MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS
SENIOR AGENCY OFFICALS FOR PRIVACY

FROM: Karen S. Evans
Administrator, Office of E-Government and
Information Technology

SUBJECT: Sample Privacy Documents for Agency Implementation of
Homeland Security Presidential Directive (HSPD) 12

The Office of Management and Budget (OMB) issued guidance on August 5, 2005 to departments and agencies regarding their responsibilities under HSPD-12 ("Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive)).[1] As you know, HSPD-12 required the Department of Commerce to develop, and departments and agencies to implement, a government-wide standard for secure and reliable credentialing of Federal employees and contractors. Section 6 of OMB's August 5, 2005 guidance itemizes the privacy-related elements of HSPD-12 implementation based on existing requirements that individuals be fully informed about collections of their personal information.[2]

As was noted in OMB's guidance, attached are sample privacy documents to use as models in implementing HSPD-12 at your agencies. Included are sample Privacy Act systems of records notices, Privacy Act statements, and a privacy impact assessment developed by a working group of privacy experts. You may modify the samples to meet your agency-specific requirements, including those not anticipated by the working group, but overall your documents should comport with the models provided.

If you have questions about the privacy elements of HSPD-12 implementation or the sample documents provided, contact Eva Kleederman, Senior Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget. Phone (202) 395-3647, fax (202) 395-5167, or e-mail: ekleeder@omb.eop.gov.

Attachments

[1] OMB M-05-24: Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, 8/5/05, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf.
[2] See Privacy Act of 1974 (5 U.S.C. § 552a), the E-Government Act of 2002 (44 U.S.C. ch. 36), and OMB M-03-23 Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, 9/26/03, http://www.whitehouse.gov/omb/memoranda/m03-22.html.

SAMPLE PRIVACY DOCUMENTS
TABLE OF CONTENTS

Information underlined is intended to be specific to the agency publishing the notice. Other portions of the documents can be adopted exactly as drafted.

This sample system of records notice covers the initiation of the HSPD-12 process — the collection and management of personnel security information. While most agencies have an existing system of records for personnel security files and, if applicable, background investigations, this model is intended as an update to replace or amend existing agency systems of records so that they are compliant with both HSPD-12 and the Privacy Act and conform to the Privacy Act notices on the standard forms which are used to initiate the HSPD-12 process.

This sample system of records notice covers the HSPD-12 process after adjudication determines the individual can receive an identification card. It includes both mandatory and optional information necessary to the request for a card, registration, verification, and issuance procedures, the index/database of active and invalid cards, and the information stored on the cards. It may include records maintained by agencies of individuals who entered and exited facilities or accessed systems.

This sample Privacy Act Statement provides notice to a department or agency's own employees and contractors at the time the agency issues an identification card. This notice describes the information the agency is collecting and how it will be used and stored. In addition, it describes what information is stored on the card itself, which may differ from what can be visibly seen on the card. The Privacy Act Statement will vary based on each agency's implementation of the program.

This Privacy Act Statement gives notice to cardholders entering a facility or using a system of another agency, but it can be applicable to using the card at one’s home agency. The statement assumes cardholders have already received a Privacy Act notice upon issuance of the card explaining what information is in the system(s) of their own agency, and what information is stored on the card (see the explanation in attachment C above). We expect each agency will need to modify the language of this notice, depending on what information the agency collects and stores when a cardholder uses the card for access.

Attachment E: Privacy Impact Assessment for Personal Identity Verification (pp. 16-36)

The privacy impact assessment analyzes the information technology systems used to implement the Directive and the associated privacy impacts. Many sections will need to be customized based on agency specific decisions related to system design and risk mitigation. These sections are noted in [*bracketed italicized*] text.

Attachment A: System of Records Notice for Personnel Security Files[3]

DEPARMENT/Agency ####-####

SYSTEM NAME: Personnel Security Files

SYSTEM LOCATION: <addresses>

SECURITY CLASSIFICATION: Most personnel identity verification records are not classified. However, in some cases, records of certain individuals, or portions of some records, may be classified in the interest of national security.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals who require regular, ongoing access to federal facilities, information technology systems, or information classified in the interest of national security, including applicants for employment or contracts, federal employees, contractors, students, interns, volunteers, individuals authorized to perform or use services provided in Agency facilities (e.g., Credit Union, Fitness Center, etc.), and individuals formerly in any of these positions. The system also includes individuals accused of security violations or found in violation.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, former names, birth date, birth place, home address, phone numbers, employment history, residential history, education and degrees earned, names of associates and references and their contact information, citizenship, names of relatives, birthdates and places of relatives, citizenship of relatives, names of relatives who work for the federal government, criminal history, mental health history, drug use, financial information, fingerprints, summary report of investigation, results of suitability decisions, level of security clearance, date of issuance of security clearance, requests for appeal, witness statements, investigator's notes, tax return information, credit reports, security violations, circumstances of violation, and agency action taken.

Forms: SF-85, SF-85P, SF-86, SF-87

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Depending upon the purpose of your investigation, the U.S. government is authorized to ask for this information under Executive orders 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12. [from SF-86]

PURPOSE(S): The records in this system of records are used to document and support decisions as to the suitability, eligibility, and fitness for service of applicants for federal

[3] This system of records does not duplicate or supersede the Office of Personnel Management's (OPM) Central-9 system of records which covers the investigations OPM and its contractors conduct on behalf of other agencies. Each agency must have a system of records to cover the intake of background investigation applications (i.e. forms SF-85/85P/86/87), summary reports from OPM or another agency conducting background investigations, results of adjudications, security violations, etc.

employment and contract positions, and may include students, interns, or volunteers to the extent their duties require access to federal facilities, information, systems, or applications. They may also be used to document security violations and supervisory actions taken.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.
2. To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.
3. Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.
4. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.
5. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. §§ 2904 and 2906.
6. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
7. To any source or potential source from which information is requested in the course of an investigation concerning the retention of an employee or other personnel action (other than hiring), or the retention of a security clearance, contract, grant, license, or other benefit, to

the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

8. To a Federal State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel or regulatory action.
9. To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy.
10. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.
11. To the Office of Management and Budget when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.

POLICIES AND PRACTISE FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE: Records are stored on paper and electronically in a secure location.

RETRIEVABILITY: Background investigation files are retrieved by name, Social Security Number (SSN), or fingerprint.

SAFEGUARDS: For paper records: Comprehensive paper records are kept in locked metal file cabinets in locked rooms at the <Headquarters> office responsible for suitability determinations. Paper records limited (in number and scope) are kept in the agency's regional offices in locked metal file cabinets in locked rooms. Access to the records is limited to those employees who have a need for them in the performance of their official duties.

For electronic records: Comprehensive electronic records are kept in the <Personnel Security Office>. Access to the records is restricted to those with a specific role in the Personal Identity Verification (PIV) process that requires access to background investigation forms to perform their duties, and who have been given a password to access that part of the system including background investigation records. An audit trail is maintained and reviewed periodically to identify unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about how to protect individually identifiable information.

RETENTION AND DISPOSAL: These records are retained and disposed of in accordance with General Records Schedule 18, item 22, approved by the National Archives and Records Administration (NARA). Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

SYSTEM MANAGER(S) AND ADDRESS: <agency, office, address>

NOTIFICATION PROCEDURE: An individual can determine if this system contains a record pertaining to him/her by sending a request in writing, signed, to <name of official> at the following address: address

When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, name, date of birth, social security number, and home address in order to establish identity.

RECORDS ACCESS PROCEDURES: Same as notification procedures. Requesters should also reasonably specify the record contents being sought. Rules regarding access to Privacy Act records appear in __ CFR part __. If additional information or assistance is required, contact Agency Official, address, phone, fax, email.

CONTESTING RECORD PROCEDURES: Same as notification procedures. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete. Rules regarding amendment of Privacy Act records appear in ___ CFR part ___. If additional information or assistance is required, contact Agency Official, address, phone, fax, email.

RECORD SOURCE CATEGORIES: Information is obtained from a variety of sources including the employee, contractor, or applicant via use of the SF-85, SF-85P, or SF-86 and personal interviews; employer's and former employers' records; FBI criminal history records and other databases; financial institutions and credit reports; medical records and health care providers; educational institutions; interviews of witnesses such as neighbors, friends, co-workers, business associates, teachers, landlords, or family members; tax records; and other public records. Security violation information is obtained from a variety of sources, such as guard reports, security inspections, witnesses, supervisor's reports, audit reports.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE PRIVACY ACT: Upon publication of a final rule in the Federal Register, this system of records will be exempt in accordance with 5 U.S.C. § 552a(k)(5). Information will be withheld to the extent it identifies witnesses promised confidentiality as a condition of providing information during the course of the background investigation.

Attachment B: System of Records Notice for Identity Management System(s)

AGENCY NAME ####-####

SYSTEM NAME: Identity Management System (IDMS)

SYSTEM LOCATION: Data covered by this system are maintained at the following locations: AGENCY NAME, address; second address; third address. Some data covered by this system is at Agency locations, both Federal buildings and Federally-leased space, where staffed guard stations have been established in facilities that have installed the Personal Identity Verification (PIV) system, as well as the physical security office(s) or computer security offices of those locations.

SECURITY CLASSIFICATION: Most identity records are not classified. However, in some cases, records of certain individuals, or portions of some records, may be classified in the interest of national security.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals who require regular, ongoing access to agency facilities, information technology systems, or information classified in the interest of national security, including applicants for employment or contracts, federal employees, contractors, students, interns, and volunteers, and individuals formerly in any of these positions. The system also includes individuals authorized to perform or use services provided in agency facilities (e.g., Credit Union, Fitness Center, etc.)

The system does not apply to occasional visitors or short-term guests to whom agency will issue temporary identification and credentials.

CATEGORIES OF RECORDS IN THE SYSTEM: Records maintained on individuals issued credentials by agency include the following data fields: full name, Social Security number; date of birth; signature; image (photograph); fingerprints; hair color; eye color; height; weight; organization/office of assignment; company name; telephone number; copy of background investigation form; Personal Identity Verification (PIV) card issue and expiration dates; personal identification number (PIN); results of background investigation; PIV request form; PIV registrar approval signature; PIV card serial number; emergency responder designation; PIV card expiration date; copies of documents used to verify identification or information derived from those documents such as document title, document issuing authority, document number, document expiration date, document other information); level of national security clearance and expiration date; computer system user name; user access and permission rights, authentication certificates; digital signature information.

Records maintained on card holders entering Agency facilities or using Agency systems include: Name, PIV Card serial number; date, time, and location of entry and exit; company name; level of national security clearance and expiration date; digital signature information; computer access dates, times, and locations.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. § 301; Federal Information Security Act (Pub. L. 104–106, sec. 5113); Electronic Government Act (Pub. L. 104–347, sec. 203); the Paperwork Reduction Act of 1995 (44 U.S.C. § 3501); and the Government Paperwork Elimination Act (Pub.L. 105–277, 44 U.S.C. § 3504); Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended.

PURPOSE: The primary purposes of the system are: (a) To ensure the safety and security of agency facilities, systems, or information, and our occupants and users; (b) To verify that all persons entering federal facilities, using federal information resources, or accessing classified information are authorized to do so; (c) to track and control PIV cards issued to persons entering and exiting the facilities, using systems, or accessing classified information.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. § 552a(b), and:

(1) To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

(2) To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

(3) Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

(4) To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

(5) To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. §§ 2904 and 2906.

(6) To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

(7) To a Federal State, local, foreign, or tribal or other public authority the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel or regulatory action.

(8) To the Office of Management and Budget when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.

(9) To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

(10) To notify another federal agency when, or verify whether, a PIV card is no longer valid.

Note: Disclosures within agency of data pertaining to date and time of entry and exit of an agency employee working in the District of Columbia may not be made to supervisors, managers or any other persons (other than the individual to whom the information applies) to verify employee time and attendance record for personnel actions because 5 U.S.C. § 6106 prohibits Federal Executive agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless used as a part of a flexible schedule program under 5 U.S.C. § 6120 *et seq.*

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE: Records are stored in electronic media and in paper files.

RETRIEVABILITY: Records are retrievable by name, Social Security number, other ID number, PIV card serial number, image (photograph), fingerprint.

SAFEGUARDS: Paper records are kept in locked cabinets in secure facilities and access to them is restricted to individuals whose role requires use of the records. The computer servers in

which records are stored are located in facilities that are secured by alarm systems and off-master key access. The computer servers themselves are password-protected. Access to individuals working at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A Privacy Act Warning Notice appears on the monitor screen when records containing information on individuals are first displayed. Data exchanged between the servers and the client PCs at the guard stations and badging office are encrypted. Backup tapes are stored in a locked and controlled room in a secure, off-site location. [Agencies should describe their own security situation at this level of detail.]

An audit trail is maintained and reviewed periodically to identify unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about how to protect individually identifiable information.

RETENTION AND DISPOSAL: Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations, for maximum security facilities, records of access are maintained for five years and then destroyed by degaussing hard drives and shredding paper. For other facilities, records are maintained for two years and then destroyed by wiping hard drives and shredding paper. All other records relating to employees are destroyed two years after ID security card expiration date.

In accordance with HSPD-12, PIV Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by shredding 90 days after deactivation.

SYSTEM MANAGER(S) AND ADDRESS: Agency Official, address, phone, fax, email, etc.

NOTIFICATION PROCEDURES: An individual can determine if this system contains a record pertaining to him/her by sending a request in writing, signed, to <name of official> at the following address: address

When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records in person must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID. Individuals requesting notification via mail or telephone must furnish, at minimum, name, date of birth, social security number, and home address in order to establish identity.

RECORDS ACCESS PROCEDURES: Same as notification procedures. Requesters should also reasonably specify the record contents being sought. Rules regarding access to Privacy Act records appear in __ CFR part __. If additional information or assistance is required, contact Agency Official, address, phone, fax, email.

CONTESTING RECORD PROCEDURES: Same as notification procedures. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete. Rules regarding amendment of Privacy Act records appear in ___ CFR part ___. If additional information or assistance is required, contact Agency Official, address, phone, fax, email.

RECORD SOURCE CATEGORIES: Employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other federal agencies; contract employer; former employer.

EXEMPTIONS CLAIMED FOR THE SYSTEM: None.

Attachment C: ID Proofing and Registration Privacy Act Statement

What is the Personal Identity Verification (PIV) Card? You are being issued a PIV card that is one part of a system for protecting federal buildings, computers, applications, and data. This is a secure and reliable card based on your verified identity. It is extremely hard to fake, change, or duplicate. It is only issued by accredited employees. If you previously had a government badge, the PIV Card replaces your badge.

What is the Authority for the PIV Card Program? Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. The directive can be reviewed at: http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html

Why do I need a PIV Card? Common to all federal agencies, the PIV card is a way for you to prove that you are who you claim to be. We issue PIV cards to reduce identity fraud, protect your privacy, save time, and improve security through a standardized process. As part of this process, the U.S. Government conducts a background investigation on you to decide whether you are suitable for your job and eligible to use the buildings, computers, applications and data you need to do your job. Some of the information you provide for your background investigation, along with information from the office that hired you, is used to verify your identity, create a PIV card for you, and create a record that you have been issued a card.

What Information Is Stored in the System About Me? We keep the following information in our records: your full name, facial photograph, two fingerprints, date of birth, home address, home phone number, your background investigation form, the results of your background check, the approval signature of the person who registers you in the system, your PIV card expiration date, the PIV card serial number, and copies of the documents you used to verify your identity, such as your driver's license or passport.

What Information is Stored on the PIV Card? The card itself displays a printed picture of your face, your full name, agency, organization, card expiration date, card serial number, and an issuer identification number. The card also stores a Personal Identification Number (PIN), a unique identifier, an PIV authentication key, and two electronic fingerprints. In addition, Agency stores/displays _____, _____, and ____ on the card.

How Will My Information Be Used? Agency and other agencies will use the information on the PIV card and may use some of the stored information about you when you access to federal facilities, computers, applications, or data to prove your identity and your right of access. This information will be kept as long as you have a valid PIV card.

Who Will See My Information? Information about you that we store to issue you a PIV Card and run the program may be given without your consent as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a(b)) and: to the appropriate government organization if your records show a violation or potential violation of law; to the Department of Justice, a court, or other decision-maker when the records are relevant and necessary to a law suit; to a federal, state, local, tribal, or foreign agency that has records we need to decide whether to retain an employee, continue a security clearance, or agree to a contract; to a Member of Congress or to Congressional staff at your written request; to the Office of Management and Budget to evaluate private relief legislation; to 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; to the National Archives and Records Administration for records management inspections; and to other federal agencies to notify them when your card is no longer valid. The full system of records notice with

complete description of routine uses was published in the Federal Register at cite and can be viewed at: <URL for SORN>.

What Happens if I Don't Want a Card? While there is no legal requirement to use a PIV Card, if you do not give us the full information we need, we may not be able to create your record and complete your identity check, or complete it in a timely manner. If you do not have a PIV Card, you will be treated as a visitor when you enter a federal building. You will not have access to certain federal resources. If using a PIV card is a condition of your job, not providing the information will affect your placement or employment prospects.

Where Can I Get More Information About How My Information is Used? If you have questions or concerns about the use of your information, you may contact Senior Official for Privacy/Card Applicant Representative (CAR), <official's name, address, room #, phone number, email address>. Further information is available on the agency web site at <URL for HSPD-12 information>.

Attachment D: Card Usage Privacy Act Statement

Personal Identity Verification (PIV) Card Privacy Act Statement

We are required by the Privacy Act of 1974 (5 U.S.C. § 552a) to tell holders of Personal Identity Verification (PIV) Cards what information we collect from your card and how it will be used. The goal of PIV is to reduce identity fraud, protect your privacy, save time, and improve security.

Why Do I Need to Show My Card? The PIV card is a way for you to prove that you are who you claim to be when you enter a federal building, and your right of access to computers, applications or data. All federal agencies use the PIV card to verify your identity and your rights to enter federal facilities and use federal computers, applications and data.

What is the Authority for the PIV Card Program? The PIV enrollment process and the PIV card interoperability standards are authorized by Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. The directive can be reviewed at: http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html.

What Happens When I Use my PIV Card at Agency? When you show, swipe or insert your card into a reader, your identity will be verified by a person or a machine. A person will look at the picture on your card and compare it to your face. A machine will compare the data stored on the card to the database of cardholders. The machine may compare the biometric stored on the card to your actual biometric (fingerprint). When you come in our building, use our computers, or access information controlled by us, and you use your card, we collect <your name, agency, organization, card expiration date, card serial number, date/time, etc.> and store it in our system. We keep this information for length of time, and if, after that time, it is not needed for safety or security reasons, or to investigate improper behavior by anyone, we destroy it. If it is used in an investigation, it will be kept until the investigation is concluded and the record is no longer needed.

How Will My Information Be Used, and Who Else Will See It? Information about you displayed or stored on your PIV Card may be given without your consent as permitted by the Privacy Act (5 U.S.C. § 552a(b)): to the appropriate government organization if your records show a violation or potential violation of law; to the Department of Justice, a court, or other decision-maker when the records are relevant and necessary to a law suit; to a federal state, local, tribal, or foreign agency that has records we need to decide whether to retain an employee, continue a security clearance, or agree to a contract; to a Member of Congress or to Congressional staff at your written request; to the Office of Management and Budget to valuate private relief legislation; to 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; to the National Archives and Records Administration for records management inspections, and to other federal agencies to notify them when your card is no longer valid. The full system of records notice with complete description of routine uses was published at cite, and can be viewed at: <URL for SORN>.

What Happens if I Don't Want to Use or Show My Card? While there is no legal requirement to give us this information or to use a PIV Card, if you do not, we will treat you like a visitor. It may take more time, and you will not have access to certain computers, applications or data. If using a PIV card is a condition of your job, not using it will affect your placement or employment prospects.

Where Can I Get More Information About the PIV Card Program? If you have questions or concerns about the use of your information, talk to our agency Senior Official for Privacy/Card Applicant Representative (CAR), <official's name, address, room #, phone number, email address>. Further information is available on our web page at: <URL for HSPD-12 information>.

Attachment E: Privacy Impact Assessment for Personal Identity Verification

PIV Program PIA Reference Sheet

Unique Project Identifier Number (UPI): _____
(If no UPI, please explain why.): _____

System of Records (SOR) Number:_____
SOR Title:_____

Legal Authority(ies): Privacy Act of 1974, E-Government Act of 2002, Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standard 201: Policy for a Common Identification Standard for Federal Employees and Contractors

IT Security Plan Number(s):_____
IT Security Plan Title:_____
Accreditation and Certification Date: _____

OMB Exhibit 300 Number:_____
OMB Exhibit 300 Title:_____

Identity Proofing and Registration Process Approval Date:_____
PIV Implementation Plan Approval Date:_____

Contact Name, Title:_____

E-Mail:_____

Organization/Department:_____

Phone Number:_____

Activity/Purpose of Program: To store, manage, and maintain information related to the issuance and maintenance of PIV credentials to federal employees and contractors, and, the process of verification and authentication of access to federal resources by federal employees and contractors.

INTRODUCTION

Program Overview

Homeland Security Presidential Directive 12 (HSPD-12), issued on August 27, 2004, required the establishment of a standard for identification of Federal Government employees and contractors. HSPD-12 directs the use of a common identification credential 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. The National Institute of Standards and Technology (NIST) published a standard for secure and reliable forms of identification, Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors. The credential is for physical and logical access.

FIPS 201 has two parts: PIV I and PIV II. The requirements 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 specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards) for use in a Federal system. Simply stated, FIPS 201 requires agencies to:

- Establish roles to facilitate identity proofing, information capture and storage, and card issuance and maintenance.
- Develop and implement a physical security and information security infrastructure to support these new credentials.
- Establish processes to support the implementation of a PIV program.

In response to HSPD-12 and to meet the requirements summarized above, [*Agency*] Office of [*agency*] is responsible for the identity management and all aspects of the [*agency*] 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. [*Agency*] is currently expecting to equip approximately [*999*] PIV cards for building and computer access at over [*999*] facilities nationwide beginning in FY 2006.

PIA Scope

This PIA provides detail about [*agency's*] role in the collection and management of personally identifiable information for the purpose of issuing credentials (ID badges) to meet the requirements of HSPD-12 and comply with the standards outlined in FIPS 201 and its accompanying special publications. HSPD-12 requires the standardized and secure processes required 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: (i) background investigation; (ii) identity proofing and registration; (iii) Identity Management System (IDMS), the database used for identity management and access control; and (iv) 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 will continue to occur. Additionally, PIV-I may not require the implementation of any new systems or technology. [*Agency*] 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.

This PIA covers both the PIV-I and PIV-II processes. This system will be referred to throughout this PIA as the [*agency*] PIV system 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 (1) to individuals whose true identity has been verified, and (2) 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 such that 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, a Federal employee or a contractor. As required by FIPS 201, [*agency*] will collect biographic and biometric information from the PIV Applicant in order to: (i) conduct the background investigation or other national security investigation; (ii) complete the identity proofing and registration process; (iii) create a data record in the PIV Identity Management System (IDMS); and (iv) issue a PIV card. Figure 1 below depicts what information is collected from the PIV Applicant in relation to each of these processes. [*Note: If your agency is sharing enrollment capabilities, the PIA will need to go beyond your program and cover other agency PIV applicants.]*

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

[*Note: Agencies should revise table based on their system implementation*.]

	Background Investigation	**Identity Proofing and Registration**	**IDMS (Electronically Stored)**	**PIV Card (Physically Displayed)**	**PIV Card (Electronically Stored)**
Date of birth	X	X	X		
Place of birth	X				
Social Security Number (SSN)	X	X	X		
Other names used	X				
Citizenship	X			Stripe for foreign national	

	Background Investigation	Identity Proofing and Registration	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)
Other identifying information (height, weight, hair color, eye color, gender/sex)	X			Optional	
Organizational affiliation (e.g. Agency name)	X	X	X	X	X
Employee affiliation (e.g. Contractor, Active Duty, Civilian)		X	X	X	X
Fingerprints (10)	X	X	X		
Biometric identifiers (2 fingerprints)		X	X		X
Digital color photograph		X	X	X	Optional
Digital signature [4]			X	X	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		X[5]		
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		X		
Copies of identity source documents	X		X		

[4] Public key infrastructure (PKI) digital certificate with an asymmetric key pair.
[5] Please note only the Applicant's current address, extracted from the PIV Request Form, is retained in IDMS.

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 [*and <agency> 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 6 months). Two forms are used to initiate the background investigation, Questionnaire for Non-Sensitive Positions Standard Form 85 (SF-85) or the Questionnaire for National Security Positions Standard Form 86 (SF-86).[6] This process entails conducting a full National Agency Check (NAC) or National Agency Check with Inquires (NACI), which are described below:

   - **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.
   - **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.

   It's important to note that the background information collected as part of this process and its results are kept in the background investigation files; however, not stored on the PIV card.
2. **Complete the identity proofing and registration process.** The biographic information collected as part of this process is used to establish the PIV applicant's identity. Biometrics are used to ensure PIV Applicants have not been previously enrolled in the [*agency*] 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 come from the list of acceptable documents included in Form I-9, OMB No. 115-0316, Employment Eligibility Verification.[7] 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, confirms the intent to participate in the PIV process, and submit to a named-based threat background check as required depending on job requirements.
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, manage and maintain this information throughout the PIV

[6] SF 85 and SF 86 can be downloaded at: http://www.opm.gov/forms/html/sf.asp
[7] Form I-9 can be downloaded at: http://uscis.gov/graphics/formsfee/forms/i-9.htm

card lifecycle, and, 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 and identity proofing and registration process, and, successful completion of the enrollment process. Biometrics are used during PIV card issuance to verify PIV Applicant identity and complete activation of the card. This provides much stronger security assurances than typical card activation protections such as Personal Identification Numbers (PINs) or passwords. Once the individual has been issued a PIV Card, the IDMS is updated to reflect that the card has been issued. [*Describe any agency specific situations and agency workflows, e.g. the issued PIV card cannot be used for access to <agency> facilities and networks until activated at the participating location, by the local facility operator.*]
5. **Usage of PIV Card for physical and logical access:** The biometrics collected are used to verify that the rightful cardholder is presenting the card in relation to physical and logical access to federal facilities and information (i.e., computers). The biographic and other information displayed on the PIV card is used by physical security guards for identity verification purposes.

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

Additionally, the [*agency*] PIV IDMS and PIV cards contain other data not collected from the PIV Applicant that are either (i) electronically stored on the card; (ii) electronically stored in the IDMS; and/or (iii) physically displayed on the card. This information and the purpose of its use is described in Figure 2.

[*Note: Agencies should revise table based on their system implementation.*]

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 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 buildings/ space or to log-on to sensitive computer systems ("level 3") that require

	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)	Purpose
				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		Verify issuers authority
Contact Integrated Circuit Chip (ICC)			X	Used to authenticate a PIV cardholder's identity with card readers that require card 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 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 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/No. If yes, please describe the circumstances behind its use and its impact on privacy. Update the sample system of records notice to include a description.]*

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.

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.

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

If the role based model is used by [*agency*], then the role-based then the critical roles are PIV identity proofing, registration and issuance processes are described below. All individuals will be trained to perform his or her respective role; however, these roles may be ancillary roles assigned to personnel who have other primary duties.

1. **PIV Sponsor:** 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: (i) is a Federal Government employee and be authorized in writing by the Bureau, Organization or Regional Office to request a PIV credential; (ii) have valid justification for requesting a PIV credential for an Applicant; (iii) be in a position of responsibility for the Bureau, Organization or Regional Office; and (iv) 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
- Signature of the PIV Sponsor.

2. **PIV Registrar**: The entity responsible for identity proofing of 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 shall meet the following minimum standards: (i) is a Federal Government official and is designated in writing as a PIV Registrar; (ii) 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 (iv) is capable of evaluating whether a PIV application is satisfactory and apply 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, or equivalent
   - Two forms of identity source documents

   The PIV registrar will record the following data for each of the two identity source document, sign the records and keep it 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 info provided by the applicant at an earlier visit.
   - Captures a facial image of application and retains a file copy of the image.
   - Fingerprints the applicant, obtaining all fingerprints and retains a copy.
   - Initiates a NACI.

- Notifies the sponsor and designated PIV Issuer that applicant had been approved or not.

3. **PIV Issuer:** The entity that 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 is also 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 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 entity that digitally signs the PIV biometrics and CHUID. This role applies for PIV-II. The PIV Registrar makes available to the PIV Digital Signatory:
   - Electronic biometric data for card personalization
   - Other data associated with the applicant that is required for generating signed objects for card personalization.

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

6. **PIV Adjudicator:** [*Note: In some cases, the PIV Adjudicator may perform the role of the PIV Registrar so describe your situation.*] The entity responsible for determining whether the Applicant is suitable to receive a credential, based on results obtained from the OPM background investigation. Adjudicator responsibilities include: (i) confirming fingerprint results from OPM/FBI; (ii) adjudicating NACI (or higher level OPM investigation) and resolving issues if necessary; (iii) providing final results to the PIV Registrar; and (iv) updating the Official Personnel File (OPF) or Contract file with "Certificate of Investigation."

7. **Enrollment Official (EO):** [*Note: In some cases, the Enrollment Official may perform the role of the PIV Registrar so describe your situation.*] 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. The EO verifies the claimed identity of the applicant, creates the registration package to be submitted to the <Agency> for registration and enrollment and issues the personalized PIV credential to the applicant.

8. **PCIF Manager:** [*Include if this individual has access to personal information.*] The PCIF Manager is responsible for each PCIF Facility and ensures that all the services specified in FIPS 201 are provided reliably and that PIV credentials are produced and issued in accordance with its requirements.

9. **System Administrator:** [*Describe the role of the system administrator at your agency*.]

SECTION 3.0 EXTERNAL SHARING AND DISCLOSURE

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

During the up-front background investigation process and identity proofing, relevant personal data will be:

1. Shared with the Office of Personnel Management (OPM) who is responsible for conducting the NACI and other higher-level investigations for [*agency*]; and
2. Matched against databases at the Federal Bureau of Investigations (FBI) and [*agency*] 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 [*agency*] PIV program may be given without individual's consent as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a(b)), including 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 the Office of Management and Budget 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 to notify them when a PIV card is no longer valid.

The full system of records notice with complete description of routine uses was published in the Federal Register at [*add citation*] and can be viewed at: [*Add URL for SORN*].

3.2 Is [agency] either providing or receiving card issuance services pursuant to a serving agreement? [*If yes for either case, describe the privacy implications of the servicing agreement (including the transmission, storing and maintenance of data) and how each agency will address the potential privacy risks.*]

SECTION 4.0 AGENCY POLICY REQUIREMENTS

[*Identify any existing department or agency policies that relate to or apply to this program (i.e. policy on unauthorized browsing, labeling/handling of sensitive data, etc.).*]

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?

[*Response provided as a sample discussion. Update based on your agency*] In all cases, PIV applicants are provided a notice required by the Privacy Act, 5 USC 552(a)(e)(3). The notice states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. The collection, maintenance, and disclosure of information complies with the Privacy Act and the published System of Records Notice(s) (SORN) for the PIV program. PIV applicants using an electronic signature process conforming to the Electronic Signature (ESIGN) Act confirm presentation of and agreement with the Privacy At Statement, agree to participate in the PIV process and submit to a background check appropriate to job requirements.

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

5.2.1 Cite any procedures or regulations in place that allow access to information according to FOIA/Privacy Act regulations. Agencies that have customer satisfaction units should provide phone and email information in addition to specific FOIA/Privacy Act procedures.

5.2.2 If the system is exempt from the amendment/correction provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found (i.e., the exemption rulemaking published in the Federal Register).

5.3 What are the procedures for correcting information?

5.3.1 Discuss the procedures and provide contact information for the appropriate person to whom such issues should be addressed. [*Cite information from agency Privacy Act regulation.*]
5.3.2 Describe how information collected from individuals or derived from the system is checked for accuracy.
5.3.3 Describe any processes or procedures in place to reduce inaccuracies in data collected.

5.4 How are individuals notified of the procedures for correcting their information? [*Describe.*]

5.5 If no opportunity to amend is provided, what alternatives are available to the individual? [*Describe.*]

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

[*Sample discussion provided.*] By signing the PIV application form, applicants acknowledge that [*agency*] 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 treated as visitors when entering a federal building and will be barred from access to certain 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?

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

SECTION 6.0 DATA PROTECTION CONTROLS

6.1 General Program Controls

[*For your Agency describe whether and how you implement general program controls. Sample provided below.*]

- The organization has an approved identity proofing and registration process.
- The applicant appears in-person at least once before the issuance of a PIV credential
- The PIV identity proofing, registration and issuance process adheres 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.
- The identity proofing and registration process is accredited by the department or agency as satisfying the requirements and approved in writing by the head of the Federal department or agency.
- The organization has an approved PIV credential issuance and maintenance process.
- The organization issues 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).
- A comprehensive PIA is conducted on systems containing personal information in identifiable (IIF) form for implementing PIV, consistent the E-Government Act.
- The organization has generated a SORN identifying the type of information collected, the purpose of the collection, how the information is protected, and the compete set of uses of the credential and related information during the life of the credential.
- The organization assures that systems containing IIF for the purpose of enabling the implementation of PIV are handled in full compliance with the Privacy Act.
- The organization ensures 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.
- The organization coordinates with appropriate department or agency officials to define consequences for violating privacy policies of the PIV program.
- The organization assures 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.
- The organization utilizes security controls described in NIST SP800-53, Recommend Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable.
- The organization ensures 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. Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless 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?

[*Note: This section assumes central card production and shared enrollment capabilities across agencies. Agencies may need to modify once final decisions on these work flow components are made.*]

Privacy risks include both system security and security of the PIV credential.

System security: [*Describe protections, e.g.*] The risks include the electronic security of the transmission networks and the physical and visual security of the systems and locations in the agency facility where the information is stored. These risks are addressed by the IT Security Plan established for this PIV program and any associated IT Security Plan identified for each component of the PIV program listed in Section 7. More specific program controls include protecting data through the use of FIPS approved encryption algorithms in transit and at rest.

Networks: [*Describe protections, e.g.*] The IT infrastructure that supports the PIV program is described in detail in the [*IT Security Plan*]. All data exchange takes place over encrypted data communication networks that are designed and managed specifically to meet the needs of the PIV Program. Private networks and or encryption technologies are used during the electronic transfer of information to ensure that Internet "eavesdropping" is not allowed and that data is sent only to its intended destination and to an authorized user, by an authorized user. Enrollment data may be temporarily stored at enrollment centers for encrypted batch transmission to the IDMS. Access is PIN protected.

Databases: [*Describe protections, and identify the administrative, operational and technical controls applied to protect this IDMS data repository containing biographical data, photo images and biometric identifiers.*]

Data Transmission: [*Describe protections, e.g.*] 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: [*Describe protections, e.g.*] 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).

[*For central card production only: e.g.*] The IDMS sends confirmed enrollment information to the card production facility 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: [*Describe protections, e.g.*] 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 personal ID number, pin and/or biometric (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.
- 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 control 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 [*agency*] and complete a training process associated with their specific role in the PIV process.

Separation of Duties Controls: [*Describe the roles of PIV Applicant, Sponsor, Registrar, PIV issuer and PIV Digital Signatory. Are the roles exclusively drawn? How does the agency ensure these roles do not overlap?*]

Security of ID credential issued to an employee or contractor is achieved by full compliance with the mandatory requirements of the Federal Information Processing Standard Publication 201 (FIPS Pub 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 ad 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 contactless access to stored information
- Employees are alerted to importance of protecting card
- Card expiration within 5 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 Who will have access to the information?

[*Sample Discussion provided.*] Authorized information technology (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 [*agency*] Office of Inspector General (OIG) may request and be given access to the data, and the [*agency*] General Counsel's Litigation Division may request and be given access to the data to represent [*agency*] in litigation matters related to the PIV system. The described access by OIG and OGC is authorized by section (b) (1) of the Privacy Act.

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

All [*agency*] 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.

[*Agency*] ensures this through legal agreements with its contractors and enforcement of internal procedures with all [*agency*] 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. Are audit procedures applied?

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 by the enrollment workstation or center. The enrollment record can only be viewed or retrieved by an [*agency*] enrollment official 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 will be enforced to ensure that only [*agency*] employment officer 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.?

For example, if a decision was made to increase the number of user roles so that access to information was further tightened, include such a discussion.

SECTION 7.0 DATA STORAGE AND RETENTION

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

The information collected to issue a PIV card is retained and used for [*XX years/months. Cite the National Archives and Records Administration (NARA) General Records Schedule for records pertaining to this program relevant to both the PIV I and PIV II.*]

SECTION 8.0 RESULTS OF FISMA REVIEW

8.1 Has the system completed a C&A as required by FISMA or other applicable standards?

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

8.3 Has the agency conducted a risk assessment, and identified and implemented appropriate technical, administrative, and operational security controls? [*List each type of control.*]

SECTION 9.0 ANALYSIS AND ASSESSMENT

[*Describe your agency's analysis and assessment.*]

9.1. Whether or not competing technologies were evaluated, describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

9.2 Did you evaluate competing technologies to assess and compare their ability to effectively achieve system goals?

9.3 If applicable, describe the competing technologies.

9.4 Changes made to the PIV process due to the assessment:

9.5 What unique issues does this system present?

9.6 What specific strategies are used to address these issues?

9.7 What unique issues are not mitigated completely? What are the potential impacts of these issues on privacy?

SECTION 10.0 CONCLUSIONS

[*Summarize the privacy risks identified in the above questions and the means by which you have mitigated and/or considered those risks.*]

SECTION 11.0 DETERMINATIONS OF OFFICIALS

The sensitivity of this system requires [*agency*] ensure that it meets the following requirements:

- Achieve an IT Security accreditation and certification 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 is considered adequate.