



**U.S. Department of the Interior
Personal Identity Verification (PIV)
Policy and Guide
For
Federal Employees and Contractors**

December, 2005

**Guidance complies with
Homeland Security Presidential Directive 12 (HSPD-12)
And
Federal Information Processing Standards 201 (FIPS 201)**

Final Version 1.0

Document Information and Revision History

Version	Date	Author(s)	Revision Notes
1 st Draft	12/14/2005	HSPD-12 Core	Initial Draft
2 nd Draft	12/21/2005	Cyndy Anderson	Updates included from MIT
Final	12/22/2005	Cyndy Anderson	Final updates included from HSPD-12 team.

TABLE OF CONTENTS

CHAPTER 1 – INTRODUCTION 4

 1.1 PURPOSE.....4

 1.2 BACKGROUND5

 1.3 APPLICABILITY5

 1.4 SCHEDULES AND DEADLINES6

 1.5 ABBREVIATIONS7

 1.6 DEFINITIONS.....8

CHAPTER 2 – PERSONAL IDENTITY VERIFICATION, PART I (PIV-I) 11

 2.1 PIV-I APPLICABILITY 11

 2.2 PRIVACY POLICY..... 11

 2.3 BACKGROUND INVESTIGATION REQUIREMENTS.....12

 Figure 1: High-Level PIV-I Process 13

 2.4 REGISTRATION, IDENTITY PROOFING, & CREDENTIAL ISSUANCE.....13

 Figure 2 Process Overview.....20

 2.6 REPLACEMENT CREDENTIALS.....21

 2.7 PROVISIONAL CREDENTIALS21

 2.8 TEMPORARY CREDENTIALS21

 2.9 VISITOR CREDENTIALS22

 2.10 VOLUNTEER CREDENTIALS.....22

 2.11 CONTRACTING IMPACTS22

 2.12 AUDIT & RECORDS MANAGEMENT.....22

CHAPTER 3 – TRAINING 23

 3.1 WHERE TO GET ASSISTANCE.....23

 3.2 REPORTING REQUIREMENTS.....23

APPENDICIES 24

 Appendix A OMB Memo M-05-24 24

 APPENDIX B PIV-I Credential Request Form27

 APPENDIX B -1 Instructions for PIV I Form29

 APPENDIX B -1 Instructions for PIV I Form30

 Appendix C PIV Card Usage Privacy Act Notice.....34

 APPENDIX D I-9 Documents Acceptable for Identity Proofing.....36

 APPENDIX E Appeal Rights for the Denial of a Credential38

 Appendix F Acquisition Policy Release 2006-3, October 18, 2005 (DIAPR).....40

 Appendix G Definition of Card Issuance and Facility Guidance44

 Appendix H Model Statement of Work/Performance Work Statement Language.....47

 Appendix I PIV Information Notice49

 Appendix J Checklist for Review of a Privacy Act System or Records Maintenance Practices.49

 Appendix J Checklist for Review of a Privacy Act System or Records Maintenance Practices.50

 Appendix K Background Investigation Scheduling.....53

(This page intentionally left blank.)

Chapter 1 – Introduction

1.1 PURPOSE

This DOI Guidance provides policies and procedures governing the Personal Identity Verification (PIV) process and Smartcard (DOI ID Badge) issuance requirements of the following directive, standards, and policies:

[Homeland Security Presidential Directive 12 \(HSPD-12\)](#), “Policy for a Common Identification Standard for Federal Employees and Contractors,” dated August 27, 2004

National Institute of Standards and Technology (NIST) [Federal Information Processing Standards 201 \(FIPS 201\)](#), Personal Identity Verification (PIV) of Federal Employees and Contractors, dated February 25, 2005

[Office of Management and Budget \(OMB\) Memorandum M-05-24](#), dated August 5, 2005

[HSPD-12](#) mandates the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (and contractor employees).

[FIPS 201](#) defines a reliable, government-wide Personal Identity Verification (PIV) process for use in applications such as access to federally controlled facilities and information systems. It also specifies a PIV Part II (PIV-II) system within which common identification credentials can be created and later used to verify a claimed identity.

[OMB Memorandum M-05-24](#) provides guidance for implementing the requirements in FIPS 201 and HSPD-12. The guidance clarifies timelines, applicability, and the requirements of PIV-I.

For purposes of this Guidance, DOI organizations are collectively referred to as “Offices.”

No provision in this Guidance shall have the effect of nullifying or limiting protections for equal employment opportunity as defined under Title VII of the Civil Rights Act, 42 U.S.C. 3535(d), Executive Order (EO) 11478, or DOI’s implementing regulations under 24 CFR Part 7. DOI will not implement this Guidance in such a way as to impede equal employment opportunity on the basis of race, color, religion, sex, national origin, age, or disability.

1.2 BACKGROUND

In years past, government agencies required levels and means of authenticating the identification of Federal employees and contractors as a requirement to enter government facilities and use of government systems. Where appropriate, the agencies also implemented authentication mechanisms to allow access to specific areas or systems. The methods and levels of assurance for authentication and authorization, (i.e., identification and permission) varied widely from agency to agency, and sometimes within a single agency.

[HSPD-12](#) requires that all government agencies develop specific and consistent standards for both physical and logical identification systems. The National Institute of Standards and Technology's (NIST's) [FIPS 201](#) establishes detailed standards on implementing processes and systems to fulfill the requirements of HSPD-12. FIPS 201 outlines two phases to implementing an HSPD-12 program. Part I (PIV-I) describes the registration and identity proofing process that must be in place beginning October 27, 2005. Part II (PIV-II) describes the technical and interoperability requirements of an HSPD-12-compliant system that must be in place beginning October 27, 2006. This Guidance addresses the PIV-I requirements only.

The 2002 [Federal Information Security Management Act \(FISMA\)](#) does not permit waivers to the FIPS 201 standards.

1.3 APPLICABILITY

According to FIPS 201, the standard “is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for ‘national security systems’ as defined by 44 U.S.C. §3542(b)(2).”

Specifically, PIV-I applies to all Federal employees, as defined in title 5 U.S.C §2105 “Employee,” within a department or agency. In addition, all individuals under long-term (6 months or longer) contract to the Federal government will be subject to PIV.

It is not required that temporary employees (less than 6 months), short-term guests, and occasional visitors to Federal facilities be subject to PIV-I. These individuals can be issued alternate credentials as described in section 2.8 of this Guidance. DOI reserves the right to subject any individual to the PIV-I process following a risk-based assessment. Office of Law Enforcement and Security Memorandum, Definition of Card Issuance and Facility Guidance Regarding HSPD-12, dated July 14, 2005 ([Appendix G](#)), outlines requirements for temporary federal employees, contractors, and

others affiliated with the agency for less than 6 months. Background investigations are long-standing requirements and not a new requirement of the HSPD-12 and PIV-I process.

([Appendix A](#) for an excerpt from [OMB Memorandum M-05-24](#))

1.4 SCHEDULES AND DEADLINES

Per HSPD-12, FIPS 201, and OMB Memorandum 05-24, all Federal Agencies must create and implement a PIV-I-compliant process beginning no later than October 27, 2005.

All Agencies must create and begin implementation on a PIV-II-compliant system for new employees and contractors beginning no later than October 27, 2006.

All existing DOI contractors must be identity proofed (with at minimum a National Agency Check with Written Inquiries (NACI)) no later than October 27, 2007 or upon contract renewal or ID expiration, whichever is earlier.

All Federal employees with less than 15 years of Federal service, as of October 27, 2005, must be identity proofed with at minimum a NACI no later than October 27, 2007.

All Federal employees with more than 15 years of Federal service, as of October 27, 2005, whose NACI or other OPM approved background investigation is not on file must be identity proofed with at minimum a NACI, no later than October 27, 2008.

Access to DOI's local area network (LAN) will require use of the PIV-II Card by employees and contractors no later than October 27, 2007.

Access to DOI's NCI and level 4 physical facilities (GSA-owned and leased space, or others as deemed necessary based on risk assessment) will require use of the PIV-II Card by employees and contractors no later than October 27, 2007. ([Appendix G](#))

1.5 ABBREVIATIONS

BI:	Background Investigation
CHUID:	Cardholder Unique Identifier
DHS:	Department of Homeland Security
e-QIP:	Electronic Questionnaire for Investigations Processing
FBI:	Federal Bureau of Investigations
FBI FP Check:	FBI National Criminal History Fingerprint Check
FIPS:	Federal Information Processing Standards
FISMA:	Federal Information Security Management Act
HSPD:	Homeland Security Presidential Directive
IDMS:	Identity Management System
LACS:	Logical Access Control System
NAC:	National Agency Check
NACI:	National Agency Check with Inquiries
NIST:	National Institute of Standards and Technology
OCIO:	Office of the Chief Information Officer
OIG:	Office of the Inspector General
OMB:	Office of Management and Budget
OPM:	Office of Personnel Management
PACS:	Physical Access Control System
PIV:	Personal Identity Verification
PIV-I:	Personal Identity Verification, Part I
PIV-II:	Personal Identity Verification, Part II
PKI:	Public Key Infrastructure

1.6 DEFINITIONS

Access control – the process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also “logical access control system” and “physical access control system.”

Authentication - the process of establishing an individual’s identity and determining whether individual Federal employees or contractors are who they say they are.

Authorization - process of giving individuals access to specific areas or systems based on their rights for access and contingent on successful authentication.

Background Investigation – any one of various Federal investigations conducted by OPM, the FBI, or by Federal departments and agencies with delegated authority to conduct personnel security background investigations.

Biometric – a measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.

Contractor – see “Employee.”

Employee – as defined in Executive Order (EO) 12968, “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts on behalf of an agency as determined by the agency head. See also “Employee” as defined in title 5 U.S.C §2105.

e-QIP Tracking Number – Number assigned by e-QIP to each Form SF-85 application. For those Interior bureaus and offices using e-QIP, the tracking number must be written on the fingerprint card when it is submitted to OPM in order to bind the fingerprint card to the proper applicant.

FBI FP Check – National Criminal History Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI, and is the minimum requirement for provisional card issuance.

FD-258 - Fingerprint Chart to accompany the NACI request when the individual to be investigated is a contractor (neither a Federal employee nor an applicant for Federal employment), or when agreed to by OPM.

Identity Management System (IDMS) - one or more systems or applications that manage the identity verification, validation, and card issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.

Identity-proofing – the process of providing identity source documents (e.g., driver’s license, passport, birth certificate, etc.) to a registration authority, or the process of verifying an individual’s information that he or she is that individual and no other. FIPS 201 requires that one of these documents be an original State or Federal Government-issued photo ID, and the other be from the approved set of identity documents listed on Form I-9.

Logical Access Control System (LACS) – protection mechanisms that limit users' access to information technology (IT) systems by restricting their form of access to those systems necessary to perform their job function. These LACS may be built into an operating system, application, or an added system.

National Agency Check (NAC) – The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index, Defense Clearance and Investigation Index, FBI Name Check, and FBI National Criminal History Check.

National Agency Check with Inquiries (NACI) – the basic and minimum investigation required of all Federal employees and contractors consisting 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. A NACI also includes written inquiries and searches of records covering specific areas of an individual’s background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

Physical Access Control System (PACS) – protection mechanisms that limit users' access to physical facilities or areas within a facility necessary to perform their job function. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

PIV-II Credential – a government-issued identity credential, referred to as a Smart Card, which contains a contact and contact-less chip. The cardholder’s facial image will be printed on the card along with other identifying information and security features that can be used to authenticate the user for physical access to federally controlled facilities. The card may include a PKI certificate, which controls logical access to federally controlled information systems.

Public Key Infrastructure (PKI) – A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.

SF-87 - Fingerprint Chart for Federal employee(s) or applicant for Federal employment.

Submitting Office Identifier (SOI) – Number assigned by OPM to identify office that submitted the NACI request.

Temporary Employee - Temporary, Term, Student (SCEP, STEP), or intern paid or obtaining some type of benefit directly from DOI

VIP – See “Volunteer”

Volunteer - a non-paid individual working under the supervision of DOI.

Chapter 2 – Personal Identity Verification, Part I (PIV-I)

2.1 PIV-I APPLICABILITY

PIV-I requires the implementation of registration, identity proofing, and issuance procedures in line with the requirements of FIPS 201. PIV-I does not require the implementation of any new systems or technology.

DOI will continue to issue existing credentials (ID badges) under the temporary paper-based process, but the process for credential application and issuance will change, in compliance with HSPD-12 and FIPS 201.

2.2 PRIVACY POLICY

HSPD-12 explicitly states that “protect[ing] personal privacy” is a requirement of the PIV system. As such, DOI Offices shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in FIPS 201, as well as those specified in Federal privacy laws and policies, including but not limited to Section 207 of the E-Government Act of 2002, the [Privacy Act of 1974, as amended \(5 U.S.C. §552a\)](#), and [OMB Memorandum M-03-22](#), as applicable.

Personal Identify Verification records are subject to the Privacy Act and E-Government Act of 2002 requirements. DOI Offices and staff that collect, maintain, safeguard and use this information must comply with the Government statutory requirements and Policy, and DOI Privacy Act regulations (43 CFR 2.45 – 2.79) and DOI Privacy Act manual sections (383 DM Chapters 1-13).

The Departmental Privacy Act regulation requirements on safeguarding Privacy Act information must be used to ensure that appropriate safeguards are in place for handling PIV information (refer to 43 CFR 2.51 and 383 DM 8).

Ensure that those authorized to access personnel records subject to the Privacy Act understand how to apply the Act’s restrictions on disclosing information from a system of records, and specific Privacy Act system of records instructions.

See OPM’s Guide to Personnel Recordkeeping, Chapters One and Six, at: <http://www.opm.gov/feddata/recguide.pdf> for instructions on proper safeguarding of personnel records.

One new privacy measure is that certain information on PIV information be provided to card applicants ([Appendix C](#)). Another new measure is that the Department post in multiple locations the Department’s PIV Privacy Act statement/notice, complaint procedures, and appeals procedures for those denied identification or whose identification credentials are revoked and sanctions for employees violating agency privacy policies ([Appendix I](#)) and post the notice.

2.3 BACKGROUND INVESTIGATION REQUIREMENTS

A National Agency Check with Inquiries (NACI) is the minimum background investigation (BI) that must be performed for all employees and contractors, except where the position designation requires a higher-level BI. In such cases, the BI shall be commensurate with the risk and security controls prescribed in the Position Designation or in accessing, managing, using, or operating Federal resources, including federal facilities and federal information systems as defined in [OMB Memorandum M-05-24](#).

[Appendix K](#) describes the types of forms required for various background investigations and OPM scheduling and contact information.

Locating and referencing a completed and successfully adjudicated NACI or unexpired higher-level BI may also satisfy the requirements. To locate and reference a previously completed and successfully adjudicated NACI, contact the Bureau/Office Personnel Security Office or Human Resources Office as appropriate. If the applicant indicates that he/she has already been the subject of a Federal BI without a subsequent break in Federal employment, or Federal contracting employment not exceeding two (2) years, the applicant will be asked to furnish specific information, which will be used to verify the BI. The Office Human Resources (OHR) may meet the above requirements by completing the Form SF-75, Request for Preliminary Employment Data, Section K, Security Data, for federal employees transferring to the Department.

The Office of Human Resources (OHR) is responsible for determining the position sensitivity designation for all applicant positions, and for ensuring that employees have the appropriate investigation commensurate with that determination. Bureaus/Offices are responsible for ensuring periodic reinvestigations are scheduled as required.

At a minimum, the National Criminal History Fingerprint Check (FBI FP) portion of a NACI must be completed prior to issuance of any credential. The Advance NAC report consists of a search of the following three searches:

- OPM Security/Suitability Investigations Index (SII)

- FBI's arrest records

- FBI FP Check

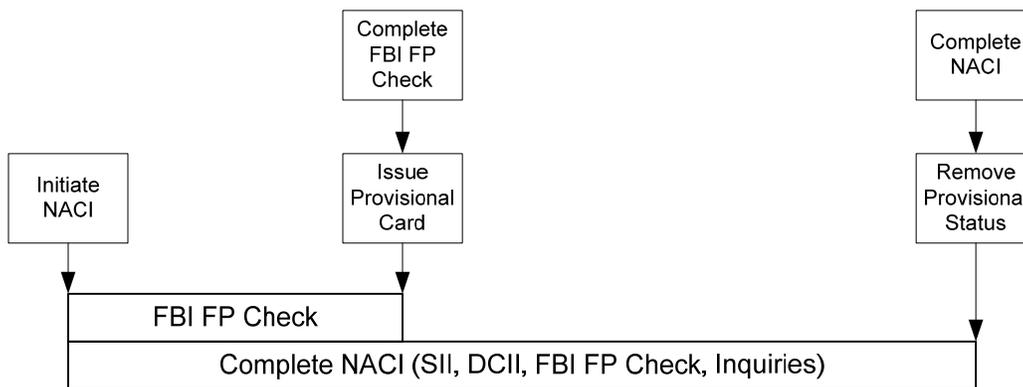
A credential may be issued after the successful completion of the FBI FP check, however, the completion and successful adjudication of a full NACI or higher level investigation as appropriate, is still required for all applicants.

DOI will revoke the credential and the employee/contractor's access if the BI process (including the adjudication of the investigative results) has not been completed within six months of credential issuance. A credential may also be revoked at any time for just cause during the investigative process or thereafter. Higher-level BIs that take greater

than 6 months to complete require an office bureau to extend the expiration date of the credential.

See [Appendix E](#), Appeal Procedures for Denial of a Credential.

Figure 1: High-Level PIV-I Process



When available through OPM’s secure website, applicants shall complete the Electronic Questionnaires for Investigations Processing (e-QIP) Standard Forms SF-85, SF-85P and SF-86. Completing the e-QIP web-based security questionnaires will lead to improved processing time of all types of investigations and dramatically reduce the overall error and rejection rates.

Refer to section 2.4 below for specific step by step instructions on completing and adjudicating a BI.

2.4 REGISTRATION, IDENTITY PROOFING, & CREDENTIAL ISSUANCE

The PIV-I process contains critical roles associated with identity proofing, registration, and credential issuance. They are: the Applicant, the Sponsor, the Registrar, and the Issuer. The roles of the Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process for one applicant. These roles may be ancillary roles assigned to personnel who have other primary duties.

The roles of Registrar and Issuer require training and certification. More information regarding training can be found in [Chapter Three](#) of this Guide.

Each PIV-I role and its corresponding responsibilities are listed below. The following roles shall be employed for the PIV-I identity proofing, registration, and issuance process.

A. Roles and Responsibilities

(1) Applicant

The Applicant is the individual to whom a PIV-I credential is to be issued. The following are Applicant responsibilities:

- Complete required forms.
- Provide two forms of legal identification, from the list of approved identity documents. ([Appendix D](#)). One must be a valid State or Federal Government issued photo ID.
- Appear in person during various stages of the process.

(2) Sponsor

The Sponsor is the individual who substantiates the need for a PIV-I credential to be issued to the Applicant, and is the federal authority that requests PIV credentials for the Applicant. Sponsors are responsible Federal officials to include supervisors, managers, Contracting Officer Representatives, Administrative Officers, Human Resources or Security Specialists, Project Chiefs, Primary Investigators or similar level positions.

The following are Sponsor responsibilities:

- Verify need for PIV credential.
- Coordinate initial registration activities.
- Serve as intermediary between Applicant and Registrar.

(3) Registrar

The Registrar is responsible for the identity proofing of the Applicant and coordinating the NACI or other BI activities. One or more individuals may perform the Registrar role. The Registrar provides the final approval for issuance of a credential to the Applicant. The following are Registrar responsibilities:

- Ensure all necessary forms are provided to the Applicant.

- Validate Applicant's identity source documents. Documents must be in original form, not copies. One of these documents must be a State or Federal Government issued photo ID, and the other must be from the set of acceptable documents listed on Form I-9 (see Appendix C), as defined in [FIPS 201](#).
- Arrange for fingerprinting and obtaining a digital picture (facial image).
- Make one copy of each identity source document.
- Ensure a BI has been successfully adjudicated in accordance with DM 441, Personnel Suitability and Security, prior to the issuance of a credential.
- Approve or Deny Issuance of a credential.

(4) Issuer

At the DOI, the role of the Issuer has three functional areas:

1. Card generation

Centralized within the National Business Center at the Department of the Interior, and includes credential personalization and operation.

2. Dissemination to a central Bureau or Office contact

Bureaus will designate a specific contact or office.

3. Issuance to the applicant.

At time of PIV Card issuance, the Issuer confirms the Applicant's identification source document which must be a State or Federal-issued photo ID in original form (not copies), as defined in [FIPS 201](#).

Issue credential (ID badge) to the Applicant, obtaining a signature from the Applicant attesting to the acceptance of the credential and related responsibilities.

(5) Other roles and responsibilities include:

Office of Personnel Management (OPM)

The OPM is responsible for conducting the NACI and other higher-level investigations as well as the initiating the FBI FP Check.

B. Registration, Identity Proofing, and Issuance Procedures

The following is a sequential list of steps for the application and issuance of a PIV credential. This procedural outline provides a detailed description of logical flow, dependencies, and responsible parties.

Note: Offices that modify the following to accommodate unique workflow requirements must ensure full compliance with FIPS-201 guidance.

(1) Sponsor – The Sponsor provides the following forms to Applicants that require a BI:

Federal Employees are required to complete the following four documents:

1. Standard Form (SF) 85 OPM Questionnaire for Non-Sensitive Positions, [or equivalent (SF-85P, SF-86)],
2. OF-306, Declaration for Federal Employment
3. SF-87, Fingerprint card
4. Fair Credit Reporting Release (if submitting an SF-85P or SF-86).

Contractor Employees are required to complete the following four documents:

1. Standard Form (SF) 85 OPM Questionnaire for Non-Sensitive Positions, [or equivalent (SF-85P, SF-86)],
2. OF-306, Declaration for Federal Employment. Complete item #'s 1, 2, 6, 8-13, 16, 17
3. FD-258, Fingerprint card
4. Fair Credit Reporting Release (if submitting an SF-85P or SF-86).

Note: The Fair Credit Reporting Release is not required when submitting forms for a NACI (SF-85).

(2) Applicant – Completes all forms provided except the Fingerprint card, which will be completed by the Applicant in the presence of the Registrar.

If available, the OPM e-QIP system may be used to complete the SF-85, SF-85P, and SF-86 online. The Registrar or appropriate Bureau/Office authority

will register the Applicant in e-QIP and provide the Applicant the website address and login information.

The Registrar completes the SF-xx (85, 85P, 86) and if using e-QIP, records the transaction number for future reference. The Registrar retains a copy of completed SF-xx until the investigation process is completed.

Note: The Office of Personnel Management serves as the official repository for investigation paperwork after the investigation is finalized.

(3) Sponsor – The Sponsor completes a Request for DOI Personal Identity Verification (PIV) Credential ([Appendix B](#)) for an Applicant, and submits the request to the Registrar. Once the Sponsor signs the form, the form should never be given to the Applicant except to fill in Applicant information in the presence of the Registrar or Delegated issuer.

(4) Registrar – The Registrar ensures the validity of the PIV request.

(5) Applicant – After completion of the forms, the Applicant must appear in person in front of the Registrar with completed forms (including one copy of SF-85, SF-85P, or SF-86 if completed online), Fair Credit Reporting Release (if submitting an SF-85P or SF-86), and two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, Employment Eligibility Verification ([Appendix C](#)), as defined in [FIPS 201](#). At least one document shall be a valid State or Federal government-issued photo identification (ID).

(6) Registrar - The Registrar shall visually inspect the identity source documents and authenticate them as being genuine and unaltered. In addition, the Registrar shall electronically verify the authenticity of the source documents, when the issuer of the source documents provides such services. When electronic verification is not offered, the Registrar shall use other available tools (i.e., Passport and Drivers License checking guides) to authenticate the source and integrity of the identity source documents. The Registrar shall copy and subsequently compare the picture on the source documents with the Applicant to confirm that the Applicant is the holder of the identity source documents. If all the above checks are deemed to be successful, the Registrar shall copy the documents; file them in the Official Personnel Folder and record the following types of data for each of the two-identity source documents presented. Then sign, and date the PIV form.

Any other information used to confirm the identity of the Applicant

Note: It is acceptable to make and retain one copy of each identity source document and keep this copy in the Official Personnel Folder. If an electronic IDMS is used, this data shall be captured and entered into the system automatically.

(7) Registrar – The Registrar shall ensure the Applicant provides fingerprints as described below:

A full set of fingerprints shall be collected from all Applicants who can provide them. The fingerprints shall be used for “one-to-many” matching with the database of fingerprints maintained by the FBI. The Registrar shall refer to [FIPS 201](#) and seek OPM guidance for alternative means for performing law enforcement checks in cases where obtaining ten fingerprints is not possible.

Retain a hardcopy of the prints or scan prints into the IDMS if available.

(8) Registrar – The Registrar shall capture a digital facial image of the Applicant per [FIPS 201](#) specifications, and retain a file copy of the image or insert the image into the IDMS, if available.

(9) Registrar – The Registrar ensures the investigation paperwork is submitted to OPM for processing. The clock starts here. A credential may be issued while an investigation is pending at OPM. The PIV credential may be issued based upon the results of the FBI FP Check. ([OMB memo M05-24](#)).

However, the PIV-I requires that the registrar must verify successful completion and adjudication of the investigation within six months of credential issuance, or the credential and PIV-I authentication certificate for the credential shall be revoked. (FIPS-201, section 5.3.1, PIV-I Card Issuance) Higher-level investigations may take longer to process and are not limited by the six-month time constraint.

(10) Registrar – If FBI FP results are successful, complete Registrar section of PIV Request form and forward request to Issuer. Send approval notification to Sponsor. If NAC results are unsuccessful, notify Sponsor and determine next course of action.

Registrar consults with Sponsor. If NAC is unsuccessful (unusable fingerprints, incorrect identity, or criminal history), determine whether to proceed with another fingerprint check or terminate the process. If a decision is made to terminate the process, the Registrar must terminate the PIV request.

If the registrar determines to issue a credential, based on the successful FBI FP or a NAC, the registrar sends the request to the issuer (NBC) for card printing.

The credential is issued to the centralized bureau/office contact who then notifies the Issuer that the credential is available.

The Issuer contacts the Registrar and the Applicant that the credential is available.

(11) Registrar – Contacts Applicant and informs the Applicant to appear in person in front of the Issuer with original identification source document to receive a credential.

(12) Applicant – Appearance

Appears in person in front of Issuer and present a State or Federal Government issued photo ID and one other identity source document from the approved list on Form I-9. ([Appendix D](#))

(13) Issuer – Printing and Issuing Credential

Confirms Applicant's identity in person (compare photo with Applicant) by verifying State or Federal Government issued photo ID with identity source document information on PIV-I Request received from Registrar.

Completes the Issuer section of PIV-I Request form and witnesses the Applicant signing the acknowledgement of receipt and use of the Credential.

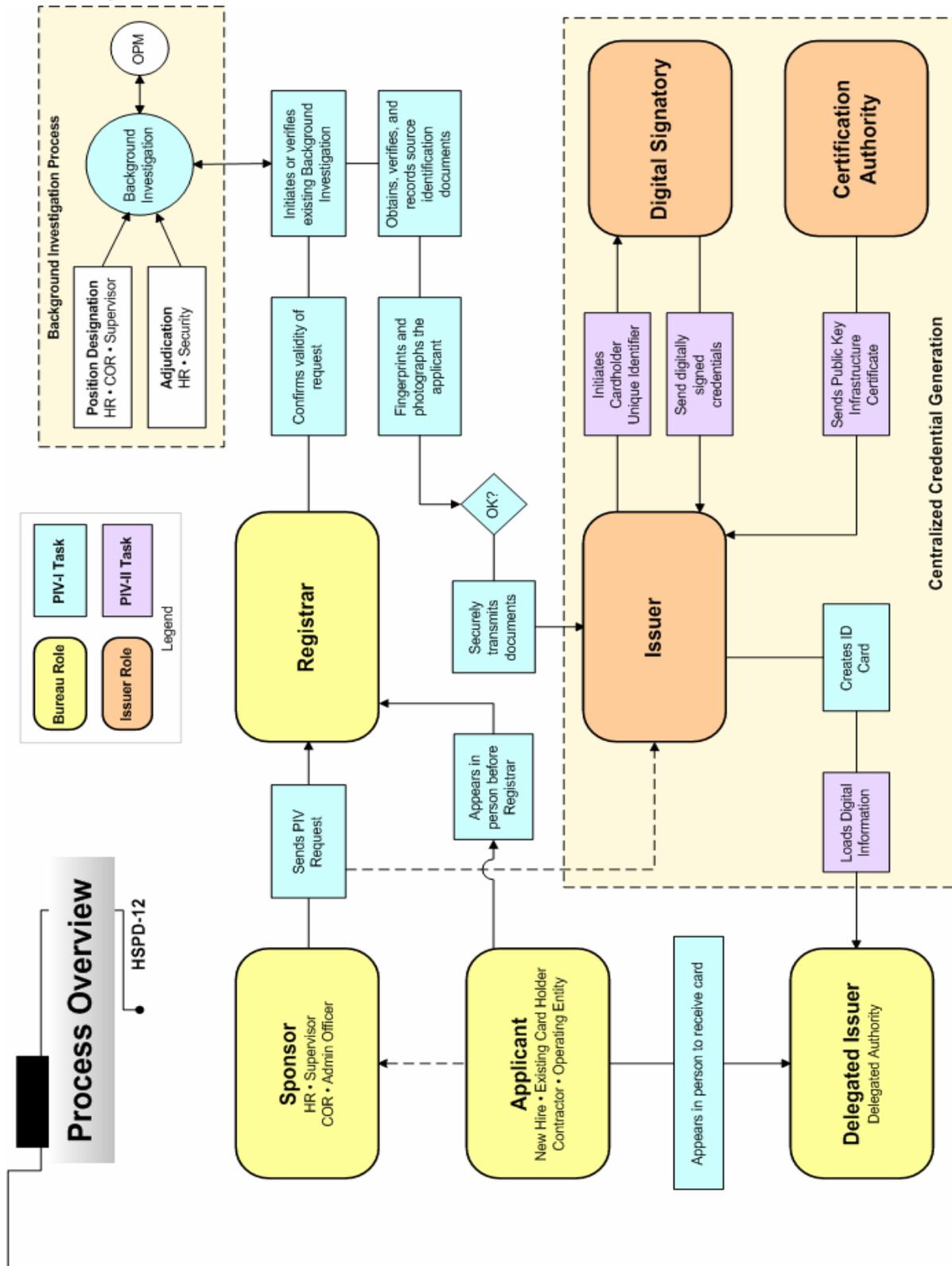
If specific Office guidelines requires, the Issuer forwards the completed PIV-I Request to Registrar, otherwise the PIV-I Issuer shall be responsible for maintaining the completed PIV form. In some cases they may also keep copies of the identity source documents.

(14) Issuer or Registrar- Filing the PIV documents.

Maintain original copy of PIV-I requests in secure centralized location, as determined by specific guidance at the Office. This may be in the Official Personnel Folder (OPF) or other secure location.

Offices must notify the Department where they are keeping the PIV documents in writing to the HSPD-12 Program manager.

Figure 2 Process Overview



2.5 EXPIRATION DATE REQUIREMENTS

All credentials issued by DOI must have an expiration date printed on the card. The expiration date for all credentials must be 5 years or less from the date of issuance.

The expiration date of Foreign Nationals cannot exceed the expiration date of their INS documents (green card, work permit, etc.).

New employees and new contractors must be issued PIV-II credentials beginning October 27, 2006. All existing employees and all existing contractors must be issued their PIV-II credentials by October 27, 2007.

2.6 REPLACEMENT CREDENTIALS

Replacement credentials are to be issued when an employee or contractor credential is lost, damaged, stolen, or expired. Offices are to:

- Ensure the IDMS record for the individual states the credential is not expired;
- Verify the individual with a 1:1 biometric match against the IDMS record;
- Verify the individual's identity against the IDMS record digital photograph;
- Recapture the Applicant's fingerprints or other biometrics;
- Issue a new credential and update the IDMS record; and
- Ensure that the Issuing Authority digitally signs the new credential record.

2.7 PROVISIONAL CREDENTIALS

At a minimum, the FBI FP Check portion of a NACI must be completed prior to issuance of any credential. Provisional credentials may be issued to new employees and contractors pending the results of the FBI Fingerprint Check. The provisional credentials will allow limited physical access to DOI facilities and limited logical access to DOI's information systems.

2.8 TEMPORARY CREDENTIALS

Temporary credentials with limited access rights may be issued to temporary employees or contractors (less than 6 months), short-term guests, and/or occasional visitors. In addition, should a long-term employee or contractor forget his/her credential on a particular day, they will be issued a temporary credential after their identity is confirmed.

Temporary credentials may be issued to new employees and contractors pending issuance of provisional credentials.

2.9 VISITOR CREDENTIALS

Follow existing procedures for issuing visitor badges to grant limited access – after verifying the visitor’s identity by checking a State Driver’s license or other photo ID.

2.10 VOLUNTEER CREDENTIALS

All volunteer’s who are affiliated with DOI for more than 180 days and who require access to federally controlled information systems and federally controlled facilities must abide by the identity proofing and registration requirements for employees as defined in the Guidance. ([Appendix G](#))

2.11 CONTRACTING IMPACTS

Contractors must abide by the identity proofing requirements defined in this Guidance. PIV-I language must be included in all applicable contracts. Please refer to DIAPR 2206-3 ([Appendix F](#)) for specific language and model contract language ([Appendix H](#)). In cases where contractors have access to mission-critical systems or sensitive data, they may be required to have a higher-level BI.

2.12 AUDIT & RECORDS MANAGEMENT

The Office of the Inspector General has responsibility for auditing identity proofing and registration records. As such, all agencies should be prepared for such reviews.

Agencies must comply with DOI “Records Disposition Management”, for the creation, maintenance, use, and disposition of all records associated with the PIV-I process.

Chapter 3 – Training

Training is available on a computer-based training disk produced by the U.S. Department of the Interior and made available to all agencies through the Smart Card Interagency Advisory Board. The training is available online at: <http://www.vodium.com/goto/blm/hspd12.asp> for a copy of the training in CD form contact the Office HSPD-12 project manager. Training modules include HSPD-12 Overview, PIV Roles and Responsibilities, Privacy, and Records Management.

3.1 WHERE TO GET ASSISTANCE

Contact the DOI's HSPD-12 Program Management Office, Office of Human Resources.

Cynthia Anderson, PMP
HSPD-12 Program Manger
(202) 219-0867
Cyndy_Anderson@ios.doi.gov

3.2 REPORTING REQUIREMENTS

DOI Offices are required to submit quarterly and annual reports on its PIV-I card programs to ensure controls are in place for tracking all PIV-I credentials. The HSPD-12 Program Manager will ensure all reporting requirements are met and provided to senior DOI managers and the DAA along with the HSPD-12 Executive Steering Committee.

APPENDICIES

Appendix A OMB Memo M-05-24

The following is an excerpt from [OMB Memorandum M-05-24](#), Implementing Guidance for HSPD-12:

“1. To whom does the Directive apply?”

As defined below, Department and Agency heads must conduct a BI, 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.

A. Departments and Agencies

- “Executive departments” and agencies listed in title 5 U.S.C. § 101, and the Department of Homeland Security; “independent establishments” as defined by title 5 U.S.C. §104(1); and the United States Postal Service (title 39 U.S.C § 201).

Does **not** apply to:

- “Government corporations” as defined by title 5 U.S.C. § 103(1) are encouraged, but not required to implement this Directive.

B. Employee

- Federal employees, as defined in title 5 U.S.C § 2105 “Employee,” within a department or agency.
- Individuals employed by, detailed to or assigned to a department or an agency.
- Within the Department of Defense (DoD) and the Department of State (DoS), members of the Armed Forces, Foreign Service, and DoD and DoS civilian employees (including both appropriated fund and non-appropriated fund employees).
- Applicability to other agency specific categories of individuals (e.g., short-term (i.e. less than 6 months) guest researchers; volunteers; or intermittent, temporary or seasonal employees) is an agency risk-based decision.

Does **not** apply to:

- Within DoD and DoS, family members and other eligible beneficiaries.
- Occasional visitors to Federal facilities to whom you would issue temporary identification.

C. Contractor

- Individual under contract to a department or agency, requiring routine access to federally controlled facilities and/or federally controlled information systems to whom you would issue Federal agency identity credentials, consistent with your existing security policies.

Does not apply to:

- Individuals under contract to a department or agency, requiring only intermittent access to federally controlled facilities.

D. Federally Controlled Facilities

- Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of a department or agency covered by this Directive.
- Federally controlled commercial space shared with non-government tenants. For example, if a department or agency leased the 10th floor of a commercial building, the Directive applies to the 10th floor only.
- Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.
- Facilities under a management and operating contract. Such as for the operation, maintenance, or support of a Government-owned or-controlled research, development, special production, or testing establishment.

E. Federally Controlled Information Systems

- Information technology system (or information system), as defined by the Federal Information Security Management Act of 2002 (44 U.S.C. § 3502(8)).
- Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency (44 U.S.C. § 3544(a)(1)(A)).
- Applicability for access to Federal systems from a non-Federally controlled facility (e.g. a researcher up-loading data through a secure website or a contractor accessing a government system from their own facility) should be based on the risk determination required by existing National Institute of Standards and Technology (NIST) guidance.

Does not apply to:

- Identification associated with national security systems as defined by the Federal Information Security Management Act of 2002 (44 U.S.C. § 3542(2)(A)).

¹ Federal Information Processing Standard (FIPS 199): Standards for Security Categorization for Federal Information and Information Systems, 2/04,

<http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

² See NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System, 8/03, <http://www.csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf>.

APPENDIX B PIV-I Credential Request Form

PIV-I Form can be found on the following two pages.

Request for DOI Personal Identity Verification (PIV) Credential

Pursuant to Section 3(e)(3) of the Privacy Act of 1974 (Public law 93-573), the individual furnishing information on this form is hereby advised as follows: 1. The authority for solicitation of the information is 5 U.S.C. 301, Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995, and Homeland Security Presidential Directive – 12, August 27, 2004. 2. The principle purposes for which the information is intended to be used are: (a) To ensure the safety and security of DOI facilities and their occupants in which the system is installed; (b) To verify that all persons entering DOI facilities or other Government facilities with smart card systems are authorized to enter them; and (c) To track and control ID security cards issued to persons entering and exiting the facilities. 3. The routine disclosures of the information are: (a) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs, on DOI's behalf, services requiring access to these records; (b) To the Federal Protective Service and appropriate Federal, State, local or foreign agencies responsible for investigating emergency response situations or investigating or prosecuting the violation of or for enforcing or implementing a statute, rule, regulation, order or license, when DOI becomes aware of a violation or potential violation of a statute, rule, regulation, order or license; (c) To another agency with a similar smart card system when a person with a smart card desires access to that agency's facilities; and (d) To those identified in the Department of the Interior system of records notice: Interior, Computerized ID Security System, OS-1. A copy is available on the Department of the Interior Privacy Program website at www.doi.gov/ocio/privacy. 4. The effect on the individual of not providing all or any part of the requested information may result in disapproval of the issuance of the PIV ID credential.

A. Sponsor/COR - PIV Request

1. Replacement Card? No Yes: 1a. Reason for Replacement _____
2. Legal Name (L,F M): _____ Phone No: _____
3. Affiliation: Employee Temporary Employee Contractor Volunteer
4. U.S. Citizen? Yes No: 4a. Country of Citizenship _____
 4b. Work Permit Number: _____ Expiration Date: _____
5. Employee Title: U.S. Government LE Firefighter Security Investigator
6. Federal Emergency Response Official? (Must be approved by Bureau/Office Law Enforcement Director)
7. Bureau: _____ Office: _____
8. Work Address: _____
9. City: _____ State: _____ Zip: _____
10. Contractor Company: _____ Contract Number: _____

Sponsor Information

11. Name: _____ Phone Number: _____
12. Organization: _____ Title: _____
13. Email: _____

I agree to sponsor the above application for a PIV credential and certify that the information is accurate to the best of my knowledge.

14. Sponsor/COR Signature: _____ Date (mm/dd/yyyy): ____/____/____

B. Registrar - Source Document Confirmation, Applicant's Picture, and Fingerprints (Only for New Cards after Section A is completed)

Applicant Information

15. Birth date (mm/dd/yyyy): ____/____/____ Social Security Number: ____-____-____
16. Hair Color _____ Eye Color _____ Height _____ Weight _____ Gender _____
17. Home Address: _____
18. City: _____ State: _____ Zip: _____
19. Email: _____

I certify that the information is accurate to the best of my knowledge.

20. Applicant Signature: _____ Date (mm/dd/yyyy): ____/____/____

Identity Source Document 1 (Attach copy)

21. Name: _____
22. Document #: _____ Document Title: _____
23. Issuer: _____
24. Document Expiration Date (mm/dd/yyyy): ____/____/____

25. Name: _____
26. Document #: _____ Document Title: _____
27. Issuer: _____
28. Document Expiration Date (mm/dd/yyyy): ____/____/____

Applicant's Picture

29. Picture taken? Yes
30. Fingerprints taken or received? Yes (Employees use SF-87/ Contractors use FD-258)
31. Background Investigation Forms Complete? Yes (required for new cards only)

Field Registrar Certification: I hereby confirm that the information contained in the above documents was checked and verified.

32. Name: _____ Phone No.: _____
33. Organization: _____ Title: _____
34. Field Registrar Signature: _____ Date (mm/dd/yyyy): ____/____/____

Human Resources /Security Management Office

NAC Adjudication Results

35. Fingerprint check NAC NACI Date Completed (mm/dd/yyyy): ____/____/____
36. Successful? Yes No
37. Comments: _____

I certify that the information regarding the above applicant is accurate to the best of my knowledge and approve this applicant for credential issuance.

38. Human Resources/Security Management Office Signature: _____
Date (mm/dd/yyyy): ____/____/____

Registrar Information

39. Name: _____ Phone No.: _____
40. Organization: _____ Title: _____
41. Email: _____

I hereby confirm that the information contained in the above documents were checked and verified and the FBI fingerprint results have been successfully adjudicated.

42. Registrar Signature: _____ Date (mm/dd/yyyy): ____/____/____

C. Issuer (To be completed by Issuer, after Sections A and B are completed)

43. Name on Credential: _____
44. Credential Identifier: _____
45. Credential Expiration Date (mm/dd/yyyy): ____/____/____

Issuer Information

46. Name: _____ Phone No: _____
47. Organization: _____ Title: _____
48. Email: _____

I hereby acknowledge issuance of a credential to the applicant identified above based on verification of the applicant's identity and verification of the above Registrar's issuance approval.

49. Issuer Signature: _____ Date (mm/dd/yyyy): ____/____/____

D. Applicant Acknowledgement (To be completed by Applicant, after Section C is completed)

I, the Applicant, confirm receipt of the PIV credential identified above and that the information is accurate to the best of my knowledge, and agree to abide by all rules and responsibilities associated with this credential.

50. Applicant Signature: _____ Date (mm/dd/yyyy): ____/____/____

APPENDIX B -1 Instructions for PIV I Form

All information must be legibly printed in blue or black ink.

All strikethroughs must be initialed.

Forms with whiteout will not be accepted.

All signatures must be original signatures, no copies or stamped signatures.

Sponsors / Registrars / Issuers should maintain a log of all applicant forms they sign (Name, badge type, and date). When the information is entered into the electronic PIV system you maybe asked to digitally sign the forms of applicants that you have processed through the manual (paper-based) process.

Once the Sponsor signs the form, the form should never be given to the applicant except to fill in applicant information in the presence of the Registrar or Issuer.

Sponsor

Complete lines 1 – 10 about the applicant, lines 11 – 13 about yourself, and sign and date line 14. Send the form to your designated Registrar's office.

Line 2 Legal Name of Applicant: - Last, First Middle names – as they appear on official documents (identity proofing source documents)

Line 3 Affiliations:

Employee – Permanent (career/ career conditional) DOI employee

Temporary Employee – Temporary, Term, Student (SCEP, STEP), or intern paid or obtaining some type of benefit directly from DOI

Contractor – an individual working, under contract, for DOI

Volunteer – a non-paid individual working under the supervision of DOI

Line 4 Citizenship: If applicant is not a U.S. citizen please note the country of citizenship (4b), work permit number (or other INS documentation indicating eligibility to work) and expiration date (4c), and verify that the applicant has been a resident of the United States for at least the last 3 years. If the applicant has not been a resident of the U.S. for at least 3 years, they may not qualify for a PIV card due to restrictions associated with the BI. Please contact your Bureau Personnel Security Specialist for further information. Also note; the expiration of their

ID cannot extend past the expiration date of their INS documents (i.e., work permit, visa, etc.).

Line 5 Employee Title – Only for permanent employees of DOI

United States Government – used for employees without a specific title listed below and temporary employees, contractors, retirees, and volunteers. This is the default title for the area above the photo on the PIV cards.

LE (Law Enforcement) – DOI employees who are sworn Law Enforcement Officers

Firefighter – Individuals who are employed by DOI in a firefighter capacity.

Security – DOI employee in 080 job series

Investigator – DOI employee in 1801 and 1810 job series

Line 6 Federal Emergency Response Official - Must be approved by Bureau/Office Law Enforcement Director

Line 7 Bureau: - bureau name that will appear on the applicant’s card

- | | |
|---------------------------------|-----------------------------------|
| Bureau of Land Management | Bureau of Indian Affairs |
| Bureau of Reclamation | Minerals Management Service |
| National Business Center | National Indian Gaming Commission |
| National Park Service | U.S. Fish and Wildlife Service |
| United States Geological Survey | Office of Surface Mining |
| Office of the Inspector General | Office of the Secretary |
| Office of the Solicitor | |

Lines 8 & 9 – Work address: – Duty station location

Line 10 Contractor Company / Contract Number – for contractors only

Registrar

Field Registrar: When applicant arrives in your office, have the applicant complete lines 15 – 19 and sign and date line 20. Verify identity source documents (see attached list of acceptable documents), record the document information, and attach a copy of the documents to the request form.

If the applicant is not a U.S. citizen, verify that “No” has been checked on Line 4 and ensure that the applicant has been a resident of the U.S. for at least the past 3 years. If the applicant’s INS documentation expires in less than 5 years from the application date, circle the expiration date of the document in red. The PIV card cannot be issued with an expiration date that is later than the date the applicant is legally allowed to reside and work in the U.S.

Complete lines 32 & 33 and sign & date line 34. Forward this document to the Human Resources / Security Management Office to have background check completed and/or verified.

Line 15 Birth Date and Social Security Number: SSN is needed by the Personnel Security Specialist to verify BI information with OPM.

Line 16 Applicant Physical Characteristics:

Hair color: Auburn, Bald, Black, Blond, Brown, Gray, Red, White,

Eye Color: Black, Blue, Brown, Green, Gray, Hazel

Height – Feet and Inches

Weight - in pounds

Lines 21- 28 Identity Source Documents: - List of acceptable documents is on the last page of these instructions. Copies of both identity source documents must be attached to the PIV request form.

One of the documents must be a State or Federal issued photo ID

Lines 21 & 25 - Name of the applicant as it appears on the document

Lines 23 & 27 – Name of department or agency that issued the document

Line 29 Picture taken: – photo must be sent to Issuer (Polaroid for DI-238A/ DI-238 and digital for others). Registrar must also digitally store picture for later use in smartcard issuance.

Line 30 Fingerprints taken or received: Fingerprints can either be done digitally or on the paper cards. Ensure the correct fingerprint card was used; Employees and Temporary Employees use SF-87 and Contractors and Volunteers use FD-258.

Line 31 Background Investigation Application Forms Complete: Background Investigation (BI) forms are required for applicants for whom an appropriate BI cannot be verified. If the applicant is a current DOI employee or affiliate, verify that at least a NACI has been completed and is on file. If there is not any record of a NACI for the applicant, they must complete the BI forms. BI forms include SF-85, SF-85P with Credit Report Release, or SF-86 and OF-306. The minimum investigation for the issuance of a PIV credential is a National Agency Check with Inquiries (NACI) and the NAC portion must be completed prior to the issuance of the card. For a NACI an employee needs to complete the SF-85 and a contractor or other affiliate must complete an SF-85P. To receive an advanced NAC (Fingerprint check

results) you must make sure that code #3 is placed in block B “Extra Coverage” of the SF-85, SF-85P, or SF-86. Place an “R” in the code block in the area marked for ‘OPM use only’ to receive the fingerprint check results as soon as they are completed (prior to the NAC).

Human Resources / Security Management Office: After the BI has been successfully completed; fill in lines 35 - 37 and sign & date line 38. The form should then be forwarded to the Registrar for final approval.

Lines 35 – 37 NAC Adjudication Results: Any applicant receiving a PIV card must have at least a NACI done. The PIV card may be issued after the NAC portion of the NACI is completed. Adjudication of the NAC, which includes the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII) and the FBI FP, must be complete before the PIV card can be issued. If the results are not received within 5 days, the PIV credential may be issued based upon the results of the FBI FP (OMB memo M05-24).

Note on the form which portion of the NACI was completed (fingerprint, NAC, NACI). If the applicant has a higher-level BI on record with OPM, mark that the NACI (minimum requirement) was completed and note the type of investigation on the comments line.

Registrar: Review the PIV form for completeness and accuracy, ensure that copies of the identity source documents are attached to the form, fill in lines 39 – 41, and sign & date line 42. Forward the PIV form and copies of the identity documents to the designated issuer and notify the applicant to report to the designated issuer. If necessary, ensure that the applicant’s photo has been sent to the designated Issuer.

Issuer

The issuer is responsible for issuing the PIV credential, only after Sections A and B are complete and signed. The Issuer must verify the identity of the applicant by comparing the ID to the attached source documents and the source document presented by the applicant at the time of issuance. The Issuer then completes lines 40 – 48 and signs & dates line 49. The Issuer must then have the applicant sign for the receipt of the PIV credential on line 50.

Lines 43 – 45 PIV credential information: - Fill in the name on the credential, the credential serial number, and the expiration date printed on the credential. Verify that the expiration date is not greater than 5 years from the issuance date and that the expiration date does not exceed the expiration date of the INS documents for non-U.S. citizens.

Appendix C PIV Card Usage Privacy Act Notice

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. If you have a Government badge, the PIV Card will replace your badge.

What is the Authority for the PIV Card Program? *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. PIV cards are issued 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 BI 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 BI, 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 BI 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 authentication key, and two electronic fingerprints.

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. Use of the card is limited to that identified by the Government guidelines and to that identified in the Privacy Act system of records notices that cover

each system for the PIV Card process.

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.

What Happens if I Don't Want a Card? Currently there is no legal requirement to use a PIV Card. However, if you do not give us the 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 your organization's HSPD-12 Coordinator or Privacy Act official.

APPENDIX D I-9 Documents Acceptable for Identity Proofing

Per FIPS 201, the Applicant must appear in person before the Registrar with two original form identity source documents. One of these must be a Federal or State issued photo ID, and the other must be from the approved list of identity proofing documents listed in table shown below.

List A	List B	List C
U. S. Passport (unexpired or expired)	Driver’s license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	U.S. social security card issued by the Social Security Administration (other than a card stating it is not valid for employment)
Certificate of U.S. Citizenship (Form N-560 or N-561)	ID card issued by Federal, State or local government agencies of entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address	Certification of Birth abroad issued by the Department of State (form FS-545 or Form DS-1350)
Certificate of Naturalization (Form N-550 or N-570)	School ID card with a photograph	Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal.
Unexpired foreign passport, with I-551 stamp or attached Form I-94 indicating unexpired employment authorization	Voter’s registration card	Native American tribal document

Permanent Resident Card or Alien Registration Receipt Card with photograph (Form I-151 or I-551)	U.S. Military card or draft record	U.S. Citizen ID Card (Form I-197)
Unexpired Temporary Resident Card (Form I-688)	Military dependent's ID card	ID Card for use of Resident Citizen in the United States (Form I-179)
Unexpired Employment Authorization Card (Form I-688A)	U.S. Coast Guard Merchant Mariner Card	Unexpired employment authorization document issued by DHS (other than those listed under List A)
Unexpired Reentry Permit (Form I-327)	Driver's license issued by a Canadian government authority	
Unexpired Refugee Travel Document (form I-571)	For persons under age 18 who are unable to present a document listed above:	
	School record or report card	
	Clinic, doctor or hospital record	
	Day-care or nursery school record	

APPENDIX E Appeal Rights for the Denial of a Credential

The following procedure is to be followed:

(1) Appeal Rights for Federal Service Applicants

When the PIV-I Adjudicator determines that a PIV-I Applicant has not provided his or her true identity during the registration process or is otherwise found unsuitable, and the determination results in a decision by the agency to withdraw an employment offer, or remove the employee from the federal service, the procedures and appeals rights of either 5 CFR Part 731, Subparts D and E (Suitability), 5 CFR Part 315, Subpart H (Probationary Employees), or 5 CFR Part 752, Subparts D through F (Adverse Actions) will be followed, depending on the employment status of the federal service applicant, appointee, or employee. Employees who are removed from federal service are entitled to dispute this action using applicable grievance, appeal, or complaint procedures available under Federal regulations, Departmental directives, or collective bargaining agreement (if the employee is covered).

(2) Appeal Rights for Contract Applicants and Agency Affiliates

Notice of Proposed Action - When the PIV-I Adjudicator determines that a PIV-I Applicant has not provided his or her true identity or is otherwise not suitable to be employed in the current or applied for position, e.g. an unsuccessful adjudication, the PIV-I Adjudicator shall provide the individual reasonable notice of the determination including the reason (s) the individual has been determined to not have provided his or her true identity or is otherwise unsuitable. The notice shall state the specific reasons for the determination, and that the individual has the right to answer the notice in writing. The notice shall inform the individual of the time limits for response, as well as the address to which such response should be made.

Answer - The individual may respond to the determination in writing and furnish documentation that addresses the validity, truthfulness, and/or completeness of the specific reasons for the determination in support of the response.

Decision - After consideration of the determination and any documentation submitted by the PIV-I Applicant for reconsideration of the initial determination, the Agency Head/Staff Office Director or his/her designee will issue a written decision, which informs the PIV-I

Applicant/Respondent of the reasons for the decision. The reconsideration decision will be final.

Appendix F Acquisition Policy Release 2006-3, October 18, 2005 (DIAPR)

SUBJECT: Implementation of Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors

1. **Purpose:** This policy release establishes procedures for standard implementation of HSPD-12 in DOI contracts.
2. **Effective Date:** Upon signature.
3. **Expiration Date:** Upon revision of the FAR or DIAR.

4. **Backgrounds and Explanation:**

HSPD-12, issued on August 12, 2004, directs the creation of a new Federal standard for secure and reliable identification issued by Federal agencies to their employees and contractors, including all tiers of subcontractors. Implementation will be in several stages, with the initial phase being put in place on October 27, 2005. This first phase consists of implementation of procedures under which Personal Identity Verification (PIV) credentials such as security badges, building passes, and so forth, will only be issued after the individual's identity has been independently verified. Later phases will expand coverage to personnel who have already been issued credentials as of October 27, and use of Smart Cards.

Not every contractor and subcontractor (hereafter, "contractor") employee will need PIV credentials. There are two categories of contractor personnel who will be subject to the BIs:

- Those who need routine and regular unsupervised access to a Federally controlled facility for more than 180 days;
- Those who need any unsupervised access to a Level 3 or 4 Federally controlled information system.

Physical Access. A "Federally controlled facility" is federally owned or leased space, whether for single or multi-tenant occupancy, all or any portion of which is under the jurisdiction, custody or control of DOI. If a building is shared with non-government tenants, only access to the Federal area is controlled. The requirements for contractor credentialing apply even if there is no guard, card reader, or other physical control at the entrance to the office. The 180-

calendar day period begins on the first day of the individual's affiliation with DOI (in this case, the date that contract performance begins rather than contract award) and ends exactly 180 days later, regardless of the number of times the contractor actually accessed a building or IT system.

Logical Access. An "information technology system" is defined in the Federal Information Security Management Act of 2002 (44 U.S.C. §3503(8)). Use of an information system by a contractor on behalf of an agency is defined in 44 U.S.C. §3544(a)(1)(A). If a contractor needs *any* amount of unsupervised access to a DOI IT system, HSPD-12 compliant credentials must be issued regardless of the duration of access. The credentialing requirement applies whether the contractor accesses the IT system from the premises of a DOI facility, from their own facility, through the Internet, or by any other means.

Uncredentialed Contractors. Contractors who do not fit into one of the above two categories will be treated as visitors. This group includes temporary and seasonal workers, and those needing intermittent physical access such as delivery services. These persons must access the facility via a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times. Normally, persons working exclusively outside on the grounds of federally controlled facilities, such as grounds maintenance workers, parking attendants, and some construction workers, need not receive PIV credentials.

Special Cases. The preceding paragraphs describe the minimum requirements. Depending on risk, increased application of HSPD-12 will be appropriate in some cases. Workers at construction sites may or may not need PIV credentials depending on the nature of what is being built. For example, it may be appropriate to credential workers on a critically sensitive dam. Similarly, even grounds workers at a sensitive site, such as the White House, should be credentialed. If higher-level security, such as Secret or Top Secret, is needed, other clearances can be added to the HSPD-12 requirements.

Verification Process. To the extent possible, HSPD-12 clearance of contractor personnel will be handled through the same procedures as for employees. The process has two steps: a National Agency Check (NAC) and a NAC with Written Inquiries (NACI). After the individual applies for a PIV credential, a NAC will be processed. If the NAC does not reveal any unfavorable information, a PIV credential will be issued; this should take about one week. Simultaneously, a NACI will also be initiated, with adjudication taking about six months. If the adjudication is favorable, nothing more needs to be done. If the adjudication is

unfavorable, the credentials will be revoked.

Should a contractor's PIV credentials be declined or revoked, the contract administration team must take some action to accommodate this in the contract. For example, the contract may have to be terminated if there is no alternative to on-site performance by the individual in question. On the other hand, it may be possible to arrange off-site performance or some other accommodation. In any case, the contracting officer must work together with the sponsor, security personnel, and the contractor to address this situation promptly.

All PIV credentials will automatically have a five-year expiration, except for foreign nationals. Foreign nationals' cards may be issued for five years, unless that date would extend past the expiration date of their work permit or visa. Government wide, the HSPD-12 clearance process for foreign nationals has not been finalized yet. Please be aware that there may be extra delay in obtaining verification for these individuals, especially during the early months of implementation.

If contractor personnel have already been investigated by another agency through OPM, the results of a prior HSPD-12 (or higher) clearance will be accepted by DOI upon receipt of appropriate verification.

Contracting Procedures. Early coordination with requisitioners is recommended in order to avoid delays in contract start-up. Contractors who already have badges may continue to use them until they naturally expire. However, there will be (at least) a week delay for individuals who start unsupervised physical or logical access for the first time on or after October 27.

For now, the Government must pay for the BI. A source of funding has not been clearly defined, but it appears likely that the sponsoring program will bear the cost. Some program offices may not be aware of this yet. They should be referred to the Bureau's budget office for further guidance. We recommend that solicitations and contracts address limiting the number of contractor employees who will be investigated.

Contracting Officer's Representatives (CORs) will have additional duties, which should be reflected in the COR appointment letter. CORs will act as sponsors for contractor personnel. In this capacity, they will be responsible for ascertaining the risk level for the position, including credentialing requirements in Statements of Work, validating individuals' need for a PIV credential, facilitating the credentialing process, and ensuring that credentials are renewed

and rescinded in a timely manner. It is the COR's responsibility to make sure that contractors' credentials are returned to the Government at the end of the contract or whenever a contractor employee's affiliation with DOI ends.

Model Section C language is attached. The language may be modified to suit circumstances, except that the flow down requirement must be included. It should be used in all contracts where the requisitioner needs contractor personnel to have routine and regular unsupervised access to a Federally controlled facility for more than 180 days or unsupervised access to a Federally controlled Level 3 or 4 information system. It should rarely be applicable to contracts for supplies. When contracting on behalf of other agencies, language from the requisitioning agency that serves the same purpose may be used.

In addition to new contracts, HSPD-12 requirements must be added to some contracts awarded prior to this DIAPR's issuance. Current contracts that require contractor personnel to have physical and/or logical access as described above must be modified to include the PIV requirements when an option is exercised, or before expiration when the contract term (i.e., the need for contractor access) extends past the expiration date of their current credentials. Contracts that do not currently require contractor personnel to have physical and/or logical access as described above must be modified to include the HSPD-12 requirements if circumstances change such that contractor physical or logical access is newly required.

5. Action Required:

Distribute this DIAPR as widely as possible, including to requisitioners. Coordinate with program offices and other requisitioners to ensure that the new procedures are followed and that contract work is not delayed. Starting immediately, insert language substantially similar to the attached model language in solicitations that require contractor personnel to have physical or logical access as described above. At the earliest opportunity, but no later than exercise of an option, modify applicable contracts to include language substantially similar to the model language. ([Appendix H](#))

6. Additional Information: If you have questions about this matter, please contact Dee Emmerich at (202) 208 3348 or delia_emmerich@os.doi.gov.

//ss//

Debra E. Sonderman

Director, Office of Acquisition and Property Management

Appendix G Definition of Card Issuance and Facility Guidance

July 14, 2005

Memorandum

To: Bureau Security Directors

From: Glenn F. Smith
Assistant Director, Office of Law Enforcement and Security

Subject: Definition of Card Issuance and Facility Guidance Regarding HSPD-12

Reference is made to HSPD-12 (Policy for a Common Identification Standard for Federal Employees and Contractors), FIPS 201 (Federal Information Processing Standards Publication) dated February 25, 2005, OCIO Directive 2004-08, specifically the procurement of physical access (card reader) systems, 444 DM - Physical Protection and Building Security, OLES Guidance 5/25/05-Requirements for the DOI Personal Identity Verification Card (Smart Card) Visual Card Topography and OLES Guidance 5/25/05-Installation of Smart Card Readers at DOI Facilities.

1) Individuals who will receive HSPD-12 compliant identification cards are (except as noted under item #2):

- a) Federal employees, as defined in title 5 U.S.C §2105 "Employee," within a department or agency.
- b) DOI specific categories of individuals (e.g., contractors, guest researchers, tribal users, volunteers or intermittent, temporary or seasonal employees, etc.) who are affiliated with DOI for more than 180 days and who require access to Federally controlled information systems and Federally controlled facilities as defined in sections 3 and 4.
- c) Individuals affiliated with DOI who are granted access to Federally controlled information systems but are not supervised by an individual with an active HSPD-12 identification card, regardless of the duration of access.
- d) HSPD-12 compliant BIs (National Agency Check with Inquiries) or equivalent (pending further guidance from OMB) must be conducted on non-US citizens affiliated with DOI.

2) Supervised physical and logical access will be granted to certain individuals without

the use of HSPD-12 compliant identification under the following conditions:

- a) These individuals are described as Federal employees, contractors, visitors, cooperatives, partners, guest researchers, volunteers, interns, and intermittent, temporary or seasonal employees, etc. who are affiliated with the DOI less than 180 days.
- b) The 180-day period begins the first day the individual is affiliated with DOI and ends exactly 180 days later, no matter the frequency or duration of the activity (one or five days a week).
- c) All of these individuals must be controlled when entering facilities using or operating federally controlled information systems. At a minimum, individuals must access the facility via a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times.
- d) Contracts and agreements requiring access to Federally controlled information systems must require supervision (by an individual with an active HSPD-12 identification card) or HSPD-12 compliant identification for all individuals working in support of the contract/agreement, even those working less than 180 days.
- e) Vendors, delivery services, recurring services contracts, or other individuals (e.g. volunteers) who do not access Federally controlled information systems but require sporadic physical access in excess of 180 days must access the facility via a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times.
- f) If at any time a risk-based analysis determines HSPD-12 compliant identification is warranted for a particular individual or facility, all exceptions listed in this section (#2) will be immediately rescinded.
- g) Waiver of HSPD-12 compliant identification does not modify Federal investigative requirements, application of statutory standards of character, or implementation of national security systems requirements, e.g., 44 U.S.C. § 3542(2)(A), 18 U.S.C. § 921, 5 CFR Part 731, 5 CFR Part 732, 441 DM 5, 446 DM 2.

3) Federally Controlled Information Systems

- a) Information technology system (or information system), as defined by the Federal Information Security Management Act of 2002, (44 U.S.C. §3502(8)).
- b) Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, (44 U.S.C. §3544(a)(1)(A)).
- c) Applicability for employee or contractor access of Federal systems from a non-

Federally controlled facility (e.g. researchers' up-loading data through a secure website or a contractor accessing a government system from their own facility) should be based on risk. Minimum acceptable requirements (risk) for individuals accessing Departmental information systems are defined in Sections 1 & 2 of this document).

- d) This Directive Does not alter requirements for national security systems as defined by the Federal Information Security Management Act of 2002, (44 U.S.C. §3542(2)(A)).

4) Federally Controlled Facilities:

- a) Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of the Department, its Bureaus or Offices.
- b) Federally controlled commercial space shared with non-government tenants. For example, if DOI leased the 10th floor of a commercial building, the Directive applies to the 10th floor only.
- c) DOI-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.
- d) Educational institutions that meet the definition of federally controlled facility and/ or enjoy privileged access to Federally controlled information systems. Unless specifically designated by DOI, this Directive does not apply to Educational institutions that conduct activities on behalf of DOI, its Bureaus or Offices, or at which Federal employees are hosted.

Questions regarding this guidance should be forwarded to Glenn F. Smith at 202/208-5836.

Appendix H Model Statement of Work/Performance Work Statement Language

Contractor Personnel Security and Suitability Requirements

Performance of this contract requires contractor personnel to have a Federal government-issued personal identification card before being allowed unsupervised access to a DOI [facility and/or information system]. The Contracting Officer's Representative (COR) will be the sponsoring official, and will make the arrangements for personal identify verification and card issuance.

At least two weeks before start of contract performance, the Contractor will identify all contractor and subcontractor personnel who will require [physical and/or logical] access for performance of work under this contract. The Contractor must make their personnel available at the place and time specified by the COR in order to initiate screening and BIs. The following forms, or their equivalent, will be used to initiate the credentialing process:

- OPM Standard Form 85 or 85P
- OF 306
- Fingerprint card (local procedures may require the fingerprinting to done at a police station; in this case, any charges are to be borne by the contractor)
- Release to Obtain Credit Information
- PIV card application (web-based)

Contractor employees are required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed to reach a suitability determination. Refusal or failure to furnish or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the contractor personnel being screened or investigated in person, by telephone or in writing, and the Contractor agrees to make them available for such contact.

Alternatively, if an individual has already been credentialed by another agency through OPM, and that credential has not yet expired, further investigation may not be necessary. Provide the COR with documentation that supports the individual's status.

During performance of the contract, the Contractor will keep the COR apprised of changes in personnel to ensure that performance is not delayed by compliance with credentialing processes. Cards that have been lost, damaged, or stolen must be reported to the COR and

Issuing Office within 24 hours. Replacement will be at the contractor's expense. If reissuance of expired credentials is needed, it will be coordinated through the COR.

At the end of contract performance, or when a contractor employee is no longer working under this contract, the Contractor will ensure that all identification cards are returned to the COR.

Before starting work under this contract, a National Agency Check (NAC) will be conducted to verify the identity of the individual applying for clearance. Upon successful completion of the NAC process, an identification card will be issued and access granted.

Simultaneously, a NAC with Inquiries (NACI) will be initiated to determine the individual's suitability for the position. If the NACI adjudication is favorable, nothing more needs to be done. If the adjudication is unfavorable, the credentials will be revoked. In the event of a disagreement between the Contractor and the Government concerning the suitability of an individual to perform work under this contract, DOI shall have the right of final determination.

This requirement must be incorporated into any subcontracts that require subcontractor personnel to have regular and routine unsupervised access to a Federally controlled facility for more than 180 calendar days or any unsupervised access to a Federally controlled Level 3 or 4 information system.

Appendix I PIV Information Notice

PIV INFORMATION NOTICE!

- 1. ACCESS TO THESE RECORDS IS LIMITED TO AUTHORIZED PERSONS ONLY!**
- 2. INFORMATION MAY NOT BE DISCLOSED FROM THIS FILE UNLESS PERMITTED PURSUANT TO DEPARTMENT OF THE INTERIOR PRIVACY ACT REGULATIONS AT 43 CFR 2.56.**
- 3. THESE RECORDS MAY NOT BE ALTERED OR DESTROYED EXCEPT AS AUTHORIZED BY 43 CFR 2.52.**
- 4. THE PRIVACY ACT CONTAINS PROVISIONS FOR CRIMINAL PENALTIES FOR KNOWINGLY AND WILLFULLY DISCLOSING INFORMATION FROM THIS FILE UNLESS PROPERLY AUTHORIZED.**
- 5. DEPARTMENT OF THE INTERIOR DISCIPLINARY AND ADVERSE ACTIONS MANUAL SECTION 370 DM 752 IDENTIFY PENALTIES FOR SEVERAL OFFENSES FOR MISUSE AND FAILURE TO SAFEGUARD GOVERNMENT RECORDS.**
- 6. APPEAL RIGHTS FOR APPLICANTS DENIED A PIV CARD ARE IDENTIFIED IN DOI MANUAL SECTION 441 DM 2.**

Appendix J Checklist for Review of a Privacy Act System or Records Maintenance Practices

This review checklist will help to ensure that the office managing a system of records is maintaining it according to the Privacy Act requirements.

The attached checklist is based on:

- Privacy Act guidance found in the Department of the Interior (DOI) Privacy Act Manual Section (383 DM Chapters 1 – 13)
- DOI Privacy Act regulations at 43 CFR 2.45 – 2.79
- OMB Circular A-130, Appendix I
- National Institute of Standards and Technology (NIST) Special Publication 800-26

The Bureau/Office Privacy Act Officer, local Privacy Act Coordinator, and IT should maintain copies of the review Security Manager if the system reviewed is an electronic system.

Requirement and Guidance Cite	Compliant (Yes/No)
I. Physical Security of the Area	
a. Is a Privacy Act Warning Notice” posted in records system areas that are not automated? 383 DM 8.3 and Illustration I 43 CFR 2.51(b)	
b. If this is an automated system, is a Privacy Act Warning Notice or equivalent made available to those who have access to the Privacy Act system of records (e.g., JAVA scripted pop-up notice)?	
c. If this is an automated system, is there documentation that ensures that 383 DM 8.4 and 43 CFR . List the documentation in the “Discussion” section. 43 CFR 2.51(c).	
d. If this is a computerized system, does the IT Security Plan appropriately identify that this is a Privacy Act system of records?	
e. Are these records that are covered by an Office of Personnel Management (OPM) Government-wide or Central Privacy Act system of records notice? (e.g., employee clearance files). If yes, write “system notice” name in the “discussion” section.	
f. If these are OPM managed files, do they meet the security requirements set out by OPM regulations 293.106 and 293.107 (see 5 CFR 293)?	

Requirement and Guidance Cite	Compliant (Yes/No)
<p>43 CFR 2.51(d) 383 DM 8.6</p>	
<p>II. Instructions to Employees Handling the Information</p>	
<p>a. Are system guidelines in place for employees working with a system of records? For example are there operating procedures to be followed in maintaining a specific records system and supplement the DOI regulations? 383 DM 1.4.G. 43 CFR 2.51(e)</p>	
<p>b. Do the IT Security business rules address the specific handling and disclosure and “need to know” access restrictions identified in the Federal Register notice for this system? OMB A-11 (See Exhibit 300 “Security/Privacy” section)</p>	
<p>c. Are employees who manage, use, or handle information from the Privacy Act system familiar with the Privacy Act and regulatory requirements and familiar with “any special requirements that their specific jobs entail.” 383 DM 3, Appendix I 43 CFR 2.52: Conduct of Employees 43 CFR 2.51(e) 383 DM 3.11 383 DM 7: Disclosure Procedures 383 DM 8: Safeguarding 383 DM 9: Handling PA Records</p>	
<p>d. Do the system manager and other employees using the information know who their Privacy Act contact is?</p>	
<p>e. Was a Privacy Impact Assessment done for the computerized system?</p>	
<p>f. Was it used to help identify the privacy concerns and handling requirements?</p>	
<p>g. Do contractors manager, use or handle information from the Privacy Act system?</p>	
<p>h. If yes to the above, are contractors provided with Privacy Act and DOI guidelines on handling the Privacy Act information, and with the specific instructions for this particular system? (e.g., business rules, <i>Federal Register</i> notice)</p>	
<p>i. Are paper records properly secured and not made visible to those who do not have a “need to know” the information?</p>	
<p>j. Are computer terminals, which may display sensitive information properly placed in order that only those who have a “need to know” can view the information?</p>	
<p>k. If there are no locked cabinets, do doors to the rooms have locks to ensure that only those who have a “need to know” will have access?</p>	
<p>III. Privacy Act Contract Clauses</p>	

Requirement and Guidance Cite	Compliant (Yes/No)
<p>a. Do contracts, which will be used to manage Departmental Privacy Act system on behalf of the agency, have appropriate privacy contract clauses included in them?</p> <p>FAR 48 CFR 24.102(a) The Privacy Act, Section (m) Federal Acquisition Regulations (FAR) at 48 CFR 24.103 DOI Acquisition Regulations 1452.224-1 See links at DOI Privacy Program website reference list at: http://www.doi.gov/ocio/privacy/guidelines_and_references.html</p>	
<p>b. If contractor is used, was a system manager designated to work with the contractor and to address the Privacy Act handling issues?</p> <p>43 CFR 2.53 FAR at 48 CFR 24.103</p>	
<p>IV. Accounting for Disclosures</p>	
<p>a. The Privacy Act requires that records be kept on all disclosures and made under the exceptions described in 2.56(c). Is there an accounting log or accounting system in place to track disclosure requests for information from the system and on what individual?</p> <p>383 DM 7.7 43 CFR 2.57</p>	
<p>Transfer of Privacy Act Records</p>	
<p>a. Are there procedures in place at the location that addresses the proper transfer of information from Privacy Act systems?</p> <p>383 DM 8.7</p>	
<p>b. When records are transferred to Federal Records Center or other facilities are 384 DM 4 followed?</p>	
<p>c. If information is moved, is it properly marked, and are handling instructions and use identified?</p>	
<p>Destruction of Privacy Act Records</p>	
<p>a. Does this system have have a records schedule? What is it?</p> <p>5 U.S.C. 552a(</p>	
<p>b. Are the records disposed of according to National Archives regulations at 36 CFR 1228.74.</p> <p>383 DM 8.8</p>	

Appendix K Background Investigation Scheduling

(found on next page)

HSPD-12 IMPLEMENTATION
OFFICE OF PERSONNEL MANAGEMENT INVESTIGATIONS

REQUIRED FORMS

	Non-Sensitive Position	National Security, Sensitive Position	Public Trust Position
New Federal Appointment	SF 85 (original) SF 87 OF 306 Application/Resume	SF 86 (original) SF 87 OF 306 Application/Resume	SF 85P (original) SF 87 OF 306 Application/Resume
Contractor	SF 85 (original) FD 258 OF 306 (limited items)	SF 86 (original) FD 258	SF 85P (original) SF 85P-S (Special Agreement) FD 258
Reinvestigation	SF 85 (original) SF 87 (Federal) FD 258 (Contractor) OF 306 (limited items)	SF 86 (original) Fingerprints optional SF 87 (Federal) or FD 258 (Contractor)	SF 85P (original) SF 85P-S (Special Agreement) SF 87 (Federal) or FD 258 (Contractor)
Update/Upgrade Investigation	Not Applicable	SF 86 (original) SF 87 (Federal) or FD 258 (Contractor)	SF 85P (original) SF 85P-S (Special Agreement) SF 87 (Federal) or FD 258 (Contractor)

Also see FIN Letter 98-02 and Fair Credit Reporting Act regarding signed releases to obtain credit checks

REQUESTING ADVANCE NAC AND FINGERPRINT CHECK

- ✓ To request an advance Fingerprint Check (FBI-CJIS Criminal Records Check only) enter "R" in the Codes block
- ✓ To request an advance National Agency Check (NAC) enter "3" in the Extra Coverage Block

TOP OF SF 85, SF 85P AND SF 86 QUESTIONNAIRE

OPM USE ONLY	Codes R	Case Number
Type of Investigation	Extra Coverage 3	

** Submitting Offices may request case status checks from the Federal Investigations Processing Center Liaison

OFFICE OF PERSONNEL MANAGEMENT CONTACTS

Security Appraisal/Assistance Officer (Policy)	202-606-1042, fax 202-606-2390
Federal Investigative Services Division, DOI Liaison Michele Lynch	202-606-2133
Federal Investigations Processing Center Liaison Assistance	724-794-2891
SII Searches, Questions about OPM Investigations, Case Status Checks	724-794-5228
Request Prior OPM Investigation Scheduled by Another Office	724-794-5228
Investigations Service webpage	www.opm.gov/extra/investigate

