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

DHS/ALL/PIA-014(d)

May 8, 2017

Contact Point

Reid Baldwin
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) Update, previously issued on October 20, 2015, to describe the new integration of the Identity Management System (IDMS) with the Office of Personnel Management (OPM) Federal Investigative Services Fingerprint Transaction System (FIS-FTS).[1] DHS is conducting this PIA update because PIV/IDMS collects, maintains, and disseminates personally identifiable information (PII) about personnel that apply for a DHS position, which includes DHS employees, contractors, affiliates, and other personnel requiring background investigations to work for or support DHS.

Overview

On October 20, 2015, DHS published a PIA update[2] 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*.[3] The PIA update and accompanying Systems of Record Notices (SORN)[4] discussed the use of the Integrated Security Management System (ISMS)[5] and the Identity Management System (IDMS). The process for candidates applying for and receiving DHS Personal Identity Verification (PIV) Cards will be modified from the October 2015 PIA update.

This PIA update details the technical changes to the upgraded PIV/IDMS system and its connection with Office of Personnel Management (OPM) Federal Investigative Services Fingerprint Transaction System (FIS-FTS). The current process depends on manual processes including sending fingerprint cards through standard mail, courier, or fax, none of which securely bind an individual's identity with his or her associated biometrics. This new process will allow for an automated, electronic process using IDMS.

This PIA update will also detail the process changes for enrollment into IDMS, lifecycle

---

[1] For more information about the this system, please *see* Fingerprint Transaction System (FTS) Privacy Impact Assessment (August 2, 2007), *available at* https://www.opm.gov/information-management/privacy-policy/privacy-policy/fts.pdf.

[2] *See* DHS/PIA/ALL-014(c) Personal Identity Verification/Identity Management System PIA Update (October 20, 2015), *available at* https://www.dhs.gov/privacy.

[3] 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.

[4] 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).

[5] For a detailed description of the Integrated Security Management System (ISMS), please *see* DHS/ALL/PIA-038 Integrated Security Management System (ISMS) (March 22, 2011), *available at* https://www.dhs.gov/privacy.

management of the associated identity data, and issuance of a DHS PIV Card as a result of the associated connection with OPM FIS-FTS.

Reason for the PIA Update

DHS is updating this PIA to describe the following update to IDMS and the enrollment and issuance process of a DHS PIV Card:

OPM FIS-FTS integration for the initial and periodic reinvestigation process

Currently, fingerprints for new DHS employees or contractors are collected twice as part of the "on-boarding" process prior to reporting for duty. The first collection occurs during the personnel security and suitability process, when the DHS Office of the Chief Security Officer (OCSO) Personnel Security (PERSEC) Division or Component PERSEC office provides a set of fingerprints to the Federal Bureau of Investigation (FBI) for a search of the Criminal Justice Information Services (CJIS) Next Generation Identification (NGI) system[6] for any criminal history records. The second collection occurs when fingerprints are captured at a DHS PIV Card Issuance Facility (PCIF) for the DHS PIV Card enrollment and issuance process. The fingerprints captured from the second collection are stored in IDMS to generate biometric templates,[7] which will be stored on the DHS PIV Card. The templates are used to perform 1:1 biometric matching of the cardholder against biometrics available on the DHS PIV Card or authoritative trusted source, as required by the PIV governing standard, the Federal Information Processing Standards (FIPS) 201-2.[8]

A vulnerability, and non-compliance with FIPS 201-2,[9] exists in the current process that there is no action taken by PIV/IDMS to verify that the DHS employee or contractor receiving a

[6] For more information about the FBI CJIS NGI, please *see* https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi. The PIA for this system is *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments, and the SORN is *available at* https://www.justice.gov/opcl/doj-systems-records#FBI.

[7] "Biometric Templates" refers specifically to a standard in the International Committee for Information Technology Standards (INCITS) 378, *Index Finger Minutiae Templates*; it is a recording of the biometric fingerprint minutiae that translates the captured fingerprint biometric into a graphical representation, which is required by the FBI for processing of the data.

[8] The Federal Information Processing Standards (FIPS) 201-2 can be found at, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf.

[9] Control EI – 7 of National Institute of Standards and Technology (NIST) Special Publication 800-79-2, *Guidelines for the Authorization of PIV Card Issuers and Derived PIV Credential Issuers*, requires that the biometrics (fingerprints, facial image, and the optional iris images) that are used to personalize the PIV card must be captured during the identity proofing and registration process. FIPS 201-2 requires a full set of fingerprints (except when not available), because biometric identification using fingerprints is the primary input to law enforcement checks. NIST SP 800-79-2 control EI – 13 requires that if the biometric (fingerprint) data collected to personalize the PIV card and the biometric data (fingerprints) collected to support background investigations are collected on separate occasions, then a 1:1 biometric match of the applicant is performed at each visit against biometric data collected during a previous visit. DHS seeks to close the gap and ensure that the fingerprint biometric data collected for the

DHS PIV Card is in fact the same individual who provided the original fingerprints during the registration process (i.e., the personnel security process). In other words, the current process and solution does not link the biometric captured during the enrollment process with the biometric used for the background investigation or the prints used for the DHS PIV Card for identification or for access, as intended.

DHS OCSO plans to replace this manual biometric process, and non-compliance with FIPS 201-2, with an interconnection between IDMS and OPM FIS-FTS for DHS employees, contractors, affiliates, and other personnel requiring background investigations to work for or support DHS. The connection will not send new information to OPM but replaces the existing manual process for print capture and submission with a more secure and efficient capability through IDMS. By replacing the current manual processes of sending fingerprint cards through standard mail, courier, or fax, this new automated process will securely bind a person's identity with his or her associated biometrics. The current process cannot effectively and authoritatively bind the person's identity when biometrics are gathered at time of enrollment into IDMS for initial issuance of the DHS PIV Card.

With this new process, a DHS applicant[10] chosen to support a position[11] at DHS will come to a PCIF to enroll his or her biometric and biographic information only once.[12] That information is stored electronically and maintained in IDMS. After enrollment, a DHS PERSEC or Component PERSEC will transmit biographic and biometric fingerprint check information to OPM FIS-FTS. Upon receipt of the transmission, OPM FIS-FTS searches the FBI CJIS NGI system gallery, which returns a response to OPM FIS-FTS. Ultimately, OPM FIS-FTS will return the response about criminal history data for the applicant directly to ISMS. This same process will take place for reinvestigations within the Department. The existing connection between OPM FIS-FTS and ISMS is covered by the ISMS PIA.[13]

background investigation are the same that are 1:1 matched against during the issuance and activation phase of the process.

[10] The term *applicant*, for purposes of this PIA update, refers to any employee, contractor, affiliate, and any other personnel supporting the Department who requires a background investigation.

[11] The term *position*, for purposes of this PIA update, refers to positions in general such as federal, contractor, affiliate, and other position types supporting or planning to support the Department.

[12] Existing DHS personnel with a previously approved background investigation will have their fingerprint biometrics recaptured through attrition when new fingerprint biometrics are required to support a new position or an investigation upgrade.

[13] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS) (March 22, 2011), *available at* https://www.dhs.gov/privacy.

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,[14] DHS/ALL-024,[15] and DHS/ALL-026[16] SORNs, to the extent that they are still applicable and current law, cover the OPM FIS-FTS to IDMS data interface.[17]

Characterization of the Information

DHS is not collecting or using any new information as a result of this update. DHS OCSO is replacing the manual biometric process with an interconnection between IDMS and OPM FIS-FTS for DHS employees, contractors, affiliates, and other personnel requiring background investigations to work for or support DHS. The connection will not send new information to OPM but replaces the existing manual process for print capture and submission with a more secure and efficient capability through IDMS. The data elements that are sent to OPM are listed in Appendix A of this PIA.

Uses of the Information

The connection between IDMS and OPM FIS-FTS will be used for the following purposes:

- Establish a biometric chain of trust, linking the fingerprint biometric data captured as part of the background investigation with data used for managing the identity and PIV lifecycle;
- Automate the fingerprint biometric data management process by establishing an automated connection to OPM FIS-FTS for fingerprint submissions;
- Achieve compliance with the OPM directive for fingerprint processing;[18]
- Provide a method to perform biometric impersonation checks;[19] and

[14] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[15] *See* DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).
[16] *See* DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).
[17] In addition, the following Executive Order provides authority for PIV/IDMS: Executive Order 13764, amending Executive Orders 13488 and 13467.
[18] For more information on the OPM mandate, please *see* https://nbib.opm.gov/hr-security-personnel/federal-investigations-notices/2016/fin-16-03.pdf.
[19] Biometric impersonation checks are a method to identify when biometrics submitted previously by any identity applying for a DHS position or under reinvestigation, and are flagged as being associated with the name of someone else. These encounters are provided to IDMS which forwards the encounters to the Personnel Security Division via ISMS for investigative research and decision.

- Provide initial and recurring biometric checks of the FBI CJIS NGI system in support of the personnel background investigation process.

This information was already being used by DHS to conduct background investigations to allow individuals to work for or support DHS. This PIA update only reflects that the information is being transferred in a different manner.

Notice

There are no changes to notice from the October 2015 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

There have been no 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 was approved by 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 was 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. The previous exchange of information between DHS and the FBI occurred through several connections, some of which were manual and many leveraging paper based submissions through fingerprint cards. This PIA update reflects the automation and security enhancements applied to the existing process (biometric linking and the ability to perform continuous biometric checks).

Privacy Risk: There is a risk that DHS information may be compromised once shared with the OPM system.

Mitigation: This risk cannot be fully mitigated, but DHS OCSO has taken steps to reduce the risk. The requirement for federal agencies to provide biographic and fingerprint biometrics for background investigations is not new; the new requirement is that it be performed electronically instead of manually. DHS OCSO has requested OPM to provide documented safeguards for how OPM will protect the data that is transmitted. OPM has taken significant steps to enhance its system to ensure a data breach does not occur. As a result, agreements exist between OPM FIS and DHS

OCSO for this interconnection, as listed in the Auditing and Accountability section of this PIA update.

Redress

There has been no change from the October 2015 PIA update.

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).

Data provided by IDMS to OPM FIS-FTS is protected by OPM through system access controls preventing unauthorized access. The contents of the following documents explain how DHS data is protected:

- *Final MOU between the U.S. Office of Personnel Management (OPM) Federal Investigative Services and the Department of Homeland Security for access to the Fingerprint Transaction System (FTS)*;
- *Final ISA between the DHS Office of the Chief Security Officer (OCSO) Identity Management System (IDMS) and the U.S. Office of Personnel Management (OPM) Federal Investigative Services (FTS) Fingerprint Transaction System (FTS) via the U.S. DHS Redundant Trusted Internet Connection (DHS RTIC)*; and
- *Final MOU between the U.S. Office of Personnel Management (OPM) Federal Investi*gative *Services Division and the DHS for Electronic Delivery (eDelivery)*.

The provisioning and de-provisioning of IDMS roles 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 or PCIF Manager;
- Have received a favorable background investigation and granted suitability by a DHS or Component PERSEC 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[20] 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 OPM FIS-FTS interface. An electronic audit report can be generated to determine and verify authorized access to information as needed.

Responsible Official

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

Approval Signature

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

_____

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

[20] In-person training is provided in some instances when Operational Components requests it from the DHS PIV Card Issuer. In these instances, the DHS PIV Card Issuer coordinates in-person training with a member from the DHS PIV Card Issuer team. The majority of training is performed online through the DHS PIV Card Issuer SharePoint site.

APPENDIX A

Data Elements	OPM FIS-FTS
Name (first, middle, last)	X
Social Security number (SSN)	X
Agency (e.g. DHS)	X
Organization Affiliation (e.g. FEMA)	X
Employee Affiliation (employee or contractor)	X
Fingerprint Biometric	X
Race	X
Gender	X
Height	X
Weight	X
Eye Color	X
Hair Color	X
Transaction Control Number	X
Originating Agency Identifier (ORI)	X
Controlling Agency Identifier (CRI)	X
Type of Transaction (TOT)	X
Type of Search Requested (TSR)	X
Retention Code	X