Version Number: 09-2016

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

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

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Personal Identity Verification System Card Management System

Unique Project Identifier: PTOI-007-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Senior Agency Official for Privacy (SAOP).

Description of the information system and its purpose: *Provide a general description of the information system and its purpose in a way that a non-technical person can understand.*
The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

Questionnaire:

1. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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):					

☒ This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☒ Yes. *Please describe the activities which may raise privacy concerns.*

Each step of the PIV credentialing process as described below:

1. Sponsorship: During the sponsorship step, a portion of the applicant's personal information is collected including name, contact information, birth history, and affiliation with the sponsoring organization.

2. Enrollment: During enrollment, two key identity and vetting processes are performed: 1) establishing the applicant's identity, and 2) capturing and validating the applicant's identity data. During this identity proofing process, the applicant is required to appear in person and provide two forms of identification:

a. One State or Federal government issued photo ID, and
b. One other document from the list of documents on Form I-9, OMB No. 1115-0136, Employment Eligibility Verification.

3. Investigation: 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).

4. Security Review: During the processing of any credential application, security concerns that require comments or approval from a USPTO Security Officer may be identified. Security reviews are documented to ensure both the applicant and USPTO have the requisite audit trail in the event a credential is denied.

5. Issuance: The process of issuing a credential includes the following steps:

a. Printing: The physical printing of the card, including the logos, photograph, expiration date, and hologram.
b. Encoding: The electronic encoding of the card which places the fingerprints, photograph, public key infrastructure (PKI) certificates, and other information on the smart chip.
c. Activation: The process of the applicant accepting the new credential and choosing and entering a PIN.

Activation requires the applicant to appear in-person to meet with the Issuance Officer. The applicant is required to provide one or more fingerprints for comparison and validation against the fingerprints captured during enrollment. At the completion of the Activation stage, the applicant is issued a smartcard credential.

☐ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

☐ Companies

☐ Other business entities

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Personal Identity Verification System Card Management System (HSPD12-PIVS/CMS) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of System Owner (SO): Jimmy Orona III

Signature of SO: Users, Orona, Jimmy III Digitally signed by Users, Orona, Jimmy III DN: dc=gov, dc=USPTO, cn=Users, cn=Orona, Jimmy III Date: 2017.11.15 14:13:44 -05'00' Date: _____

Name of Senior Information Security Officer (SISO): for Rami Dillon

Signature of SISO: S. D. Ramsingh Date: 11/15/2017.

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): David Chiles

Signature of AO & BCPO: [signature] Date: 11/27/2017