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

DHS/ALL/PIA-014(e)

May 18, 2017

Contact Point

Reid Baldwin
Acting Director
Enterprise Security Services Division
Office of the Chief Security Officer
(202) 447-0504

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), previously issued on May 8, 2017,[1] to describe new Identity Management System (IDMS) functionality for issuance of Derived PIV Credentials[2] onto DHS-issued mobile devices (*e.g.*, iPhone, Android). This update also addresses the Office of the Chief Security Officer's (OCSO) need to add data elements required for the interface between IDMS and the DHS Office of the Chief Information Officer's (OCIO) Trusted Identity Exchange (TIE).[3] 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, contractors, and other Department-associated affiliates.

Overview

On October 20, 2015, the Department of Homeland Security (DHS) published a Privacy Impact Assessment (PIA) update[4] detailing how the Department continues with implementation of the Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.[5] That PIA update and accompanying System of Records Notices (SORN)[6] discussed the use of the Integrated Security Management System (ISMS)[7] and Identity Management System (IDMS), as well as IDMS

[1] *See* DHS/PIA/ALL-014(d) Personal Identity Verification/Identity Management System (May 8, 2017), *available at* https://www.dhs.gov/privacy.
[2] Derived PIV Credentials are based on the general concept of derived credentials in NIST SP 800-63-2, which leverages identity proofing and vetting results of current and valid credentials. When applied to the DHS PIV Card process, identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential. Instead, the user proves possession of a valid DHS PIV Card to receive a Derived PIV Credential.
[3] The IDMS to TIE interface is covered under DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System (October 20, 2015), but additional data elements were determined necessary after the PIA was released. There is no change in use or sharing from the previously approved PIA, just the expansion of the data elements.
[4] *See* DHS/PIA/ALL-014(c) Personal Identity Verification/Identity Management System (October 20, 2015), *available at* https://www.dhs.gov/privacy.
[5] For more information on how DHS began implementation of the requirements of HSPD-12, please *see* DHS/PIA/ALL-014(a) Personal Identity Verification PIA Update (June 18, 2009), *available at* https://www.dhs.gov/privacy.
[6] This PIA update is covered by three DHS SORNs: DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010); DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010); and DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).
[7] For a detailed description of the Integrated Security Management System (ISMS), please *see* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.

interconnections with the DHS Component Active Directories (AD) and the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT),[8] a new IDMS scheduling tool, new sharing with DHS internal investigative organizations, and issuance of temporary badges.

This PIA update details the technical changes to the Personal Identity Verification (PIV)/IDMS system for issuance of Derived PIV Credentials onto DHS-issued mobile devices, and will also discuss the additional data elements required for the IDMS interconnection with Trusted Identity Exchange (TIE) to work effectively for business within the Department.

Reason for the PIA Update

DHS is updating this PIA to describe the following update to IDMS and the addition of required data elements for use in the IDMS to TIE interconnection.

Office of the Chief Information Officer (OCIO) Mobile Device Manager (MDM) integration for Derived PIV Credential Issuance Process

The Federal Information Processing Standards (FIPS) 201[9] originally required that all PIV credentials and associated keys be stored in a PIV Card. While the use of the PIV Card for electronic authentication works well with traditional desktop and laptop computers, it is not optimized for mobile devices. In response to the growing use of mobile devices within the Federal Government, FIPS 201 was revised to permit the issuance of an additional credential, a Derived PIV Credential. Derived PIV Credentials leverage the current investment in the PIV infrastructure for electronic authentication and build upon the solid foundation of well-vetted and trusted identity of the PIV Cardholder – achieving substantial cost savings by leveraging the identity-proofing results that were already performed to issue PIV cards. The Derived PIV Credential allows users to access their email, contact lists, and calendar from their mobile devices with equivalent security features when using a DHS PIV Card to access a DHS-issued laptop or desktop.

A Derived PIV Credential is an X.509 Derived PIV Authentication certificate, which is issued in accordance with the requirements specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-157[10] when the PIV Authentication certificate on an applicant's PIV Card serves as the original credential. The Derived PIV Credential is an

[8] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy.
[9] The Federal Information Processing Standards (FIPS) 201-2 can be found at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.
[10] For more information, please *see* NIST Special Publication 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials, *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf.

additional common identity credential under HSPD-12 and FIPS 201 that is issued by a federal department or agency and that is used with mobile devices.

A Derived PIV Credential is not automatically loaded onto a user's mobile device. An approved DHS-issued mobile device must be assigned to the current DHS PIV Cardholder. The PIV Cardholder must request a Derived PIV Credential. The process to receive a Derived PIV Credential is:

1. The applicant accesses an IDMS portal and authenticates him or herself by using his or her DHS PIV Card and Personal Identification Number (PIN) to log on;
2. IDMS obtains information about the user's mobile device from the OCIO Mobile Device Manager (MDM). The data elements shared depend on the MDM used by DHS HQ or an Operational Component;[11]
3. The user selects the mobile device from the IDMS portal on which the Derived PIV Credential is to be loaded;
4. The user digitally signs the DHS Derived PIV Credential Responsibility Agreement with the terms of use of the Derived PIV Credential;
5. IDMS generates the Derived PIV Credential and delivers it to the MDM to allow delivery to the user's mobile device;
6. The user creates a password for use of syncing the Derived PIV Credential onto the mobile device and to protect the password;
7. IDMS continuously monitors to ensure the PIV Card is still active and requires the Derived PIV Credential, or determines if the Derived PIV Credential must be revoked (*e.g.*, if the PIV Card is compromised).

No new information is used to create the Derived PIV Credential from the DHS PIV Card. The only new information is what IDMS receives back from the MDM as provided in the *Characterization of the Information* section of this PIA update. The DHS OCSO, the DHS OCIO, and the Office of the Chief Information Security Officer are coordinating efforts in the implementation of this technology and process into the Department. Ultimately, DHS will rely on IDMS as the authoritative source to issue Derived PIV Credentials.

Data Element Additions for TIE Integration with IDMS

The DHS OCSO needs to add data elements required for the interface between IDMS and the TIE. The TIE provides a connection hub between IDMS and the various DHS Logical Access Contol Systems (LACS) and DHS Physical Access Control Systems (PACS). This connection

[11] For example, DHS Headquartes uses AirWatch as the MDM. It collects the mobile number, operating system, and device type. FEMA uses MobileIron as the MDM. It currently does not collect anything about the device.

provides biographic, credential, and account information to improve the accuracy and timeliness of information used for access control decisions.

The additional data elements, not previously covered by DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System, that are being added are detailed in the *Characterization of the Information* section of this PIA update and Appendix A.

Privacy Impact Analysis

Authorities and Other Requirements

The authorities carried forward from the previous update to this PIA, DHS/ALL/PIA-014(c), and those authorities listed in the DHS/ALL-023, DHS/ALL-024, and DHS/ALL-026 SORNs, to the extent that they are still applicable and current law, cover the issuance of Derived PIV Crendentials and the IDMS to TIE data interface.[12]

Characterization of the Information

OCIO MDM Interconnection Updates

IDMS provides a small portion of biographic data already discussed in previous PIAs for the purpose of its interconnection with the MDM for the issuance of a Derived PIV Credential. No new information is being collected in IDMS for the purpose of this process. The data elements discussed in Appendix A will be shared by IDMS with and managed by the MDM system for issuance of the Derived PIV Credential. The mobile devices onto which the Derived PIV Credential will be loaded are DHS owned, managed, and controlled devices. No external sharing of information takes place outside of the DHS OneNet environment.

The role of PIV/IDMS within the MDM connection is to provide pertinent DHS PIV Card status to the MDM for the purpose of initial DHS Derived PIV Credential issuance, maintenance, and revocation as the status of the identity changes within IDMS. Additionally, IDMS data permits the MDM to associate the individual with the issued mobile device and the corresponding derived credential loaded onto the mobile device.

TIE Interconnection Updates

In addition to the data elements documented in DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System, the TIE interconnection with IDMS requires the use of additional data elements to seamlessly allow for users to access DHS resources remotely through

[12] In addition, the following Executive Order provides authority for PIV/IDMS: Executive Order 13764, amending Executive Orders 13488 and 13467.

their DHS-issued mobile devices, enforcing cryptographically secure two-factor credential authentication for DHS e-mail, DHS websites and web content that require stronger authentication, and secure remote access to DHS networks (*i.e.*, Virtual Private Network access). These additional data elements, to include the data elements previously approved, are passed bidirectionally between IDMS and the TIE. These additional data elements are:

- Person Name (first, middle, last);
- Suffix;
- Organization Affiliation (*e.g.*, FEMA, CBP);
- PIV Card Certificates; and
- PIV Card Certificate Serial Numbers.

All of the data elements shared by IDMS with and managed by the TIE system are listed in Appendix A of this PIA. As the scope of logical access expands within the Department, the need to share additional data elements between enterprise systems will expand. As this happens, this and other appropriate PIAs will be updated.

Uses of the Information

The connection from IDMS to the MDM will be used for the following purpose:

- Initial issuance of a DHS Derived PIV Credential;
- Maintenance of the DHS Derived PIV Credential - upon specific revocation use cases that require updates or reissuance of the derived credential (*e.g.*, name change, compromise);
- Implement a more secure method for the Department to secure data on the mobile devices issued to users; and
- Achieve compliance with the FIPS 201-2 and NIST SP 800-157 requirements, and ensure the Department's issuance of an Authorization to Operate (ATO).

Privacy Risk: There is a risk that Department personnel with a mobile device issued before the implementation of DHS Derived PIV Credentials may have a mobile device that is not as secure as those issued with a derived credential.

Mitigation: This risk is partially mitigated. The Department currently does not load any secure credential on any DHS-issued mobile device because this is new technology. The DHS Derived PIV Credential Issuer (DPCI) in coordination with OCIO is determining the phased approach to when each phase will reach a DHS Component, and how those with previously issued mobile devices will obtain an update to have the derived credential loaded onto the device. The

issued mobile device is secure based on current DHS configuration requirements for the devices to meet prior to issuance, and the Derived PIV Credential increases the security of the device.

The additional TIE data elements will be used to further improve the IDMS to TIE interface for the following reasons:

- Business Need: For logical access across the department, PIV Card certificate information needs to be shared between systems to improve security; and
- Improvements: Currently, PIV Card certificate information is obtained by relying systems through manual reading of each card. Sending PIV Card certificate information between systems will not only increase security, but it will reduce operational complexity and save the department time and money. In addition, it will enhance the end user experience and improve ease of use.

Notice

There are no changes to notice from the previous PIV/IDMS PIAs. Additionally, in order to complete the Derived PIV Credential process, an individual user digitally signs a DHS Derived PIV Credential Responsibility Agreement with the terms of use of the Derived PIV Credential.

Data Retention by the project

There have been no other changes made to the retention schedules for IDMS/PIV with the issuance of this PIA update. Records relating to an individual's access are retained in accordance with General Records Schedule (GRS) 18, item 17, which has been approved by the National Archives and Records Administration (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; only process changes.

Redress

There are no changes to redress from the previous PIV/IDMS PIAs.

Auditing and Accountability

The Access and Security Controls within IDMS are continually audited in accordance with the IDMS 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). Additionally, the DPCI maintains the *DHS DPCI Operations Plan*, that comprehensively documents the DPCI operations for issuance and maintenance of a Derived PIV Credential, to include what protections are in place to wipe a mobile device in the event it is lost, stolen, or compromised.

Data provided by IDMS to the MDM is a DHS Headquarters (HQ) to DHS HQ interface and a Memorandum of Understanding (MOU) is not required. As IDMS connects to each DHS Component MDMs, MOUs will be put into place to ensure data integrity and protection of the data being shared or received. The provisioning and de-provisioning of IDMS roles[13] is critical to safeguarding PII and sensitive PII stored and processed in IDMS. Personnel assigned an IDMS role must meet the following conditions:

- Be a DHS federal employee or designee (*e.g.*, contractor) authorized by DHS OCSO;
- 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 online 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 MDM interface. An electronic audit

[13] The provisioning and de-provisioning of roles in IDMS is performed by authorized and trained DHS DPCI personnel.

report can be generated to determine and verify authorized access to information as needed, as required by the systems Security Authorization package.

Responsible Official

Reid Baldwin
Acting Director, Enterprise Security Services Division
Office of the Chief Security Officer
Department of Homeland Security

Approval Signature

Original, signed version on file at the DHS Privacy Office.

_____

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

APPENDIX A

Table 1: Data elements provided by IDMS

Data Elements	MDM	TIE	Mobile Device
Person Name (first, middle, last)	X	X	
Suffix		X	
Electronic Data Interchange Person Identifier (EDIPI)	X	X*	
E-mail Address	X		
Organization Affiliation (*e.g.*, FEMA, CBP)		X	
PIV Card Certificates		X	
PIV Card Certificate Serial Numbers		X	
Derived PIV Authentication Certificate			X
Foreign National (if applicable)		X*	
User Principle Name (Microsoft Account Name)		X*	
Cardholder Unique Identifier (CHUID)		X*	
PIV Card Identifiers (GUID string/FASC-N string)		X*	
PIV Card Status		X*	
PIV Card Type		X*	
PIV Card Expiration Date		X*	
Entity Status		X*	

*These data elements were already being shared from IDMS to the TIE, and are discussed in DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System

Table 2: Data elements received by IDMS from the MDM

Data Elements	IDMS
International Mobile Station Equipment Identity (IMEI)	X
Serial Number of the Mobile Device	X