September 28, 2005

***** GENERIC DRAFT (90%)*****
(for agencies to select from as needed)

BACKGROUND INFORMATION FOR

PRIVACY ACT SYSTEM OF RECORDS NOTICE

"HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12), PERSONAL IDENTITY VERIFICATION FOR FEDERAL EMPLOYEES AND CONTRACTORS"

The following document is background information for a proposed Privacy Act System of Records Notice (SORN), to be published in the Federal Register for public notice and 60-day comment, as required by the Privacy Act of 1974, as amended, 5 U.S.C. § 552(a). This specific Notice is in response to Homeland Security Presidential Directive 12 (HSPD-12), "Personal Identity Verification for Federal Employees and Contractors," Aug. 27, 2004.

Because of the comprehensive nature of HSPD-12 and the new Federal-wide Personal Identity Verification (PIV) process, this Notice is composed of four parts. The four parts relate to the "life-cycle" of the PIV process – from initiating the background investigation, to using the PIV Card for both physical access (to buildings and space) and logical access (to computer systems):

- Part 1 of Notice: Background investigation (also refer to the existing Notice, OPM/Central-9, "Personnel Investigations Records" **[LINK]**).
- Part 2 of Notice: "Identity proofing" and registration (enrollment) of employees and contractors who are required to have a Personal Identity Verification (PIV) Card.
- Part 3 of Notice: Identity Management System (IDMS) and associated systems/ databases used to track/ monitor every step of the PIV process, from background investigation, identity proofing and registration (enrollment), through issuance and use of the PIV Card.
- Part 4 of Notice: Personal information contained on the new Federal-wide ID badge/ smart card referred to as the "Personal Identity Verification (PIV) Card."

This comprehensive Notice covers all HSPD-12 requirements and the entire PIV process. Agencies may adopt the Notice as-is, or they may use some content as a starting point for publishing their own Notice(s). For example, Agencies may decide to take the information from Part 3 and publish a separate Notice for the Identity Management System (IDMS) and associated systems/ databases. Or, they may publish a Notice specifically for the new IDMS, and a separate Notice for the other related systems. Alternatively, Agencies may publish one Notice on the several systems databases that support PIV, and a separate Notice for the PIV Card itself.

It is recommended that all Notices related to HSPD-12 make reference to each other, so that the public understands what personal information is being collected at different stages of the Personal Identity Verification (PIV) process, and how that personal information is used.

See next page for a sample System of Records Notice that combines all elements of HSPD-12 and PIV into one Notice (in four parts).

NOTE: This is a sample comprehensive 4-part Notice covering all phases of Homeland Security Presidential Directive 12 (HSPD-12) and the new Personal Identity Verification (PIV) process. Agencies may choose to adopt this Notice as-is, or may select material to create separate Notices, customized as desired.

September 22, 2005

***** GENERIC DRAFT *****

(for agencies to adopt as-is, or adapt as needed)

GOVERNMENT-WIDE PRIVACY ACT SYSTEM OF RECORDS NOTICE

"HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) PERSONAL IDENTITY VERIFICATION (PIV) FOR FEDERAL EMPLOYEES AND CONTRACTORS"

Agency Sponsor and number ____-__)

System name:
Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) for Federal Employees and Contractors.

Security classification:
Determined by each agency. For most agencies these records are administratively confidential. However, agencies responsible for national security or homeland security may classify some records or individual files within their system of records as secret.

Authority for maintenance of the system:
This Notice covers every step of the Personal Identity Verification (PIV) process, from background investigation, identity proofing and registration (enrollment), through issuance and use of the PIV Card for both physical access (to buildings) and logical access (to computer systems). Because of the comprehensive requirements of PIV, an extensive set of authorities is cited:

Legislation:

- Civil Service Act of 1883, Section 2 – original authority
- Public Law 82-298
- Public Law 92-261
- Public Law 93-579
- Public Law 107-347

- 5 U.S.C. (Title 5, U.S. Code), sections 552(a), 1303, 1304, 3301, 7701
- 22 U.S.C., sections 1434, 2519, 2585
- 32 U.S.C., section 686
- 40 U.S.C., section 11302(e)
- 42 U.S.C., sections 1874(c), 2165, 2455
- 44 U.S.C., section 3101, chapter 35, chapter 36

Executive Branch Orders, Directives, Policy, and Standards:

- Homeland Security Presidential Directive 12 (HSPD-12)
- Executive Orders 9397, 10422, 10450 (as amended by subsequent Executive Orders)
- 5 CFR (Title 5, Code of Federal Regulations), part 5
- OMB Circular A-130
- OMB Memoranda M-03-22, M-04-04, M-05-05, M-05-08, M-05-24
- Federal Information Processing Standards (FIPS) 140-2, 199, 201
- National Institute of Standards and Technology (NIST) Special Publications 800-37, 800-53, 800-63, 800-73, 800-76, 800-78, 800-79, 800-85

Purposes:

Beginning by Oct. 27, 2006 and to be completed by Oct. 27, 2007, all Federal employees and contractors will be required to use the new Federal-wide Personal Identity Verification (PIV) Card for access to Federal facilities as well as Federal information systems. Specifications for the new PIV Card are defined in the National Institute of Standards and Technology's (NIST) Federal Information Processing Standards 201 (FIPS 201) and NIST Special Publication 800-73. FIPS 201 and related NIST Special Publications are the implementing standards for HSPD-12.

Per the Federal Information Security Management Act of 2002, waivers to Federal Information Processing Standards are not allowed.

Because of the comprehensive nature of HSPD-12 and the new Personal Identity Verification (PIV) process, this Notice is composed of four parts. The four parts relate to the "life-cycle" of the PIV process – from initiating the background investigation, to using the PIV Card for both physical and logical access:

- Part 1 of this Notice covers: Background investigation files (also refer to the existing Federal-wide Notice on "Personnel Investigations Records," OPM/GENERAL-9) **[LINK].**

- Part 2 of this Notice covers: "Identity proofing" and registration (enrollment) of employees and contractors who are applying for a Personal Identity Verification (PIV) Card.
- Part 3 of this Notice covers: Identity Management System (IDMS) and associated systems/ databases used to track/ monitor every step of the PIV process, from background investigation, identity proofing and registration (enrollment), through issuance and use of the PIV Card.
- Part 4 of this Notice covers: Personal information contained on the new Federal-wide ID badge/ smart card known as the "Personal Identity Verification (PIV) Card."

This comprehensive Notice covers all HSPD-12 requirements and the entire PIV process as defined by FIPS 201 and the related NIST Special Publications.

Purposes – Part 1 of Notice: Background investigation files

Since President Eisenhower signed Executive Order 10450 in 1953, Federal employees have been required, as a condition of employment, to have (as a minimum) a standard background investigation known as the National Agency Check with Written Inquiries (NACI), or equivalent. Many subsequent Executive Orders have reaffirmed that requirement. Office of Personnel Management (OPM) regulations and guidelines implement this long-standing policy. For most civilian agencies, OPM investigators conduct the background investigations on a fee basis.

Homeland Security Presidential Directive 12 (HSPD-12), signed August 27, 2004, re-stated the requirement for background investigations for all Federal employees. It also extended the requirement for a NACI to long-term contractors (those working over 6 months). Agencies may exceed the minimum requirement by also requiring a NACI for shorter-term contractors, at the discretion of the Agency and according to Agency security policy and practices. Further, HSPD-12 stated that the Personal Identity Verification (PIV) process should be strengthened and standardized across the Federal Government.

OMB Memorandum M-05-24 **[LINK]**, which is the implementing Guidance for HSPD-12, states: "As defined below, Department and Agency heads must conduct a background investigation, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access to Federally controlled facilities and/ or information systems."

The basic information for the standard background investigation is based on the employee filling out Form SF-85 (for most positions) or SF-85P (for "positions of trust") or SF-86 (for positions requiring a national security clearance). On the SF-85 or SF-85P, the individual reports his/ her full name, Social Security Number (SSN), date of birth, addresses over the past 5 years, employers over the past 5 years, and schools attended.

Starting with the information from the Form SF-85 or SF-85P, the background investigator makes both written and oral inquiries regarding an individual's character and conduct, any arrest/ conviction record, etc. to determine suitability and fitness for Federal employment and loyalty to the United States. In addition to searches of records covering specific areas of an individual's background during the past five years, the full NACI includes all of the following National Agency Checks:

- Security/ Suitability Investigations Index (SSI)
- Defense Clearance and Investigation Index (DCII)
- FBI Name Check
- FBI National Criminal History Fingerprint Check.

Results of the investigation are documented in the employee's "background investigation file" and kept by:

- The employing agency
- The investigating agency (Office of Personnel Management)
- Law enforcement agencies (Federal Bureau of Investigations and the Department of Homeland Security)

Under HSPD-12, Federal contractors (longer than 6 months) are required to have the same NACI background investigation as Federal employees. As mentioned above, Agencies may also require NACIs for contractors who work less than 6 months. Therefore, this Notice covers both those who are Federal employees, as well as "private citizens" in the role of Federal contractors.

NOTE: OPM is responsible for the Notice covering the personal information required for the standard background investigation. See Notice OPM/GENERAL-9, "Personnel Investigations Records" at: _____.

Purposes – Part 2 of Notice: "Identity proofing" and registration (enrollment)

This part of the Notice covers the "identity proofing" and registration (enrollment) step in the overall PIV process. The purpose for having a stronger Federal-wide standard for PIV is to meet the four "control objectives" of HSPD-12. As directed by HSPD-12, "secure and reliable forms of identification" means identification that:

- "Is issued based on sound criteria for verifying an individual employee'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."

Personally identifiable records collected at this step include:

- Collecting a registration (enrollment) form from the individual at time of applying to receive a PIV Card. (This is required of employees when entering employment as well as when being renewed every 5 years.)
- Inspecting two identity-source documents in original form (one of which must be a Government-issued photo ID, and another must be from the acceptable list of documents on Form I-9, OMB No. 1115-0136, Employment Eligibility Verification). These two identity-source documents are then digitally scanned by the PIV Registration Authority (Registrar), and saved as electronic files in the Identity Management System.
- Taking a "head-and-shoulders" color photo that meets FIPS 201 specifications – to be placed:
  - In the individual's background investigation file
  - In the PIV master database known as the Identity Management System (IDMS) – per requirements of FIPS 201.
  - On the front of the PIV Card for visual verification of identity
  - As a digitized file on the PIV Card for electronic verification of identity (when the card is read by a card reader and the photo is displayed on a monitor for the guard to see)
- Capturing the full 10 fingerprints on a fingerprint card, for the FBI National Criminal History Fingerprint Check. These 10 fingerprints could be captured with ink on a card, or electronically with a fingerprint capture device.
- Capturing two index fingerprints – to be scanned and placed as a digital file on the PIV Card. NOTE: NIST standards have not yet been finalized on whether these digitized

index fingerprints must be either full image or "minutia" (key points for comparison).

The suggested registration (enrollment) form in the Federal Identity Management Handbook (July 2005 public draft) **[LINK]** collects basic information on the individual at time of registration (enrollment), such as:

- Full name
- Date of birth
- Position / job title
- Organization currently assigned to
- Work address
- Work phone number
- Work e-mail
- Home address
- Home phone number
- Home e-mail (optional)

This information is used to track and verify issuance of a PIV Card to an employee or a contractor. It also allows the PIV Card-issuing organization to verify that a background investigation (NACI or equivalent) was initiated and that, as a minimum, the FBI National Criminal History Fingerprint Check was adjudicated prior to the issuance of the PIV Card.

The information covered by Part 2 of this Notice is partly paper-based and partly electronic. Per FIPS 201 requirements, all documents from the "identity proofing" and registration (enrollment) step must also be scanned into the Identity Management System (IDMS)/ database described in Part 3 below. The specifications and standards for both collecting this specific information and for scanning them into the IDMS are described in Section 5 of FIPS 201.

"Separation of duties" is one of the key requirements for making the new ID badge "strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation" (one of the four control objectives of HSPD-12). This means that the person who does the "identity proofing" and registration (enrollment) of an applicant cannot be the same person who actually issues the ID badge (PIV Card). Therefore, the identity-proofing documents must be securely "passed on" to the next step in the PIV process, to an organization that has been independently certified (tested) and accredited (approved) to issue the new ID badges. See NIST Special Publication 800-79,

Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations."

The next section gives details on the entire PIV process.

Purposes – Part 3 of Notice: Identity Management System (IDMS) and associated systems/ databases

FIPS 201 (Appendix A, page 59) states that the IDMS is the "system of records" for the new PIV process. The "Identity Management System (IDMS)" is a comprehensive tracking system and database for the entire PIV process. There are also associated systems and databases that all agencies are required to use, to be compliant with the new PIV process.

Quoting from FIPS 201 (Appendix A):

> "**Identity Management System** – The Approval Authority shall maintain the IDMS that **shall be the system of records for PIV credentials issued.** It performs the identity proofing, verification and validation to establish identity claim validity. Shall provide a 1:many search to ensure the applicant has not enrolled under a different name. Shall confirm employment appropriate to the PIV request. Shall manage identity validation and verification services through government-wide standardized services which shall be provided in accordance with HSPD-11 **[LINK]**. Shall manage adjudication of identity claim. Shall approve issuance of PIV to applicant upon successful adjudication of identity claim.
>
> "A.2.7 Identity Verification Process
>
> - "The IDMS shall receive the completed package for PIV from Enrollment. The IDMS shall verify the integrity of that package by confirming completeness, accuracy, and digital signatures.
> - "The IDMS shall provide a means to confirm employment and sponsorship as identified in the package.
> - "The IDMS shall perform a 1:many search to assure that the individual identified in the package has not applied previously under a different name.
> - "The IDMS shall conduct the appropriate identity verification and validation using government-wide databases and services in accordance with HSPD-11 **[LINK]**.
> - "The Approval Authority shall provide adjudication of identity claim should any of these three core checks identify a potential risk.

- "After successful completion of the appropriate identity verification process, the Approval Authority shall approve card production for the credential. The Approval Authority may approve issuance of a PIV credential prior to completion of all core checks for identity verification and validation if these processes exceed ten days.
- "The IDMS shall be responsible to maintain:
  "1. Completed and signed PIV enrollment package;

  "2. Copies of the identity source documents;

  "3. Completed and signed background form received from the Applicant;

  "4. Results of the required background check;

  "5. Any other materials used to prove the identity of the Applicant;

  "6. The credential identifier such as an identity credential serial number;

  "7. The expiration date of the identity credential;

  "8. Unique minimal identity record for each approved Applicant;

  "9. Separated database indexed to the minimal identity record containing the original biometric data captured at enrollment. These data shall be encrypted at rest; and

  "10. Separated database of biometric data indexed to the minimal identity record supporting AFIS for 1:many identity checking.

"The IDMS shall provide services that:
  "1. Notify the Employee/Contractor Applicant of status of the PIV;

  "2. Notify the Employer of status of the PIV; and

  "3. Enable validation by anyone inquiring if an issued credential is still valid.

"The IDMS shall provide complete personalization and printing information for card production for all approved PIV credentials as required by the supporting card production facility's requirements. This information shall be provided to enable the full chain of trust between the individual, the

issuer, the identity verification performed, the credential and the biometric."

Purpose – Part 4 of Notice: Personal information contained on the new Federal-wide ID badge/ smart card known as the "Personal Identity Verification (PIV) Card"

For a complete list and description of PIV Card mandatory and allowed optional features, see FIPS 201. Pages 17-28 show and describe the visual features, and pages 29-36 gives specifications for the electronic features.

Agencies must implement all of the mandatory features, but can also select from pre-defined optional features – as allowed by FIPS 201. Of those mandatory and optional PIV Card features (from FIPS 201 pages 17-28), only some are personal in nature and therefore will be covered by Part 4 of this Notice:

FIPS 201 (pages 17-29) defines the mandatory and optional features of the new Federal-wide PIV Card. The allowable visual and electronic features are listed and displayed on pages 17-29 of FIPS 201. Of the visual and electronic features allowed by FIPS 201, **those that are personal or uniquely identifiable (or potentially so) are in bold print.** Mandatory features are marked with **:

- Visual features (mandatory):
  - Front of PIV Card:
    - **** Zone 1: Color photograph** (37 x 27.75 mm) – upper left corner of PIV Card
    - **** Zone 2: Name** – full name, printed directly under the photograph in capital letters (alternatively, pseudonyms as provided under the law)
    - ** Zone 8: Employee affiliation – for example, "contractor," "active duty," and "civilian"
    - ** Zone 10: Organizational affiliation – Department or Agency
    - ** Zone 14: Expiration date
  - Back of PIV Card:
    - ** Zone 1: Agency Card Serial #
    - ** Zone 2: Issuer Identification – consists of 6 characters for the department code, 4 characters for the agency code, ad a 5-digit number that uniquely identifies the issuing facility within the department or agency
- Visual features (optional):

- Front of PIV Card:
  - **Zone 3: Signature**
  - **Zone 4: Agency-specific text area** – agency-specific requirements, such as employee status
  - **Zone 5: Rank**
  - Zone 6: PDF bar code
  - Zone 9: Header – "United States Government" or other agency-specific information, such as identifying a Federal emergency responder role
  - Zone 11: Agency seal
  - Zone 12: Footer – "Federal Emergency Response Official"
  - Zone 13: Issue date
  - Zone 15: Color-coding for employee affiliation – blue = foreign nationals, red = emergency responder officials, green = contractors (NOTE: These colors are reserved and cannot be used for other purposes)
  - Zone 16: Photo border for employee affiliation – used with the photo to further identify employee affiliation
  - **Zone 17: Agency-specific data** – alternate location for agency-specific text if Zone 4 is not used
- Back of PIV Card:

  FIPS 201 NOTE: "In the case of the Department of Defense, the back of the card will have a distinct appearance. This is necessary to display information required by the Geneva Accord and to facilitate medical entitlements that are legislatively mandated.
  - Zone 3: Magnetic stripe
  - Zone 4: Return to – address of security department of the agency that the PIV Card should be returned to if found
  - **Zone 5: Physical characteristics** (as selected by agency, such as height/ weight, color of hair/ eyes, etc.)
  - Zone 6: Additional language for Emergency Responder Officials
  - Zone 7: Standard Section 499, Title 18 Language
  - Zone 8: Linear 3 of 9 Bar Code
  - **Zone 9: Agency-specific text** – in cases where other defined optional elements are not used, Zone 9 may be used for other department or agency-specific information. For example, emergency responder officials may use this area to provide additional details.

        - **Zone 10: Agency-specific text** – Zone 10 is similar to Zone 9 in that it is another area for providing department or agency-specific information. FIPS 201 NOTE: "Departments and agencies are encouraged to use Zones 9 and 10 prudently and minimize printed text to that which is absolutely necessary."
    - Electronic features (mandatory):
        - **** Fingerprints (2 index fingers, as a digitized file** – per issuance of final NIST Special Publication 800-76, "Biometric Data Specifications for Personal Identity Verification"). NOTE: NIST standards have not yet been finalized on whether these digitized index fingerprints must be either full image or "minutia" (key points for comparison).
        - **** Personal Identification Number (PIN)** – 6-digit or 8-digit PIN, for optional/ selected use, either for (1) physical access to highly secured buildings/ space; or (2) to log-on to sensitive computer systems ("assurance level 3 or 4") that require multi-factor authentication, beyond the typical user ID/ password
        - **** Card Holder Unique Identification Number (CHUID)** – to authenticate the card holder to the host computer system (comprised of the agency code + a sequential number for the employee, creating a unique number for all Federal employees, allowing interoperability of the PIV card throughout the Federal Government)
        - ** "PIV authentication key" – an asymmetric private key supporting card authentication for an interoperable environment
- Electronic features (optional, but must meet FIPS 201 specifications if on the PIV Card):
    - **Color photograph digitized on card as JPG file** (also displayable as a visual feature on monitor when read by card-reader). NOTE: The photograph is mandatory as a visual feature on the front of the card, but optional as a digitized file. The intelligence agencies requested that the photo not be a mandatory electronic feature. However, most agencies will choose to have the photo as both a visual feature on the front of the card, as well as an electronic feature that can be displayed on a monitor when read by a card-reader.
    - "Card authentication key" (optional) – may be either a symmetric (secret) key or an asymmetric private key for physical access
    - **"Digital signature key" (optional)** – an asymmetric private key supporting document signing (also known as a

public key infrastructure (PKI) digital certificate, used to "sign" transactions within computer application systems).

- "Key management key" (optional) – an asymmetric private key supporting key establishment and transport. This can also be used as an encryption key.
- "Card management key" (optional) – a symmetric key used for personalization and post-issuance activities.

System location:
Names of agencies and offices (with addresses) responsible for maintaining the master file of these records. If decentralized segments of some records are maintained, indicate the location of these records.

Categories of individuals covered by the system of records:
HSPD-12 and FIPS 201 require standard ID badges to be issued to all Federal employees and contractors. By October 27, 2006, all Federal agencies must begin issuing new FIPS 201-compliant ID badges/ smart cards to new employees and contractors. By October 27, 2007, agencies must have completed the replacement of existing ID badges for all current employees and contractors. The new ID badge/ smart card is known as the "Personal Identity Verification (PIV) Card."

This system of records notice covers individuals who require long-term access to Federally controlled buildings and Federally controlled Information systems as described below:

- All Federal employees who work in Federally controlled facilities as defined in Title 5 of the United States Code (5 U.S.C.) § 2105.
- Individuals under contract to the Federal government and who require access to Federal buildings and information technology systems, to whom the Agency would issue long-term Federal agency identification credentials, consistent with Agency's existing security procedures.
- At Agency's discretion, may or may not apply to short-term employees (such as summer interns) and short-term contractors (less than 6 months). Decision to issue PIV-II compliant ID badges and the prerequisite background investigation for short-term employees and contractors is an agency risk-based decision. If PIV-II Cards are issued to short-term employees and contractors, they are subject to collection of personal information as defined in this Notice.

- Does **not** apply to occasional visitors or short-term guests to whom the Agency would issue temporary identification (with restricted access).

Federally controlled buildings are defined in FIPS 201 as:

- Federally owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any of which is under the jurisdiction, custody or control of a department or agency covered by HSPD-12.
- Federally controlled commercial space shared with non-government tenants. For example, if a department or agency leases the 10th floor space of a commercial building, a system of records would apply to employees and contractors who work on the 10th floor only.

Federally controlled information systems are defined by the Federal Security Management Act of 2002, (44 U.S.C. § 3544(a)(1)(A)(ii)), as "Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."

Categories of records in the system:

Because of the comprehensive nature of HSPD-12 and the new Personal Identity Verification (PIV) process, this Notice is composed of four parts. The four parts relate to the "life-cycle" of the PIV process – from initiating the background investigation, to using the PIV Card for both physical access (to buildings and space) and logical access (to computer systems):

- Part 1: Background investigation files (refer to OPM/Central-9, "Personnel Investigations Records")
- Part 2: "Identity proofing and registration (enrollment) of employees and contractors
- Part 3: Identity Management System (IDMS) and associated systems/ databases – which track/ control all information needed for the new Personal Identity Verification (PIV) process.
- Part 4: Personal information contained on the new Federal-wide ID badge/ smart card known as the "Personal Identity Verification (PIV) Card"

Categories of records – Part 1 of Notice: Complete background investigation files resulting in a National Agency Check with Written Inquiries (NACI) or equivalent.

This includes name, Social Security Number (SSN), date of birth, addresses in the past 5 years, employment in the past 5 years, and where the individual went to high school and college (as applicable). The background investigation file also includes the result of the full NACI investigation, which includes the FBI Fingerprint Check and the FBI National Criminal History Name Check.

Categories of records – Part 2 of Notice: "Identity proofing" and registration (enrollment) of Federal employees and contractors

- The paper records that are collected from the individual at time of registration (enrollment) to receive a PIV Card (when entering employment or when being renewed every 5 years).
- Scanning of two identity-source documents (one of which must be a Government-issued photo ID).
- Taking a "head-and-shoulders" photo that meets FIPS 201 specifications – to be placed:
  - In the individual's background investigation file
  - In the PIV master database known as the Identity Management System (IDMS) – per requirements of FIPS 201, which is the implementing standard for HSPD-12.
  - On the front of the PIV Card (top left corner) for visual verification of identity
  - As a JPG file on the PIV Card for electronic verification of identity (when the card is read by a card reader and the photo is displayed on a monitor for the guard to see)
- Capturing two index fingerprints – to be scanned and placed as a digital file on the PIV Card.

Categories of records – Part 3 of Notice: Identity Management System (IDMS) and associated systems/ databases used to track/ monitor every step of the PIV process, from background investigation, identity proofing/ registration, through issuance and use of the PIV Card.

As stated in FIPS 201 (page 61): "The IDMS shall be responsible to maintain:

"1. Completed and signed PIV enrollment package;

"2. Copies of the identity source documents;

"3. Completed and signed background form received from the Applicant;

"4. Results of the required background check;

"5. Any other materials used to prove the identity of the Applicant;

"6. The credential identifier such as an identity credential serial number;

"7. The expiration date of the identity credential;

"8. Unique minimal identity record for each approved Applicant;

"9. Separated database indexed to the minimal identity record containing the original biometric data captured at enrollment. These data shall be encrypted at rest; and

"10. Separated database of biometric data indexed to the minimal identity record supporting AFIS for 1:many identity checking.

Categories of records – Part 4 of Notice: "Personal information" contained on the new Federal-wide ID badge/ smart card known as the "Personal Identity Verification (PIV) Card"

The National Institute of Standards and Technology's (NIST) Federal Information Processing Standards 201 (FIPS 201) defines the mandatory and optional features of the new Federal-wide PIV Card. The allowable visual and electronic features are listed and displayed on pages 17-38 of FIPS 201. Of the visual and electronic features allowed by FIPS 201, only the following are personal or uniquely identifiable:

- Visual features (mandatory):
  - ** Zone 1: Color photograph (37 x 27.75 mm)
  - ** Zone 2: Name
  - ** Zone 1: Agency Card Serial #
- Visual features (optional):
  - Physical characteristics (as selected by agency, such as height/ weight, color of hair/ eyes, etc.)
- Electronic features (mandatory):
  - ** Color photograph digitized on card as JPG file (also displayable as a visual feature on monitor when read by card-reader)
  - ** Fingerprints (2 index fingers, as a digitized file, either pattern or "minutia" – per issuance of final NIST SP 800-76, "Biometric Data Specifications for Personal Identity Verification")

- ** Personal Identification Number (PIN) – 4 digits, for optional/ selected use either for (1) physical access to highly secured buildings/ space; or (2) to log-on to sensitive computer systems ("level 3") that require multi-factor authentication, beyond the typical user ID/ password
- ** Card Holder Unique Identification Number (CHUID) – to authenticate the card holder to the host computer system (comprised of the agency code + a sequential number for the employee, creating a unique number for all Federal employees, allowing interoperability of the PIV card throughout the Federal Government)
- ** "PIV authentication key" – an asymmetric private key supporting card authentication for an interoperable environment

- Electronic features (optional, but must meet FIPS 201 specifications):
  - "Digital signature key" (optional) – an asymmetric private key supporting document signing (also known as a public key infrastructure (PKI) digital certificate, used to "sign" transactions within computer application systems)

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Overall, the purpose of Personal Identity Verification (PIV) information is guided by the four "control objectives" of HSPD-12. As directed by HSPD-12, "secure and reliable forms of identification" means identification that:

- Is issued based on sound criteria for verifying an individual employee'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.

PIV information is used in various ways, as described in the four Parts below.

Routine uses – Part 1 of Notice: Background investigation files

Form SF-85 or SF-85P is sent to Federal, State, local, and foreign authorities for use in conducting criminal, civil, or regulatory investigations, to verify the identity of an employee.

Disclosure of background investigation results may be made for routine uses as allowed by the Privacy Act of 1974, indicated below:

1. To a Congressional office in response to an inquiry from that office made at the request of the subject of a record.
2. To the Department of Justice (DOJ) or a court when the Agency determines that the use of such records by DOJ or a court is relevant and necessary to the litigation, provided, however, that in each case, the Agency determines that such disclosure is compatible with the purpose for which the records were collected and allowable under the Privacy Act of 1974, as amended.
3. To the Department of Homeland Security (DHS), when required to investigate terrorism-related matters.
4. To Federal, State, and local law enforcement agencies and private security contractors, as appropriate, information necessary:

    - to enable them to protect the safety of (Agency) employees and customers, the security of the (Agency) workplace, the operation of (Agency) facilities, or
    - to assist investigations or prosecutions with respect to activities that affect such safety and security or activities that disrupts the operation of the (Agency).

5. To the Internal Revenue Service (IRS), as necessary, for the purpose of auditing the Agency's compliance with safeguard provisions of the Internal Revenue Code of 1986, as amended. (Can be used by other Agencies if they have similar authority).

Routine uses – Part 2 of Notice: "Identity proofing" and registration of employees and contractors who are applying for a Personal Identity Verification (PIV) Card

The approved "routine uses" of the "identity proofing" and registration information (as fully described in the sections above) is for internal agency use to verify the identity of the person applying for a PIV Card.

Routine uses – Part 3 of Notice: Identity Management System (IDMS) and associated systems/ databases – which track/ control all information needed for the new Personal Identity Verification (PIV) process.

As explained in detail in the sections above, the IDMS is the master database which is needed to track every step of the process that results in issuance and use of the new Federal-wide ID badge, known as the PIV Card. Approved "routine uses" of the information stored in the IDMS are:

- Recording the results of the background investigation – for use in verifying whether an individual is eligible for a PIV Card.
- Storing a scanned copy of the identity source documents required at the "identity proofing" and registration step – to verify the person's identity prior to issuance of a PIV Card.
- Storing the two index fingerprints as a digital file – for potential use in the "1:many" verification step.
- Storing the status of PIV Card issuance and the expiration date – for determining if a PIV Card is valid.

Routine uses – Part 4 of Notice: Personal information contained on the new Federal-wide ID badge/ smart card known as the "Personal Identity Verification (PIV) Card"

As explained in detail in the sections above, pre-specified and limited personal information is actually stored on the PIV Card. The approved "routine uses" of this personal information, consistent with the intent of HSPD-12 and its four control objectives, are:

- To allow physical access to Federal facilities
- To allow logical access to Federal computer systems

If agencies intend to use the personal information on the PIV Card for any other use, OMB Memorandum M-05-24 states that it should be consistent with the four control objectives of HSPD-12. As directed by HSPD-12, "secure and reliable forms of identification" means identification that:

- "Is issued based on sound criteria for verifying an individual employee'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."

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Information is maintained in electronic or paper formats as described in detail in the sections above.

Retrievability:

Retrievability –Part 1 of Notice: Background investigation files

Background investigation files can be retrieved by name or by Social Security Number (SSN).

Retrievability – Part 2 of Notice: "Identity proofing" and registration of employees and contractors who are applying for a Personal Identity Verification (PIV) Card

These records (as described in the purposes section above) can be retrieved by name or by Social Security Number (SSN).

Retrievability – Part 3 of Notice: Identity Management System (IDMS) and associated systems/ databases – which track/ control all information needed for the new Personal Identity Verification (PIV) process.

As described in detail in the Purposes section above, the Identity Management System (IDMS) is a comprehensive tracking system and database for the entire PIV process. There are also associated systems and databases that all agencies are required to use, to be compliant with the new PIV process. The IDMS performs the identity proofing, verification, and validation to establish identity claim validity. Per FIPS 201, each Agency's IDMS is responsible to maintain the following records – and therefore be able to retrieve on any of the types of information below:

"1. Completed and signed PIV enrollment package;

"2. Copies of the identity source documents;

"3. Completed and signed background form received from the Applicant;

"4. Results of the required background check;

"5. Any other materials used to prove the identity of the Applicant;

"6. The credential identifier such as an identity credential serial number;

"7. The expiration date of the identity credential;

"8. Unique minimal identity record for each approved Applicant;

"9. Separated database indexed to the minimal identity record containing the original biometric data captured at enrollment. These data shall be encrypted at rest; and

"10. Separated database of biometric data indexed to the minimal identity record supporting AFIS for 1:many identity checking."

Safeguards:

Paper records: Comprehensive paper records are kept in locked metal file cabinets in the agency's Headquarters offices which are responsible for background investigations and for ID badge issuance. Limited paper records (limited in scope as well as limited in number of employees/ contractors) are kept in the agency's Regional Offices. Access to the records is limited to those employees who have a need for them in the performance of their official duties.

Electronic records: Comprehensive electronic records are kept in the Identity Management System (IDMS), managed by the office responsible for ID badge issuance. Access to the IDMS is restricted to those with a specific role in the new Personal Identity Verification (PIV) process. Broad access to IDMS is further restricted to those who have specific need for access but who also have received a special "sensitive systems" background investigation. Limited access to IDMS is granted to selected staff in Headquarters and Field Offices, limited to those staff having specific duties in the PIV process involving their organization's employees.

To further safeguard the records collected and used for the PIV process, OMB Memorandum M-05-24 outlined the privacy requirements for HSPD-12 that all agencies must follow:

> **"6. How must I consider privacy in implementing the Directive?**
>
> "You are already required under the Privacy Act of 1974 (5 U.S.C. § 552a), the E-Government Act of 2002 (44 U.S.C. ch. 36), existing OMB policy and section 2.4 of the Standard to satisfy privacy and security requirements. Implementing the Directive does not alter these requirements. In addition, **prior to identification issuance you must:**
>
> "A. Ensure personal information collected for employee and contractor identification purposes is handled consistent with the Privacy Act of 1974 (5 U.S.C. § 552a).
>
> "B. Assign an individual to be responsible for overseeing the privacy-related matters associated with implementing this Directive.
>
> "C. Submit to OMB, and make publicly available, a comprehensive privacy impact assessment (PIA) of your HSPD-12 program, including analysis of the information technology systems used to implement the Directive. The PIA must comply with section 208 of the E-Government Act of 2002 (44 U.S.C. ch. 36) and OMB Memorandum M-03-22 of September 26, 2003, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002." You must periodically review and update the privacy impact assessment. Email your completed PIA to pia@omb.eop.gov.

"D. Update the pertinent employee and contractor identification systems of records notices (SORNs) to reflect any changes in the disclosure of information to other Federal agencies (i.e. routine uses), consistent with Privacy Act of 1974 (5 U.S.C. § 552a) and OMB Circular A-130, Appendix 1.11. These SORNs should be periodically re-reviewed to ensure accuracy.

"E. Collect information using only forms approved by OMB under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. ch. 35), where applicable. Departments and agencies are encouraged to use Standard Form 85, Office of Personnel Management Questionnaire for Non-Sensitive Positions (OMB No. 3206-0005) or the Standard Form 85P, Office of Personnel Management Questionnaire for Positions of Public Trust (OMB No. 3206-0005) when collecting information. If you plan to collect information from individuals covered by the PRA using a new form you must obtain OMB approval of the collection under the PRA process.

"F. Develop, implement and post in multiple locations (e.g., agency intranet site, human resource offices, regional offices, provide at contractor orientation, etc.) your department's or agency's identification privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification credentials are revoked, and sanctions for employees violating agency privacy policies.

"G. Adhere to control objectives in section 2.1 of the Standard. Your department or agency may have a wide variety of uses of the credential not intended or anticipated by the Directive. These uses must be appropriately described and justified in your SORN(s) and PIA."

Retention and disposal:

These records are retained and disposed of in accordance with records schedules approved by the National Archives and Records Administration (NARA). Generally, the information covered by this Notice is retained for the length of service of the individual and then destroyed by shredding; picture passes, once surrendered, also are destroyed by shredding.

System manager(s) and address:

List agency, office, address (determined by Agency).

Notification procedure:

An individual can determine if this system contains a record pertaining to him/her by contacting the following address: _____ (List agency, office, 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 such as a Government-issued photo ID. An individual requesting notification via mail or telephone must furnish a minimum of his/her name, date of birth, Social Security Number, and address in order to establish identity.

Record access procedures:

Same as notification procedures. Requesters should also reasonably specify the record contents being sought. The Department's rules for providing access to records of the individual concerned appear in __ CFR part __. If additional information or assistance is required, contact the Agency's Privacy Act Officer.

Contesting record procedures:

Same as notification procedures. Requesters should also reasonably identify the record, specify the information they are contesting, and state the corrective action sought and the reasons for the correction along with supporting justification showing how the record is incomplete, untimely, inaccurate, or irrelevant.

Record source categories:
Information in these files is received from various sources, as described for each Part below:

Part 1: Background investigation files (refer to OPM/Central-9, "Personnel Investigations Records"): Records are collected from:

- The employee/ contractor (SF-85 or SF-85P)
- Results of the FBI Name Check and FBI Fingerprint Check
- Results of potential interviews and written inquiries by the background investigator (of employment and residences for the past 5 years)
- Other sources at the discretion of the background investigator

Part 2: Enrollment/ registration of employees and contractors: Records are collected from the employee/ contractor in 4 ways:

- Filling out an application form to request a PIV Card (which typically requires basic information such as full name full name, date of birth, home address, home phone #, and home e-mail)
- Scanning of two identity-source documents (one of which must be a Government-issued photo ID)
- Taking a "head-and-shoulders" color photograph;
- Capturing two index fingerprints – to be scanned and placed as a digital file on the PIV Card

Part 3 of Notice: Identity Management System (IDMS) and associated systems/ databases – which track/ control all information needed for the new Personal Identity Verification (PIV) process.

Records in the IDMS are collected during the background investigation phase (Part 1 above) and the enrollment/ registration phase (Part 2 above).

Part 4 of Notice: "Personal information" contained on the new Federal-wide ID badge/ smart card known as the "Personal Identity Verification (PIV) Card"

The amount of data on the PIV Card is limited both by its capacity (64 kilobytes of memory), as well as by the Federal-wide specifications in FIPS 201, which defines which features and data are mandatory, and which ones are optional. No other features or data is allowed to be put on the PIV Card, if not specified by FIPS 201 (pages 17-38). Of the visual and electronic features allowed by FIPS 201, only the following are personal or uniquely identifiable:

- Color photograph
- Full name
- Agency card serial #

- Physical characteristics (as selected by agency, such as height/ weight, color of hair/ eyes, etc.)
- Fingerprints (2 index fingers, as a digitized file, either pattern or minutia – per issuance of final NIST Special Publication 800-76, "Biometric Data Specifications for Personal Identity Verification")
- 6-digit or 8-digit Personal Identification Number (PIN)
- Card Holder Unique Identification Number (CHUID)
- "PIV authentication key" – an asymmetric private key supporting card authentication for an interoperable environment
- "Digital signature key" (optional) – an asymmetric private key supporting document signing (also known as a public key infrastructure (PKI) digital certificate, used to "sign" transactions within computer application systems).

Systems exempted from certain provisions of the Privacy Act:

None.