PRIVACY IMPACT ASSESSMENT (PIA) FOR:

THE FEDERAL TRADE COMMISSION
PERSONAL IDENTITY VERIFICATION (PIV) SYSTEM

February 2008

INTRODUCTION

Program Overview

Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, mandates the establishment of a standard for identification of Federal Government employees and contractors. HSPD-12 directs the use of a common identification credential – a Personal Identity Verification (PIV) card, more commonly known as an ID badge – for both logical and physical access to Federally controlled facilities and information systems. This policy is intended to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

HSPD-12 requires that the Federal credential be secure and reliable. A secure and reliable credential is defined by the Department of Commerce (DOC) as a credential that:

- Is issued based on sound criteria for verifying an individual's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Is issued only by providers whose reliability has been established by an official accreditation process.

The National Institute of Standards and Technology (NIST) was tasked with producing a standard for secure and reliable forms of identification. In response, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, issued on February 25, 2005. The FIPS 201 PIV credential is to be used for both physical and logical access, as well as other applications as determined by the individual agencies.

FIPS 201 consists of two parts: PIV-I and PIV-II. The standards in PIV-I support the control objectives and security requirements described in FIPS 201, including the standard background investigation required for all Federal employees and long-term contractors. The standards in PIV-II support the technical interoperability requirements described in HSPD-12. PIV-II also specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards) for use in a Federal PIV system. Simply stated, FIPS 201 requires the Federal Trade Commission (FTC) to:

- Establish new roles to facilitate identity proofing, information capture and storage, card issuance and maintenance, and privacy concerns;
- Develop and implement a new physical and technical infrastructure; and
- Establish processes to support the FTC's implementation of a PIV system.

In response to HSPD-12 and to meet the requirements summarized above, the FTC established the Joint Office of Identification and Credentialing (JOIC) under the FTC's Chief Security Officer. JOIC is responsible for the identity management and all aspects of the FTC HSPD-12 implementation, including serving as the main internal and external point of contact with respect to program planning, operations, business management, communications, and technical strategy.

The FTC's PIV System

As required by the Office of Management and Budget (OMB), this Privacy Impact Assessment (PIA) explains the privacy impact of the electronic information technology (IT) that the FTC has developed or acquired to collect and maintain information about individuals (e.g., employees, long-term contractors, interns) who need to be issued HSPD-12 credentials (PIV cards) for obtaining physical or logical access to agency resources (e.g., FTC buildings, computer networks). The FTC's PIV system, in accordance with the model prescribed by section 3.1 of FIPS 201, consists of the following PIV subsystems and related IT and IT processes:

- *The PIV "front-end" subsystem.* This includes the PIV card issued to the individual, the card and biometric readers used by the FTC, and any additional devices that the individual may be required to use or interact with in order to gain physical or logical access to FTC resources (e.g., a device for the cardholder to input a personal identification number (PIN) at a computer workstation or entry door).[1]

- *The PIV "card issuance and management" subsystem.* This refers to the FTC's process of collecting, storing, and maintaining all information and documentation required for verifying and assuring the applicant's identity, and for issuing and managing the control data associated with the PIV card. The IT used by the FTC for this PIV card issuance and management process is collectively referred to in this PIA as the Identity Management System (IDMS). The FTC's IDMS 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 (e.g., digital "key") for identification and other security purposes. For security purposes (see section 6 of this PIA), PIV data captured or generated by the IDMS are not maintained on or accessible through the FTC's agency-wide computer network. Instead, IDMS data are collected by FTC IT equipment used solely for the IDMS and transmitted using a dedicated "T-1" connection (i.e., a special type of telephone line for secure digital communication and transmission) to an off-site FTC vendor, currently Operation Research Consultants (ORC) for secure storage and management.

The FTC relies on additional IT equipment or services for the background investigation aspect of the PIV card issuance process. The FTC Personnel Security Office utilizes a commercial electronic fingerprint scanner (currently Cross Match Live Scan ID) to collect fingerprints and

[1] The FTC also relies upon various building security systems (e.g., security cameras, videotaping) in its facilities to monitor and record entry and exit of individuals. These systems do not appear to be directly covered by FIPS 201 or other guidance issued under HSPD-12, but we make note of these systems here since information collected by these systems (e.g., video, including time and date logs) could be used with other PIV-related data (e.g., PIV card data collected by front-end devices and associated logs) to identify individuals.

transmit them with related identifying data to the Office of Personnel Management (OPM) Center for Federal Investigative Services, which conducts a fingerprint check on the FTC's behalf against the Federal Bureau of Investigation (FBI) fingerprint database.[2] The FTC Personnel Security Office also utilizes proprietary IT (currently Intellitrac Personnel Security Software) to monitor the required background investigation process from start to finish for each individual who does not have a suitable, current Federal background investigation on file (e.g., a new hire who has never worked for the U.S. Government or an employee whose background check is over 15 years old).[3]

- *The "access control" subsystem.* Under FIPS 201, this refers to the data (e.g., a list of authorized individuals) used to grant or deny access to physical or logical resources when that data are matched against PIV data collected from the individual's PIV card by a front-end device (see above). It also includes data (e.g., digital keys) that are used to verify the authenticity of the PIV card when it is presented to a front-end device. These access control data may be stored electronically on the access control device (e.g., door entry system) or elsewhere.

PIA Scope

This PIA provides detail about the FTC's role in the collection and management of personally identifiable information for the purpose of issuing credentials (PIV cards) to meet the requirements of HSPD-12 and to comply with the standards outlined in FIPS 201 and its accompanying special publications. HSPD-12 requires standardized and secure processes for personal identity verification through the use of advanced and interoperable technology. This resulted in a need to collect biographic and biometric information. This PIA covers the information collected, used, and maintained for these processes, specifically the: (a) background investigation; (b) identity proofing and registration; (c) Identity Management System (IDMS), the database used for identity management and access control; and (d) the PIV card.

As noted previously, PIV-I requires the implementation of registration, identity proofing, and issuance procedures compliant with the standards of FIPS 201; however, the collection of information for background investigations has been a long-standing requirement for Federal employment. This process and the elements used are not new. The forms and information collection for the background investigation process remain the same. Additionally, PIV-I does not require the implementation of any new systems or technology. The FTC will continue to issue existing ID badges under PIV-I, but the process for credential application and issuance will conform to requirements of HSPD-12 and FIPS 201.

---

[2] The FTC submits fingerprints securely through OPM's Fingerprint Transaction System (FTS), so that they can be verified against fingerprint records in the FBI's Integrated Automated Fingerprint Identification System (IAFIS) operated by the FBI's Criminal Justice Information Services Division. See http://foia.fbi.gov/iafis.htm. To read about OPM's FTS program, including security controls and procedures, see OPM's description at http://www.opm.gov/extra/investigate/Fin-2004/fin04-02.asp (Federal Investigative Notice 04-02) and http://www.opm.gov/extra/investigate/Fin-2000/fin0004.asp (Federal Investigative Notice 00-04).

[3] In some cases, individuals complete and submit certain required OPM background investigation forms or supporting documents online through OPM's e-QIP (Electronic Questionnaires for Investigative Processing) Web site. OPM has posted a separate PIA for that system. See http://www.opm.gov/privacy/pia_eqip.asp (e-QIP PIA).

This PIA covers both the PIV-I and PIV-II processes. These processes will be referred to throughout this PIA as the FTC PIV program and the credentials issued referred to as PIV cards.

Basic Program Control Elements

There are four control objectives of the PIV program: Secure and reliable forms of identification for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identify fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

Each agency's PIV implementation must meet the four control objects such that:

- Credentials are only issued (a) to individuals whose true identity has been verified, and (b) after a proper authority has authorized issuance of the credential.
- Only an individual with a completed background investigation on record is issued a credential.
- An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or state government picture ID.
- Fraudulent or altered identity source documents are not accepted as genuine.
- A person suspected or known to the Government as a terrorist is not issued a credential.
- No substitution occurs in the identity-proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked, is the person to whom the credential is issued.
- No credential is issued unless requested by a proper sponsor.
- A credential remains serviceable only up to its expiration date. A revocation process exists whereby expired or invalidated credentials are swiftly revoked.
- A single corrupt official in the process cannot issue a credential with an incorrect identity or to a person not entitled to the credential.
- An issued credential is not modified, duplicated, or forged.

SECTION 1.0 INFORMATION COLLECTED AND USED IN THE PIV PROGRAM

1.1 What information is collected and from whom?

The information is collected from PIV Applicants, the individuals to whom a PIV card is issued. The PIV Applicant may be a current or prospective Federal hire, Federal employee, or a contractor for the FTC or for the Federal Mine Safety and Health Review Commission (FMSHRC). (See Section 3.2.) As required by FIPS 201, the FTC will collect biographic and biometric information from the PIV Applicant in order to: (a) conduct the background investigation or other national security investigation; (b) complete the identity proofing and registration process; (c) create a data record in the PIV Identity Management System (IDMS); and (d) issue a PIV card. Figure 1 below depicts what information is collected from the PIV Applicant in relation to each of these processes.

Figure 1: The Collection, Storage, and Use of Information from the PIV Applicant

	Background Investigation	Identity Proofing and Registration	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)
Date of birth	X		X		
Place of birth	X				
Social Security Number (SSN)	X	X			
Other names used	X				
Citizenship	X	X		Stripe for foreign national	
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	X
Fingerprints (10)	X				
Biometric identifiers (2 fingerprints)		X	X		X
Digital color photograph		X	X	X	
Digital signature [4]					X
Telephone numbers	X		X		
Spouse (current or former), relatives and associates, information regarding their citizenship	X				
Marital status	X				
Employment history	X				
Address history	X				
Educational history	X				
Personal references	X				
Military history/record	X				
Illegal drug history	X				
Criminal history	X				
Foreign countries visited	X				
Background investigations history	X				
Financial history	X				
Association history	X				
Signed PIV Request		X			
Signed SF 85 or equivalent	X				
Copies of identity source documents		X			

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

1.2 What is the information used for?

The information identified above is used in each step of the PIV process as described below:

1. **Conduct a background investigation.** The PIV background investigation, as required by FIPS 201 is a condition of Federal employment (now extended to contractors) and matches PIV Applicants' information against FBI, OPM, and FTC databases to prevent the hiring of applicants with a criminal record or possible ties to terrorism. If persons decline providing this information, they cannot be hired as a permanent employee, nor work at the agency as a contractor long-term (over six months). Three forms are used to initiate the background investigation: Questionnaire for Non-Sensitive Positions Standard Form 85 (SF-85); Questionnaire for Public Trust Positions Standard Form 85P (SF-85P); or the Questionnaire for National Security Positions Standard Form 86 (SF-86). This process entails conducting a minimum National Agency Check with Inquiries (NACI), described below:

   - **NACI:** The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquires and searches of records covering specific areas of an individual's background during the past five years.

     Note: A PIV card can be issued temporarily on the basis of a favorable National Agency Check (NAC). This portion of the NACI investigations is usually returned to the agency within one week of the submission of the fingerprints.

   - **NAC:** Consists of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary.

     Note: The background information collected as part of these processes and their results are kept in the Applicant's background investigation files and not stored on the PIV card.

2. **Complete the identity proofing and registration process.** The biographic information collected as part of this process is utilized to establish the PIV Applicant's identity. Biometrics are used to ensure PIV Applicants have not been previously enrolled in the FTC PIV system. As part of this process, FIPS 201 requires that Applicants provide two forms of identity source documents in original form. The identity source documents must be derived from the list of acceptable documents included in Form I-9, OMB No. 115-0316, Employment Eligibility Verification.[5] PIV Applicants will also participate in an electronic signature process conforming to the Electronic Signature (ESIGN) Act. This confirms: presentation of and agreement with the privacy notice; the intent to participate in the PIV process, and consent to submit to a named-based threat background check as required depending on job requirements.

[5] Form I-9 can be downloaded at: http://uscis.gov/graphics/formsfee/forms/i-9.htm

3. **Create a data record in the PIV Identity Management System (IDMS).** The IDMS is used during the registration process to create the PIV Applicant's pre-enrollment and enrollment record, to manage and maintain this information throughout the PIV card lifecycle, and to verify, authenticate, and revoke PIV cardholder access to Federal resources. A unique identifier is assigned during registration and used to represent the individual's identity and associated attributes stored in the system.
4. **Issue a PIV card.** A PIV card is issued upon successful completion of the background investigation, identity proofing and registration process, and the enrollment process. Biometrics are used during PIV card issuance to verify PIV Applicant identity and to complete activation of the card. This provides much stronger security assurances than typical card activation protections such as PINs or passwords. Once the individual has been issued a PIV card, the IDMS is updated to reflect that the card has been issued.
5. **Use the PIV card for physical and logical access.** The biometrics collected are utilized to verify that the rightful cardholder is presenting the card for physical and logical access to Federal facilities and IT resources. Biographic and other information displayed on the PIV card is visually inspected by security guards for identity verification purposes. The electronically stored information is used by FTC access control systems to grant access privileges.

1.3 What other information is stored, collected, or used?

The FTC PIV IDMS and PIV cards contain other data not collected from the PIV Applicant that are either: (a) electronically stored on the card; (b) electronically stored in the IDMS; and/or (c) physically displayed on the card. This information and the purpose of its use are described below in Figure 2.

Figure 2: Other PIV Information Stored, Collected, or Used

	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)	Purpose
Card expiration date	X	X	X	To verify that card is valid and allow access to facilities and computer systems.
Personal Identification Number (PIN)			X	For optional/selected use either for physical access to highly secured FTC buildings/space or to log-on to FTC computer systems that require multi-factor authentication, beyond the typical user ID/password.
Agency card serial number	X	X		For identifying and maintaining agency cards
Issuer identification number	X	X		To verify issuer's authority.
Contact Integrated Circuit Chip (ICC)			X	Used to authenticate a PIV cardholder's identity with card readers that require cards to be inserted or "swiped". Can be used for physical access to buildings/office space and logical access to computer systems.
Contactless ICC			X	Used to authenticate a PIV cardholder's identity with low-frequency radio signal "proximity loop" card readers that allow a card to pass by the card reader. Primary use is for physical access to buildings and office space.
PIV authentication key			X	Used to authenticate the PIV card to the host computer system in relation to validating a PIV cardholder's identity.
Cardholder Unique Identifier [Federal Agency Smart Card Credential Number (FASC-N)			X	Used to authenticate the cardholder to the host computer system, and is comprised of the agency code plus a sequential number for the employee, creating a unique number for all Federal employees. This allows interoperability of the PIV card throughout the Federal Government.
PIV Registrar Approval (digital signature)			X	Used to verify the authenticity of the individual sending the message, and verifies that the content has not been altered.

1.4 Does the PIV program utilize or depend on the use of commercial databases or commercially available data?

Yes. The FTC PIV program utilizes background investigations that are conducted by the OPM, which utilizes commercial credit checking databases (e.g., TransUnion, Equifax, Experian). Credit report data are included in the packet returned by OPM to FTC for final adjudication.[6]

1.5 Will new or previously unavailable information about an individual be obtained or generated? If so, what will be done with the newly derived information? Will it be placed in the individual's existing record? Will it be placed in an existing system of records? Will a new system of records be created? Will the agency use the newly obtained information to make determinations about the individual? If so, explain fully under what circumstances that information is used and by whom.

The FTC currently conducts background checks on all of its employees, but the HSPD-12 process will not be collecting any new information that is not currently collected by the FTC on such individuals.

1.6. What privacy risks did the agency identify regarding the amount and type of information to be collected? Describe how the agency mitigates those risks.

The FTC has identified privacy risks associated with the amount and type of information collected by the FTC. The two parts of the HSPD-12 process (PIV-1 and PIV-2) require that a significant amount of sensitive personal identifying information be collected from or about individuals in order to check their backgrounds, verify their identities, and issue PIV cards that will be accepted Government-wide under the HSPD-12 program. This information includes, for example, fingerprints, an OPM check into the individual's credit history, and FTC request and inspection of personal identification documents (e.g., passport or other government-issued identification). The risk is that this information may be misused or disclosed for an unauthorized purpose.

The FTC mitigates this risk in various ways, as described further in the security discussion of this PIA. For example, we require all employees and contractors involved with data collection, processing, and use, as well as technical support of the FTC personnel security system, to pass a security clearance. All contractors are required to sign a non-disclosure agreement.

We provide access to HSPD-12 records and data only to authorized members of the FTC Security staff and its contractors. Each staff member is assigned a unique user name and password (passwords must be strong: at least eight characters; contain a mix of letters, numbers, and special characters; and not be based on a word in any language, slang or jargon). Paper records are stored in locked filing cabinets in a locked office occupied by the Personnel Security Staff.

[6] The FTC also consults commercial credit reporting databases (e.g., Equifax) when conducting background checks to issue non-HSPD-12 credentials (e.g., FTC building pass or placement on a 90-day access list) to other vendors or government personnel with frequent FTC business to have temporary, unescorted access only to the FTC's facilities.

Information transmitted to OPM and the FBI is provided to specific offices at those agencies that are authorized to conduct background investigations.

Access to the FTC Intellitrac Personnel Security software is limited to the Personnel Security staff and authorized FTC IT staff, and is controlled by multiple layers of security controls. External access to the application is protected by a firewall.

The electronic information stored on the PIV card is encrypted using standards and protocols issued by the National Institute of Standards and Technology (NIST) and also housed in an electromagnetic sheath to prevent skimming.

Access to the ORC database is controlled by multiple layers of security and a firewall. Personnel working on the ORC database sign nondisclosure agreements.

In addition, the FTC has determined that it will load and store the minimum amount of personal data on the PIV cards needed to make them compliant with HSPD-12 standards, even though the standards allow for additional data to be stored and displayed on the cards. The FTC believes that this approach minimizes the risk of a data loss in the event that a card is lost or stolen. Likewise, the FTC issues carrying sleeves for the cards, so that information cannot be "skimmed" or read by any portable scanners or other unauthorized equipment.

SECTION 2.0 INTERNAL SHARING AND DISCLOSURE

2.1 What information is shared with which internal organizations and what is the purpose?

The information is shared only with the appropriate FTC employees and contractors involved in the design, development, implementation and execution of the FTC PIV program who, by law and contract, are bound by the Privacy Act of 1974. Specific information about a PIV Applicant or Cardholder is shared with FTC employees and its contractors who have a "need to know" for implementation of the FTC PIV Program. FTC contractors are contractually obligated to comply with the Privacy Act in the handling, use, and dissemination of all personal information.

SECTION 3.0 EXTERNAL SHARING AND DISCLOSURE

3.1 What information is shared with which external organizations and what is the purpose?

As described earlier, during the up-front background investigation process (PIV-I) and identity proofing, relevant personal data will be:

1. Shared with OPM, which is responsible for conducting the NACI and other higher-level investigations for the FTC; and
2. Matched against databases at the FBI and OPM to prevent the hiring of applicants with a criminal record or possible ties to terrorism.

Additionally, information about individuals that is stored for purposes of issuing a PIV card and to run the FTC PIV program may be provided to an external organization without individual's consent as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a(b)). This information may be provided to:

- an appropriate government law enforcement entity if records show a violation or potential violation of law;
- the Department of Justice, a court, or other adjudicative body when the records are relevant and necessary to a law suit;
- a Federal, state, local, tribal, or foreign agency whose records could facilitate a decision whether to retain an employee, continue a security clearance, or agree to a contract;
- a Member of Congress or to Congressional staff at a constituent's written request; to OMB to evaluate private relief legislation;
- agency contractors, grantees, or volunteers, who need access to the records to do agency work and who have agreed to comply with the Privacy Act;
- the National Archives and Records Administration for records management inspections; and
- Other Federal agencies for notification when a PIV card is no longer valid.

3.2 Is the FTC either providing or receiving card issuance services pursuant to a serving agreement?

Yes. The FTC provides HSPD-12 IDMS services to Federal agency tenants at its 601 New Jersey Avenue, N.W., Washington, DC, location. The tenant, FMSHRC, has authorized the FTC to perform NACI checks on it employees and reimburses the FTC by written agreement. The potential privacy risks are the same ones identified in Section 1.6. The FTC has created a section in its paper copy filing system for the HSPD-12 files associated with FMSHRC. No copies of the background checks for FMSHRC are maintained on the FTC Intellitrac Personnel Security software. The same steps taken to mitigate the potential privacy risk in Section 1.6 are the same used for this section.

SECTION 4.0 AGENCY POLICY REQUIREMENTS

The FTC's JOIC has established certain policies and for those officials and staff who have roles in the FTC's HSPD-12 program. For example, all FTC HSPD-12 Registrars have completed HSPD-12 overview training, Registrar training and personnel suitability adjudication training. All Registrars also have completed sensitive background Investigations (SBI).

All HSPD-12 Issuers have, at a minimum, a completed NACI background check. They have completed the HSPD-12 overview training and additional Issuer training provided by the FTC Security Office. All Sponsors have minimum NACI background investigations. They also have completed HSPD-12 overview training and HSPD-12 Sponsor training. All Applicants have completed HSPD-12 overview training.

Finally, all FTC personnel who work on HSPD-12 are subject to FTC agency-wide procedures for safeguarding sensitive personally identifiable information and sensitive health information.

All FTC personnel also receive annual computer-based training and other guidance explaining how to safeguard this information.

SECTION 5.0 PRIVACY ACT REQUIREMENTS

5.1 Is notice provided to the individual at the time information is collected? If yes, provide or attach the Privacy Act Statement. If notice is not provided, why not?

PIV Applicants are provided notices required by the Privacy Act, 5 U.S.C. 552(a)(e)(3) when FTC (and OPM) forms are used to collect information from individuals. The notices state the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. (Copies of the notices appear on the forms themselves, rather than as an attachment to this PIA.) PIV Applicants using an electronic signature process conforming to the Electronic Signature (ESIGN) Act confirm presentation of and agreement with the Privacy Act statement, agree to participate in the PIV process and submit to a background check appropriate to job requirements.

The collection, maintenance, and disclosure of information comply with the Privacy Act and the published System of Records Notice(s) (SORN) for the records and data collected, generated and maintained as part of the HSPD-12 process (FTC II-11, Personnel Security Files). That SORN is being updated and will be posted publicly. See http://www.ftc.gov/foia/listofpaysystems.shtm.

5.2 What are the procedures for individuals to gain access to their own information?

The FTC Personnel Security Office tracks and reviews the SF 85, 85P, 86 prior to submission to OPM. (Individuals wishing to obtain copies of their completed forms can request it from the FTC Personnel Security Office.) These forms are completed by the individual undergoing the background investigation/clearance. Individuals are able to correct erroneous information prior to submittal. Once the data has been submitted to the FTC Personnel Security Office for suitability review and clearance processing by the Personnel Security Office, individuals must contact either the Personnel Security Office directly or go through Privacy Act/FOIA office to gain access to documents used for the adjudication decision.

Each individual has the ability to address and provide mitigating information related to any derogatory information that is identified as part of his or her background investigation. Individuals are notified of any pending actions based on derogatory information, and are provided a mechanism to respond to derogatory information. If a derogatory finding is made, the individual has appeal rights, and also has the ability to request information regarding his or her case via the FTC Freedom of Information Act (FOIA) office.

5.3 What are the procedures for correcting information?

The information obtained by the FTC Personnel Security Office is from data provided directly by the individual. The background investigations process obtains information from many sources to verify or supplement the information that was submitted by the individual, which then becomes the basis for determining whether the individual has met suitability requirements for a PIV card.

Individuals are notified in writing when the FTC is prepared to make a derogatory finding based on the information at hand. The written notice advises the individual about the mechanism for challenging the derogatory information. This process is in addition to any rights to access and correct their information by submitting a formal request through the agency's FOIA/Privacy Act office.

5.4 How are individuals notified of the procedures for correcting their information?

The specific procedures for an individual to view and request changes depend on the findings and the type of case. As noted above, individuals are notified in writing when the FTC is prepared to make a derogatory finding based on the information at hand. The written notice explains to the individual the mechanism for him or her to challenge the derogatory information.

The individual will also be notified, based on a review of the individual's response, whether the derogatory information will result in a change to their background check/clearance status. If clearance is suspended or revoked, the individual will be notified in writing and be provided with the specific information regarding appeal rights and due process. Additional instructions are provided on related security forms regarding changes or updates to data that may be required after submission.

5.5 If no opportunity to amend is provided, what alternatives are available to the individual?

Not Applicable.

5.6 Do individuals have the right to decline to provide information?

Individuals may opt to not provide information; however, they cannot meet suitability requirements if they decline and are therefore ineligible for Federal service.

By signing the PIV application form, Applicants acknowledge that FTC may use their information as outlined in the Privacy Act statement and associated Privacy Act SORN. While there is no legal requirement to use a PIV card, employees who do not use a PIV card will be issued a FTC building Pass and may be treated as visitors when entering a Federal building. Employees will be barred from access to certain FTC and other Federal resources. If using a PIV card is a condition of the job, withholding requested information will affect job placement or employment prospects.

5.7 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals waive the right to choose how the information will be used on submission of the SF-85, 85P or 86.

Individuals are notified of the uses of their information prior to collection. Once the information is provided, the individual has given consent to the uses. The FTC Personnel Security Office will not use the information outside of the scope of this PIA and the System of Records Notice.

5.8 What deficiencies in your agency procedures did you remedy after performing this analysis?

The FTC did not identify any significant deficiencies on the basis of the above analysis. Our HSPD-12 program ensures that all officials and staff who are assigned roles in the HSPD-12 process complete overview training on the HSPD-12 process. All Sponsors, Registrars and Issuers are further required to go through position-specific training. The data input center for the IDMS is centralized in the FTC Security Office to control access to it.

SECTION 6.0 DATA PROTECTION CONTROLS

6.1 General Program Controls

The FTC has implemented the following for data control:

- An approved identity proofing and registration process.
- A requirement that the Applicant appears in-person at least once before the issuance of a PIV credential.
- Adherence to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.
- Issuance of PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited).
- This comprehensive PIA on systems containing personal information in identifiable form (IIF) for implementing PIV, consistent with the E-Government Act.
- A SORN identifying the type of information collected, the purpose of the collection, how the information is protected, and the complete set of uses of the credential and related information during the life of the credential.
- Assurance that systems containing IIF for the purpose of enabling the implementation of PIV are handled in full compliance with the Privacy Act.
- Ensuring that only personnel with a legitimate need for access to IIF are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.

- Coordination with appropriate department or agency officials to define consequences for violating privacy policies of the PIV program.
- Assurance that the technologies used in the department or agency's implementation of the PIV allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program.
- Categorization of the system risk level (as specified in FIPS 199) and utilization of security controls described in NIST SP800-53, Recommend Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable.
- Ensuring that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form. For example, the FTC employs an electromagnetically opaque sleeve to protect against any unauthorized contact less access to information stored on a PIV credential.

6.2 Specific program controls used to secure information.

What are the controls on data exchange and integrity of the credential?

Operational Research Consultants (ORC) is the FTC contractor that currently provides IDMS service for the FTC, by receiving, managing, controlling and securing the HSPD-12 data collected in the HSPD-12 process by the FTC. According to ORC, the ORC Public Key Infrastructure suite provides technical access controls designed to provide the least access privileges and maximum protections against unauthorized access to system resources. Technical controls have been developed and are implemented in accordance with FIPS Publication 83, Federal law, regulations and guidelines, in addition to General Services Administration (GSA) security policy and supporting security guidelines.

ORC represents that the ORC PKI suite employs proper user authentication and identification methodology. This methodology includes the use of user ID/password, token-based, and/or digital certificate authentication schemes. The use and enforcement of password security is in accordance with GSA security policy and supporting security guidelines.

Individuals filling trusted roles within the ORC facility utilize security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements that check the integrity of the system data, software, discretionary access controls, audit profiles, firmware, and hardware to ensure secure operation.

All assembly and maintenance of Certificate Authority (CA) systems is accomplished in the controlled environment of the Secure Network Operations Center located at ORC headquarters. Only personnel designated in the ORC ACES Certificate Practices Statement perform maintenance on the PKI systems. The Certificate Authority Administrator and Systems Administrator (SA) accomplish hardware and software upgrades.

ORC authorized CA equipment is dedicated to administering a key management infrastructure and does not have installed applications or component software, which are not part of the PKI configuration. Equipment (hardware and software) procured to operate the PKI is purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection. In the event that equipment is developed for the PKI, it shall be developed in a controlled environment and the development process shall be defined and documented.

All Certificate Manufacturing Authority (CMA) hardware and software is shipped or delivered via controlled methods that provide a continuous chain of accountability from the location where it has been identified as supporting a CMA function to the using facility.

For all entities responsible for local registration (including Federal, state and local government agencies/personnel), reasonable care is taken to prevent malicious software from being loaded on any equipment used in the registration process. Only applications required to perform the organization's mission are loaded on these computers, and all such software is obtained from authorized sources. Data on such equipment is scanned for malicious code on first use and periodically afterward. Hardware and software updates are purchased or developed in the same manner as original equipment, and are installed by trusted and trained personnel in a defined manner.

Access to the CA data is protected by a firewall specifically allocated to the protection of the ORC PKI suite. Only required accounts are present on the firewall. HTTPS and Online Certificate Status Protocol (OCSP) requests are the only type of data access that is allowed into the system. OCSP, HTTPS and LDAP/S are the only packet types allowed out of the system. The firewall is secured in the locked CA environment area and not accessible over the network. Restricted Issuing Authority access to the CA is via a dedicated authenticated VPN. An approved trusted SA makes all changes at the firewall station itself.

Data Transmission: The biometric image data collected at enrollment centers are handled as sensitive personal information throughout the process. Biometric images are stored as compressed and encrypted data, completely disassociated from personally identifiable information. The IDMS generates an “index key” that serves as the only link between an enrolled individual’s biographical information and biometric image data. In addition, biometric images and the biometric templates created from this data are suitably handled to prevent any interception, alteration, release, or other data compromise that could result in unauthorized use. Biometric protection techniques outlined in International Committee for Information Technology Standards (INCITS) - 383 are used to secure these biometric templates. Under no circumstances is any biometric data retained in the local enrollment station after transmission to the IDMS is complete. Enrollment centers do not retain any information. System design and architecture supports the automatic deletion of all collected information (e.g., enrollment record) after successful transmission to the IDMS. The confirmation of deletion produces an auditable record of the event for verification.

Data Storage Facilities: Access to the Security Card Facilities and equipment are secured by limiting physical access to the workspace and system, and by requiring an appropriate verification of identity for logical access to the system. Where appropriate, this method uses the PIV card providing one, two or three factors of authentication (i.e., something you have, something you know and something you are). Where necessary, this method also consists of two components (e.g., user id + password).

Card Production: The IDMS sends confirmed enrollment information to the card production facility at the FTC via a private connection. Cards that are not active cannot be used for access to federal facilities or networks. Certifications are revoked when they are reported lost, stolen, damaged beyond use, or when a cardholder has failed to meet the terms and conditions of enrollment. Cards will be deactivated upon collection of damaged cards or if the employee or contractor no longer requires a PIV card.

Equipment: For user identification, PIV cardholders are authenticated to access the PIV system using, at a minimum, two-factor authentication based on their role and responsibility. A required component (first factor) of this authentication is the PIV card itself. In combination with the PIV, the second factor of this authentication requires a PIN and/or biometric identifier (e.g., fingerprint).

- User Groups: System/application users have varying levels of responsibility and are only allowed to access information and features of the system appropriate for their level of job responsibility and security clearance. These rights are determined by the identification provided when authenticating (i.e., user identification) to the system as described above.
- Network Firewall: Equipment and software are deployed to prevent intrusion into sensitive networks and computers. As noted earlier, the FTC's IDMS is not connected to the rest of the FTC's computer network.
- Encryption: Sensitive data are protected by rendering it unreadable to anyone other than those with the correct keys to reverse the encrypted data.
- Access Control: Access to data is PIN protected.
- Audit Trails: Attempts to access sensitive data are recorded for forensic purposes if an unauthorized individual attempts to access the information contained within the system.
- Recoverability: The system is designed to continue to function in the event that a disaster or disruption of service should occur.
- Physical Security: Measures are employed to protect enrollment equipment, facilities, material, and information systems that are part of the PIV program. These measures include: locks, ID badges, fire protection, redundant power, and climate controls to protect IT equipment that are part of the PIV program.
- An Information Assurance and Security plan containing all technical measures and operational procedures consistent with Federal law, FIPS 201, related special publications and agency policy.
- A periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability.
- System users/operators are officially designated as agents of the FTC and complete a training process associated with their specific role in the PIV process.

Separation of Duties Controls: The Security Officer for the FTC appoints the Sponsors, Registrar and Issuers in writing. Their IDMS access cards are also programmed so that they only can perform their function (i.e., Sponsor, Registrar or Issuer) in the IDMS. This forces the Sponsor, Registrar and Issuer to coordinate to ensure that cards are issued. No one person has the authority to do all three functions.

1. **PIV Sponsor:** The Sponsor is the individual who substantiates the need for a PIV credential to be issued to the Applicant and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant. PIV Sponsors shall meet the following minimum standards: (a) is a Federal Government employee authorized in writing by the Bureau, Organization or Regional Office to request a PIV credential; (b) have a valid justification for requesting a PIV credential for an Applicant; (c) be in a position of responsibility for the Bureau, Organization or Regional Office; and (d) have already been issued a valid PIV credential.

   ●The PIV Sponsor completes a PIV Request for an Applicant and submits to the PIV Registrar and the PIV Issuer. The PIV Request includes the following information:

   - ●Name, organization, and contact information of the PIV Sponsor, including the address of the sponsoring organization;
   - ●Name, date of birth, position, and contact information of the Applicant name and contact information of the designated PIV Registrar;
   - ●Name and contact information of the designated PIV Issuer; and
   - ●Signature of the PIV Sponsor.

   Note: The FTC has two types of Sponsors. The Administrative Sponsor (responsible for requesting a PIV card on behalf of an Applicant) and the Operational Sponsor (FTC staff responsible for inputting the data into the IDMS database).

2. **PIV Registrar**: The Registrar is responsible for identity proofing the Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant. PIV Registrars must meet the following minimum standards: (a) is a Federal Government official and is designated in writing as a PIV Registrar; (b) is capable of assessing the integrity of the Applicant's identity source documents (i.e., is trained to detect any improprieties in the applicant's identity-proofing documents); and (c) is capable of evaluating whether a PIV application is satisfactory and applies organization-specific processes to an unsatisfactory PIV application. Thus, the PIV Registrar needs training on organization processes and procedures for evaluating an unsatisfactory PIV application.

   The PIV Registrar has access to the following information:
   - Applicant's SF 85, 85P or 86.
   - Two forms of identity source documents

   The PIV Registrar records the following data for each of the two identity source document, signs the records and maintains on file:

- document title;
- document issuing authority;
- document number;
- document expiration date (if any); and
- any other information used to confirm the identity of the applicant.

The PIV Registrar:

- Compares the Applicant's PIV request information (name, date of birth, contact info) with the corresponding information provided by the applicant from an earlier visit.
- Captures a facial image of application and retains a file copy of the image.
- Fingerprints the applicant, obtains all fingerprints, and retains a copy.
- Initiates a NACI.
- Notifies the sponsor and designated PIV Issuer that applicant had been approved or disapproved.

3. **PIV Issuer:** The Issuer performs credential personalization operations and issues the identity credential to the Applicant after all background checks, identity proofing, and related approvals have been completed. The PIV Issuer also is responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.

   The PIV Registrar makes available the following information to the PIV Issuer:

   - Facial image copy of result of background investigation
   - Other data associated with applicant (e.g. employee affiliation)

4. **PIV Digital Signatory:** The Digital Signatory digitally signs the PIV biometrics and Cardholder Unique Identifier (CHUID). This role applies for PIV-II. The PIV Registrar makes available to the PIV Digital Signatory:

   - Electronic biometric data for card personalization; and
   - Other data associated with the applicant that is required for generating signed objects for card personalization.

5. **PIV Authentication Certification Authority (CA):** The CA signs and issues the PIV Authentication Certificate. This role applies to PIV-II.

6. **PIV Adjudicator:** The PIV Registrar also acts as the PIV Adjudicator. The Adjudicator is responsible for determining whether the Applicant is suitable to receive a credential based on results obtained from the OPM background investigation. Adjudicator responsibilities include: (a) confirming fingerprint results from OPM/FBI; (b) adjudicating NACI (or higher level OPM investigation) and resolving issues, if necessary; (c) providing final results to the PIV Registrar; and (iv) updating the Official Personnel File (OPF) (for FTC employees) or contract file (in the case of contractor personnel who receive a PIV card) with a "Certificate of Investigation."

7. **Enrollment Official (EO):** Directors, Deputy Directors and Administrative Officers for the Regional Office may act as Enrollment Official. (Under HSPD-12, this is the individual responsible for performing identify-proofing for Applicants at locations that do not have a PIV Card Issuing Facility (PCIF), Registrar, or Servicing Human Resources Office, which is the case with the FTC's Regional Offices.) The EO verifies the claimed identity of the Applicant, creates the registration package to be submitted for registration and enrollment to FTC HQ and is responsible for delivering the personalized PIV credential to the applicant. The EO does not actually issue the card, which will occur at FTC headquarters.

8. **System Administrator:** Serves as Administrator for the IDMS database.

Security of the ID credential (PIV card) issued to an employee or contractor is achieved by full compliance with the mandatory requirements of the Federal Information Processing Standard Publication 201 (FIPS Publication 201), Personal Identity Verification of Federal Employees and Contractors. Specific safeguards include:

- Card issuing authority limited to providers with official accreditation pursuant to NIST Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
- Cards use at least one visual tamper proof feature such as holograms, watermarks, etc.
- Card data is encrypted and stored on the card
- Card is sheathed in electromagnetically opaque sleeve to protect against unauthorized contact to prevent access to stored information
- Employees are alerted to importance of protecting card
- Card expiration within three years from issuance
- Return of cards to agency when no longer needed (or upon employee/contractor separation from the agency)
- Deactivation of card within 18 hours (the latest) of employee/contractor separation, loss of card, or expiration
- Removal of all IIF associated with the cardholder from the system upon deactivation if cardholder will not be reissued a new card
- Specialized role-based training for all persons involved in the PIV process

6.1 [bis] Who will have access to the information?

Security personnel and authorized IT personnel or contractors (pursuant to an appropriate routine use) who handle the operations and maintenance of the system will have limited access to the system to support the credentialing activity as well as trouble shoot technical system issues encountered on a day-to-day basis. Additionally, the FTC Office of Inspector General (OIG) may request and be given access to the data, and the FTC Office of General Counsel's (OGC) Litigation Division may request and be provided access to the data to represent FTC in litigation matters related to the PIV system. Intra-agency access by OIG and OGC, if any, is authorized by section (b) (1) of the Privacy Act on a strictly need-to-know basis.

6.2 [bis] Are written procedures in place identifying who may access the system?

Yes. The written procedures for the FTC registration and issuance process describe in detail the roles, responsibilities and procedures for PIV processing. All FTC employees and assigned contractor staff will receive appropriate privacy and security training, and have any necessary background investigations and/or security clearances for access to sensitive, privacy or classified information or secured facilities. The FTC ensures this through legal agreements with its contractors and enforcement of internal procedures with all FTC entities involved in processing the background checks. Additionally, robust standard operation procedures and system user manuals describe in detail user roles, responsibilities and access privileges

6.3 What technical and/or operational controls are in place to prevent misuse of data by those having access?

By design, and for security and privacy reasons, no enrollment data is stored at or on the enrollment workstation. The enrollment record can only be viewed or retrieved by an FTC Registrar or PIV Issuer who is trained and authorized to perform enrollment activities. The ability to retrieve or view an employee's enrollment record is controlled by user authentication, which ensures only those with a need to access the data and who possess proper training can retrieve or view enrollment information. In addition to this access control, physical privacy protections will be used. These physical protections include the use of "privacy screens" that prevent passers-by from viewing enrollment record information that may be displayed on the enrollment center workstation. Additionally, the enrollment center's physical security controls (at FTC regional offices) will be enforced to ensure that only the FTC security personnel or PIV Issuer with a need for access can enter the enrollment center and view personal information displayed on screens.

6.4 Given the access and security controls you evaluated, what privacy risks were identified and describe how you mitigated them?

As described above, to prevent unauthorized access to the IDMS system, the FTC has installed a T-1 line between its HSPD-12 badging system and the ORC database, rather than routing the IDMS through the rest of the FTC's network. We also have appointed technical and administrative sponsors so that there is one location for badging and one point of entry to that location. The IDMS system is located in the Security Office and entry is restricted to security staff and personnel who are being processed in the Security Office.

SECTION 7.0 DATA STORAGE AND RETENTION

7.1 What are the retention periods for the data in the system?

Personnel Security Clearance Files

Security Clearance records relating to individuals will be retained and disposed of in accordance with General Records Schedule 18, either item 22a (case files) or item 23 (clearance lists).

(a) Item 22a covers case files documenting the processing of investigations on Federal employees or applicants for Federal employment, whether or not a security clearance is granted, and other persons, such as those performing work for a Federal agency under contract, who require an approval before having access to Government facilities or to sensitive data. These records will be destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

(b) Item 23 covers lists or rosters showing the current security clearance status of individuals. These lists or rosters will be destroyed when superseded or obsolete.

Identity Credentials and Badges

In accordance with HSPD-12, PIV Cards will be deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards will be maintained in accordance with General Records Schedule 11, Item 4. PIV Cards will be destroyed by cross-cut shredding no later than 90 days after deactivation.

Facilities Security - Access Control Files

Registers, logs and other records of physical or logical access to Agency facilities or systems by employees, contractors and visitors, including records that track the use of PIV cards, will be destroyed 2 years after the date of the record or the last entry reflected on such record, in accordance with General Records Schedule 18, item 17, unless the record needs to be retained for specific, ongoing security investigations. These records establish date, time, and location of entry into and exit from Agency facilities and also access dates, times, and locations of Agency computer systems; and can include names, PIV card serial numbers, digital signature information; level of national security clearance and expiration date, if applicable.

SECTION 8.0 RESULTS OF FISMA REVIEW

8.1 Has the system(s) completed a C&A as required by FISMA?

Yes.

8.2 If not, at what stage in the C&A process are the system(s) and what is the anticipated date of the C&A?

Not Applicable.

8.3 Has the agency conducted a risk assessment, and identified and implemented appropriate technical, administrative, and operational security controls?

For the FTC's IDMS, the ORC database was accredited, effective October 31, 2005, regarding the Federal Bridge Certification Authority (FBCA) compliance and Federal Common Policy Framework compliance. As part of that process, a risk assessment of the system, including security controls, was conducted.

As noted above, to address privacy risks, additional controls were adopted. For example, the IDMS was connected to ORC via a T-1 line, rather than connecting it to the FTC's network shared by other employees and contractors. This alternative approach provides a point-to-point connection and reduces the possibility of hackers illegally accessing the system. The FTC has written operation manuals on the use of the system to ensure that the operators properly utilize the equipment. The IDMS system is located in the FTC Security Office with restricted access. The locks are keyed only for security access. No other keys in the FTC access the security offices.

SECTION 9.0 ANALYSIS AND ASSESSMENT

The FTC's consideration of competing technologies focused on products and services identified by the GSA as compliant with HSPD-12 standards and requirements. Although the FTC procured IDMS services requiring off-site data storage by the vendor, the vendor uses secure technology for ensuring the protection of such data, as described above. Accordingly, the FTC believes that the technology it has acquired for implementing HSPD-12 is adequate to achieve system goals, and the agency did not identify any unique privacy issues that were not sufficiently mitigated, either by the technology used, or the agency procedures adopted for implementing the technology (e.g., separation of roles, T-1 line).

SECTION 10.0 CONCLUSIONS

As already discussed, the FTC addressed a major potential privacy risk by determining not to store or permit access to system data on the agency network but instead determined to use a dedicated T-1 line for transmission of such data to off-site management and storage by the vendor. The FTC has also implemented the other procedural controls required by OMB and NIST guidance to ensure data security.

SECTION 11.0 DETERMINATIONS OF OFFICIALS

The sensitivity of this system requires that the FTC ensure that it meets the following requirements:

- Achieve an IT Security accreditation and certification (i.e., vendor system) every three years
- Review associated System of Record Notices every other year
- Review and update, as necessary, applicable PIAs every year

Contingent on the three elements listed above and the satisfaction of all applicable Directives, OMB guidance, and NIST standards and requirements, the privacy controls related to the system this PIA covers are considered adequate.

Prepared for the Business Owners of the System by:

Charles King FTC Chief Security Officer	Date:

Review:

Mark Oemler Deputy Director, Administrative Services	Date:
Alexander C. Tang, Attorney Office of the General Counsel	Date:
Marc Groman Chief Privacy Officer	Date:
Margaret Mech Chief Information Security Officer	Date:

Approved:

Stanley Lowe Chief Information Officer	Date: