Version Number: 01-2015

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
Personal Identity Verification System/Card Management System
(HSPD-12-PIVS/CMS)

Reviewed by: John B. Owens II, Senior Agency Official for Privacy

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO HSPD-12-PIVS/CMS

Unique Project Identifier: PTOI-007-00

Introduction: System Description

The Personal Identity Verification System/Card Management System (HSPD-12-PIVS/CMS) is a Major Application that supports the process of issuing secure identification (ID) cards for the United States Patent and Trademark Office's (USPTO).

The system was developed to implement the requirements of Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. This directive requires all federal agencies develop and implement a standardized process for verifying the identity of employees and contractors prior to issuing an ID card. To provide guidance on how to implement HSPD-12, the National Institute for Standards and Technology (NIST) developed Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors.

In order to comply with HSPD-12 and FIPS 201, USPTO leveraged a COTS product from the FIPS 201-approved product list and the list of qualified HSPD-12 Service Providers to develop HSPD-12-PIVS/CMS. The system employs uniform standards and policies for issuing identity credentials as defined in HSPD-12 and FIPS 201. The PIV Card issuance process includes five steps encompassing discrete activities and data collection. These steps are described in further detail in the below questionnaire and include sponsorship, enrollment, investigation, security review, and issuance and activation. This process for issuance applies to all USPTO employees and contractors.

The HSPD-12-PIVS/CMS system includes a stand-alone computer, related identity management software and various peripheral devices for capturing photos and fingerprints, printing the PIV card, and loading it with certain personal or assigned data for identification and other security purposes. The process for sending electronic fingerprint information to the Federal Bureau of Investigation (FBI) is performed separately from HSPD-12-PIVS/CMS System. HSPD-12-PIVS/CMS also integrates with both the physical and logical access control systems to ensure the USPTO facilities and information systems are accessed by authorized personnel.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☒ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	e. File/Case ID	☐	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify): N/A – the only identifying number collected for PIV card sponsorship is the individual's USPTO employee ID number.					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: N/A - HSPD-12-PIVS/CMS does not collect, store or process Social Security Numbers (SSNs).					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: N/A					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☒	m. Religion	☐
b. Maiden Name	☒	h. Place of Birth	☒	n. Financial Information	☐
c. Alias	☐	i. Home Address	☒	o. Medical Information	☐
d. Gender	☒	j. Telephone Number	☒	p. Military Service	☐
e. Age	☒	k. Email Address	☒	q. Physical Characteristics	☒
f. Race/Ethnicity	☒	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☐	d. Telephone Number	☒	g. Salary	☐
b. Job Title	☐	e. Email Address	☒	h. Work History	☐
c. Work Address	☐	f. Business Associates	☐		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☒	d. Photographs	☒	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☐	c. Date/Time of Access	☐	e. ID Files Accessed	☐
b. IP Address	☐	d. Queries Run	☐	f. Contents of Files	☐
g. Other system administration/audit data (specify):					

Other Information (specify) See table below for summary of the information collected.

Information Collected	**PIV Card Sponsorship**	**Identity Proofing and Registration**	**HSPD-12-PIVS/CMS (Electronically Stored)**	**PIV Card (Physically Displayed)**	**PIV Card (Electronically Stored)**
Full Name	X	X	X	X	X
Date of birth	X		X		
Place of birth	X				
User Principal Name (UPN)	X				
Citizenship	X	X			
Other identifying information (height, weight, hair color, eye color, gender)		X	X		
Organizational affiliation (e.g. Agency name)	X	X	X	X	X
Employee affiliation (e.g. Contractor, Active Duty, Civilian)		X	X	X	X
USPTO Employee ID Number	X				
New Hire (Yes or No)	X				
Biometric identifiers (2 fingerprints)		X	X		X
Digital color photograph		X	X	X	
Digital signature[1]					X
Telephone numbers			X		
Email Address	X				
Name of Specialist (Sponsor)	X				
Emergency Response Official (Yes or No)	X				

[1] Public key infrastructure (PKI) digital certificate with an asymmetric key pair.

Background Investigation (BI) (Yes or No)	X				
Date BI Completed	X				
BI Result	X				
BI Completed By	X				
BI Type	X				
BI Comments	X				
Signed PIV Request		X			
Copies of identity source documents		X			

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☒	Hard Copy: Mail/Fax	☐	Online	☒
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☒
State, Local, Tribal	☐	Foreign	☐		
Other (specify): Investigation: The PIV background investigation, as required by FIPS 201, is a condition of Federal employment and contract employment. The PIV Applicants' information is submitted to the FBI and Office of Personal Management (OPM) databases to prevent the hiring of applicants with a criminal record or possible ties to terrorism. Fingerprint information is obtained as part of the HSPD-12 card processing, but this information will NOT be stored or maintained in the system. Fingerprint information is submitted to the FBI outside the HSPD-12 system, and background information is submitted to OPM through OPM's system (e-QIP).					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify): N/A					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	☐	For administering human resources programs	☐
For administrative matters	☐	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify): Intended use of the data is to identify and validate an employee's biographic data in order to issue them a valid government PIV card which contains pertinent applicant data required by FIPS 201, such as name, agency, photo image, etc. The biographic and biometric information collected are used to conduct a background investigation that includes a criminal history record check. The fingerprints are used to verify the identity of the credential holder, and the facial image is collected, so it can be printed on the PIV Card as a means to identify the cardholder. While FBI Criminal Fingerprint check results are obtained as a part of the HSPD-12 card processing, this information is not stored or maintained by HSPD-12-PIVS/CMS. Additionally, biometric minutiae data is deposited onto secure			

containers within the PIV Cards in accordance with the requirements from FIPS 201-1 and NIST Special Publication (SP) 800-76. This data is also stored on USPTO data center servers once the PIV Cards are manufactured and provided to the Card Applicants.

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Intended use of the data is to identify and validate an employee's biographic data in order to issue them a valid government PIV card which contains pertinent applicant data required by FIPS 201, such as name, agency, photo image, etc.

The biographic and biometric information collected are used to conduct a background investigation that includes a criminal history record check. The fingerprints are used to verify the identity of the credential holder, and the facial image is collected, so it can be printed on the PIV Card as a means to identify the cardholder. While FBI Criminal Fingerprint check results are obtained as a part of the HSPD-12 card processing, this information is not stored or maintained by HSPD-12-PIVS/CMS. Additionally, biometric minutiae data is deposited onto secure containers within the PIV Cards in accordance with the requirements from FIPS 201-1 and NIST Special Publication (SP) 800-76. This data is also stored on USPTO data center servers once the PIV Cards are manufactured and provided to the Card Applicants.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☒	☐	☒
DOC bureaus	☐	☐	☐
Federal agencies	☒	☐	☒
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☐	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
☒	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://ptoweb.uspto.gov/ptointranet/ptosecurity/hspd/PIV_privacy_notice.pdf	
☒	Yes, notice is provided by other means.	The PIV Card Issuance Privacy Notice is posted in the USPTO Security Services Center where cards will be issued and is also posted on the USPTO intranet. Additionally, each card applicant is provided a copy of this PIV Card Issuance Privacy Notice at the time of their enrollment. The PIV process employs a Web-based electronic enrollment form. The applicant, at the time of enrollment, is verbally informed of the purpose of the collected data and has the ability to obtain a privacy notice sheet. They are notified how the collected data will be used to create a PIV card, legal authority for doing so, and other uses of the collected data. In addition, the applicant signature page will identify they have read the privacy implications of the collected personal data, and understand the implications and purpose of the data.
☐	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Information is provided on a voluntary basis. While providing this information is voluntary, if personnel do not provide the requested information in whole or in part, USPTO may not be able to complete their investigation or the identity and registration process, or complete it in a timely manner. Failure to provide the requested information may affect their placement or employment, and will affect their ability to obtain a permanent PIV card. If using a PIV credential is a condition of their job, not providing the information will affect their placement or employment prospects.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Information is provided on a voluntary basis. While providing this information is voluntary, if personnel do not provide the requested information in whole or in part, USPTO may not be able to complete their investigation or the identity and registration process, or complete it in a timely manner. Failure to provide the requested information may affect their placement or employment, and will affect their ability to obtain a permanent PIV card. If using a PIV credential is a condition of their job, not providing the information will affect their placement or employment prospects.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Through the electronic Web-based portal of the HSPD-12-PIVS/CMS system
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: HSPD-12-PIVS/CMS relies on the Enterprise Monitoring and Security Operations for its auditing capability. Suspicious system log behavior and log failures are reported to the appropriate personnel to troubleshoot and remediate the issue.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 01/17/2015 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).

☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Information in HSPD-12-PIVS/CMS is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards. A System Security Plan (SSP) has been developed in accordance with the NIST SP 800-18 that describes the security controls in place or planned as derived from NIST SP 800-53, Revision 4. Assessments are performed to determine the effectiveness of these controls and include recommended remediation actions for any system vulnerabilities. Access is restricted on a "need to know" basis, utilization of HSPD-12 card access, secure network access, and card readers on doors and approved storage containers. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. Personally identifiable information is safeguarded and protected in conformance with all Federal statutory and OMB guidance requirements. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All data is encrypted in transit. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. Persons given roles in the HSPD-12 process must be approved by the USPTO and complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information. Additionally, HSPD-12-PIVS/CMS leverages technologies from the FIPS 201-approved product list (http://www.idmanagement.gov/approved-products-list) and the list of qualified HSPD-12 Service Provider (http://www.idmanagement.gov/qualified-hspd-12-service-providers). These products and services have been validated by GSA as compliant with FIPS 201 specifications.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/ PAT–TM–18 USPTO Identification and Security Access Control Systems
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: HSPD-12-PIVS/CMS follows the NARA guidelines and USPTO document retention policies. Current retention policies are to keep electronic badge information for two years after an individual has departed the agency. HSPD-12 records are purged after a two year period to keep uniformity between legacy badges and HSPD-12 cards. The record retention procedures are documented in the USPTO PIV Card Issuers Operations Plan.
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☐	Overwriting	☐
Degaussing	☐	Deleting	☐
Other (specify): HSPD-12 records are purged after a two year period to keep uniformity between legacy badges and HSPD-12 cards. The record retention procedures are documented in the USPTO PIV Card Issuers Operations Plan.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

☒	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

☐	Identifiability	Provide explanation:
☐	Quantity of PII	Provide explanation:
☒	Data Field Sensitivity	Provide explanation: This is done in accordance to USPTO policy (IT Security Handbook)
☒	Context of Use	Provide explanation: This is done in accordance to USPTO policy (IT Security Handbook)
☒	Obligation to Protect Confidentiality	Provide explanation: This is done in accordance to USPTO policy (IT Security Handbook)
☒	Access to and Location of PII	Provide explanation: This is done in accordance to USPTO policy (IT Security Handbook)
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.