IDENT gallery, and any future biometric matches (whether IDENT or NGI) will be provided to IDMS for transmission to ISMS, enabling faster, automated encounter and derogatory information for CE. IDENT will not share DHS personnel information with any IDENT customers. Only DHS Personnel Security Users will have the ability to perform searches against OCSO-submitted information into IDENT. No external users are able to access DHS OCSO data elements on personnel (e.g., federal employees, contractors).

PIV Card Issuance Process and User Provisioning

If a candidate receives a favorable suitability determination, he or she will need to undergo biometric authentication[14] against information stored within PIV/IDMS during the DHS PIV Card issuance process. This biometric information, facial image, and candidate fingerprints are retained in IDMS for placement on the DHS PIV Card.

Once a candidate is deemed suitable for employment by his or her personnel security office and is issued a DHS PIV Card, the IDMS will provide certificate information[15] to the candidate's assigned Component Active Directory to enable DHS PIV Card log-in to DHS networks and applications and to digitally sign and encrypt e-mail or electronic forms.

IDMS provides DHS PIV Card data to DHS and its Components to provision the cardholder to the PACS. This information is passed to DHS Component PACS in order to facilitate provisioning (i.e., on-boarding) and de-provisioning (i.e., off-boarding) of the cardholder based on changes in DHS PIV Card status (active, revoked, or suspended). The information is made available to the PACS through a secure communications channel from IDMS. The data elements available to Component PACS are largely biographic but include the cardholder image stored on the DHS PIV Card.

New Personnel Security Users

[14] FIPS 201-2, Section 2.8, PIV Card Issuance Requirements, at pages 10-11. One-to-one biometric authentication is the process in which initial set of fingerprints collected during the time of enrollment are the same biometrics being presented at time of PIV card issuance and activation, prior to releasing the PIV card to the applicant or current cardholder.

[15] This information consists of the cardholder Microsoft User Principal Name (UPN), the PIV Authentication, Digital Signature, and Key Encryption certificates. These items are intended to be available on the DHS network to DHS users to enable use of the DHS PIV Card for access to facilities, information technology systems, and data.

Select DHS Personnel Security organizations will be granted access to IDMS information for the purposes of enrolling and submitting biographic and biometric data into the IDMS and submitting a fingerprint check to IDENT during the background investigation process. Personnel security offices will be able to enroll individuals into the IDMS, and view and modify biographic and biometric information in accordance with the fingerprint check process.

Privacy Risk: There is a risk that the information shared and stored within the IDENT IT system may be made available to other IDENT partners, who may use the information inconsistently with the purpose for which it was collected by DHS.

Mitigation: In order to ensure that this sensitive community's information is accessed only by authorized DHS users, only OCSO will be able to perform searches against that information. Although most IDENT user information is accessible to other users, OCSO has required OBIM to limit access to OCSO data to ensure that DHS employee information is inaccessible to others. The IDMS connection is a one way connection allowing IDMS control over the data sent to IDENT. Upon receipt of the IDMS information, IDENT applies specific data filtering rules to prevent IDENT customers and non-OCSO users from accessing IDMS data. The DHS Privacy Office will conduct a Privacy Compliance Review of these filtering rules.

Notice

There are no changes to notice from the August 2012 PIA Update. When applicants submit their Standard Form (SF) 86 to their respective security office, they are provided notice that they may be subject to continuous evaluation on the SF-86 "authorization for release of information."

Data Retention by the project

E-mail addresses will be retained by IDMS per the existing records retention schedules. There have been no other changes made to the retention schedules for the IDMS/PIV with the issuance of this PIA Update. Records relating to an individual's access are retained in accordance with GRS 18, item 17, which has been approved by the NARA. For maximum security facilities records of access are maintained for five years and then destroyed unless retained for specific, ongoing, security investigations. Records are maintained for two years and then destroyed for all other facilities. All other employee records are retained and disposed of in accordance with GRS 18, item 22a, which has been approved by NARA. Records are destroyed upon notification of death or no later than five years after an employee leaves.

Information Sharing

There are no changes to external information sharing with this PIA update.

Redress

No change from the August 2012 PIA Update.

Auditing and Accountability

The Access and Security Controls within IDMS are continually audited in accordance with the IDMS System Security Plan to ensure IDMS maintains a baseline security posture. This includes auditing of unauthorized access attempts. Any unauthorized access to IDMS is audited and reported to the IDMS System Owner and Information System Security Officer (ISSO).

Data provided by IDMS to IDENT is protected by IDENT through system access controls preventing unauthorized access. A "Service Level Agreement" (SLA) and a "Letter of Agreement" (LOA) exist between IDMS and IDENT documenting the requirements to perform auditing, as well as provisions to audit and report security incidents to the corresponding System Owner and ISSO if or when they occur.

The provisioning and de-provisioning of IDMS roles is critical to safeguarding PII and Sensitive PII stored and processed in the IDMS. Personnel assigned an IDMS role must meet the following conditions:

- Be a DHS federal employee or designee (e.g., contractor) authorized by the DHS OCSO or PCIF Manager;
- Have received a favorable background investigation and granted suitability by a DHS or Component Personnel Security Division;
- Have an unexpired valid DHS PIV Card;
- Have a valid need-to-know; and
- Have received training, passed a knowledge check, received a training certificate, and received training renewal on an annual basis.

IDMS user role training is administered in-person or by the IDMS system owner through on-line training that is administered and monitored by the IDMS system owner. No individual receives an IDMS role without the proper training and assessment. Training covers the protection of PII and Sensitive PII collected in IDMS.

System access controls and audit records are maintained for all interfaces and personnel who have access to IDMS information, which includes the IDENT and NGI interfaces. An

electronic audit report can be generated to determine and verify authorized access to information as needed.

Responsible Official

David Colangelo
Chief, Enterprise Security Services Division
Office of the Chief Security Officer
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Appendix A

Table 1: Data Elements IDMS Provides to Other Systems/Programs

Data Elements	DHS PACS	DHS LACS	OBIM IDENT	TIE	Personnel Security	DHS Internal Investigative Organizations
Name (first, middle, last)	X	X	X	X	X	X
Social Security Number (SSN)					X	X
Date of Birth	X	X			X	X
Place of Birth					X	
Citizenship					X	
Agency (e.g. DHS)	X	X	X		X	X
Organization Affiliation (e.g. FEMA)	X	X	X	X	X	X
Employee Affiliation (employee or contractor)	X	X	X		X	X
Foreign National (if applicable)				X	X	X
Facial Image	X	X	X		X	X
Fingerprint Biometric			X		X	
Race					X	
Gender			X		X	
Height			X		X	
Weight			X		X	
Eye Color			X		X	
Hair Color			X		X	
Security Clearance Type	X	X		X	X	
E-mail Contact (provided to PACS after synchronized with LACS)	X	X			X	
User Principle Name (Microsoft Account Name)	X	X		X	X	
Cardholder Unique Identifier (CHUID)				X	X	
PIV Card Identifiers (GUID string/FASC-N string)	X	X		X	X	
Electronic Data Interchange Person Identifier (EDIPI)	X	X		X	X	
PIV Card Status				X	X	X
PIV Card Type				X	X	X
PIV Card Expiration Date				X	X	X
PIV Card Certificates						
PIV Card Certificate Serial Numbers						
Entity Status				X	X	X
PKI Public Key Certificate Data	X	X			X	
User E-mail Address (provided by LACS to IDMS)		X			X	
Transaction Control Number			X		X	
Originating Agency Identifier (ORI)			X		X	
Controlling Agency Identifier (CRI)			X		X	
Type of Transaction (TOT)			X		X	
Type of Search Requested (TSR)			X		X	
Retention Code			X		X	
System IDs				X		

Table 2: Data Elements IDMS Receives from External Sources

Data Received	System Received From	
	IDENT	NGI
First Name	X	X
Middle Name	X	X
Last Name	X	X
Date of Birth (DOB)	X	X
IDENT Specific		
IDENT Fingerprint Identification Number (FIN)	X	
IDENT Encounter Identification (EID)	X	
Date of Encounter	X	
Screening Organization	X	
Encounter Purpose (e.g., CBP Exit/Entry, etc.)	X	
Other Encounter Details (e.g., text data entered by screening official, etc.)	X	
FBI and NGI Specific		
FBI Universal Control Number (UCN)		X
FBI Rap Sheet (if applicable)		X