# Department of Commerce

## Personal Identity Verification

## (PIV)

## Implementation Guidance

Date: March 3, 2008

***As guidance from***

***The Office of Management and Budget (OMB), the General Services Administration (GSA) Managed Services Office (MSO), Defense Manpower and Data Center (DMDC) and the National Institute of Standards and Technology (NIST). As bureau operational relationships change, this document will be revised accordingly.***

The point of contact for this guidance is the Director for Security Project Management Office, (202) 482-4544.

# Table of Contents

**EXECUTIVE SUMMARY ............ 6**

**1. INTRODUCTION ............ 8**

1.1 BACKGROUND ............ 8
1.2 PURPOSE AND SCOPE ............ 9
1.3 TIMELINES ............ 9

**2. ROLES AND RESPONSIBILITIES ............ 10**

2.1 GOVERNANCE ............ 10
*2.1.1 Office of the Secretary ............ 10*
*2.1.2 Office of Security ............ 10*
*2.1.3 Office of the Chief Information Officer ............ 11*
*2.1.4 Office of Acquisition Management and Financial Assistance ............ 12*
*2.1.5 Office of Human Resources Management ............ 13*
*2.1.6 General Sponsorship not previously covered ............ 13*
2.2 ORGANIZATION ............ 13
2.3 PRINCIPLES OF TRUST ............ 14
2.4 TEMPORARY DUTY AND LOCAL TRAVEL ............ 15

**3. DOCUMENTATION ............ 15**

3.1 DEVELOPMENT ............ 15
*3.1.1 Operations Plan ............ 15*
*3.1.2 System Privacy Impact Assessment (PIA) ............ 16*
*3.1.3 Corrective Action Plan ............ 16*
3.2 SUBMISSION ............ 16
*3.2.1 Accreditation Package ............ 16*
3.3 STORAGE ............ 17

**4. PRIVACY REQUIREMENTS ............ 17**

4.1 GENERAL ............ 18
4.2 PRIVACY POLICY ............ 18

**5. TRAINING ............ 19**

**6. CERTIFICATION ............ 19**

**7. ACCREDITATION DECISION ............ 20**

**8. PCIF MONITORING ............ 21**

8.1 PCIF MANAGEMENT AND CONTROL ............ 21
8.2 PCIF STATUS MONITORING ............ 21
8.3 STATUS REPORTING AND DOCUMENTATION ............ 21

**9. BUREAU/OPERATING UNIT REPORTING REQUIREMENTS ............ 23**

**10. PIV CARD TOPOGRAPHY ............ 24**

10.1 BUREAU AFFILIATION PIV CARD ZONE 20 DESIGNATIONS ............ 25
10.2 EMERGENCY RESPONSE OFFICIAL ............ 25

**11. ISSUING PIV CARDS TO FOREIGN NATIONAL PERSONNEL ............ 26**

**12. IMPLEMENTATION OF THE GENERAL SERVICES ADMINISTRATION (GSA) MANAGED SERVICE OFFICE (MSO) ROLES ............ 28**

**13. IMPLEMENTATION OF THE PIV CARD PROGRAM USING DOD INFRASTRUCTURE .........29**

**14. IMPLEMENTATION OF THE PIV CARD PROGRAM: INTERNAL INFRASTRUCTURE .........30**

**15. AFFILIATES, SHORT TERM VISITATION AND SPECIAL APPOINTMENTS.............................30**

**16. SERVICING SECURITY OFFICER (SSO) ROLES ..............................................................................31**

**17. FACILITY ACCESS CONTROL...................................................................................................35**

Appendix A— PCIF Operations Plan Annotated Outline ........................................ 38

Appendix B— Sample Memoranda and Accreditation Decision Letters................. 42

B.1 Certification/Accreditation Package Transmittal Letter.................................................... 42

B.2 Accreditation Decision Letter (Authorization to Operate) ................................................ 43

B.3 Accreditation Decision Letter (Interim Authorization to Operate)..................................... 44

B.4 Accreditation Decision Letter (Denial of Authorization to Operate) ................................. 45

Appendix C— Acronyms and Abbreviations.......................................................... 46

Appendix D— References ........................................................................................ 48

## Executive Summary

On February 25, 2005, the U.S. Department of Commerce (DOC) published Federal Information Processing Standard (FIPS) 201-1, Personal Identity Verification (PIV) Standard as directed by Homeland Security Presidential Directive (HSPD)-12. PIV-I of the Standard describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of HSPD- 12, including personal identity proofing, registration, and issuance. This standard was effective upon issuance. Federal departments and agencies were required to meet the requirements of PIV-I no later than October 27, 2005, in accordance with the timetable specified in HSPD-12. On October 26, 2005 the Deputy Secretary approved the Department's PIV-I process including the required accreditation of 10 card issuing locations.

The Department of Commerce selected the General Services Administration (GSA), Managed Services Office (MSO) Shared Service Provider (SSP) Program. The Commerce Deputy Secretary designated this relationship on April 27, 2007. Furthermore, the National Oceanic and Atmospheric Administration (NOAA) received a waiver to use the Department of Defense (DOD) Common Access Card (CAC) and the U.S. Patent and Trade Office (USPTO) received a waiver to leverage its infrastructure to create PIV compliant cards.

Our initial plan was to establish four DOC identity credential-issuing facilities under the GSA MSO SSP. Applicants located at the Herbert C. Hoover Building, (HCHB), Bureau of Economic Analysis, (BEA), and National Institute for Standards and Technology, (NIST) Gaithersburg, Maryland, Bureau of the Census, Suitland, Maryland, and Jeffersonville, Indiana, will be serviced by facilities at these locations. As mentioned previously, NOAA and USPTO received waivers to use other solutions. DOC employees not located in the above mentioned duty stations will use the GSA MSO facility locations around the country. In instances where there are no issuing facilities available to an applicant, the Director of Security will explore collaborative options with other agencies.

The Department began issuing its HSPD-12, FIPS 201-1, and PIV-I on October 11, 2005. The Department's card-issuing facilities were accredited by October 21, 2005. These card-issuing facilities will maintain their PIV-I control measure processes and procedures until an approved PIV card issuing solution has been implemented

Each DOC card-issuing facility and Regional Security Office (issuing GSA MSO PIV Cards) will have a Role Administrator (RA) who will be appointed by the card issuing facility manager. The facility manager will provide to the Credential Management Program Office (CMPO) his or her operational plan to implement FIPS 201-1 requirements. These procedures are based (as appropriate) on the cited references, the GSA MSO Operational Plan, the DOD, DMDC program policies and this document.

This document implements NIST Special Publication (SP) 800-79 titled: Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations. It also describes the

requirements and maintenance of PIV control measures posture and/or the integration into a compliant PIV-Card Issuance Program.
There are three PIV-II compliant solutions in the DOC.  These solutions are summarized below:

- The GSA MSO is a shared service provider that provides Federal agencies with interoperable identity management and credentialing solutions that provide end-to-end services to enroll applicants, issue credentials, and manage the lifecycle of these credentials. (See USAccess® Program Site: http://63.240.249.157/default.aspx )

- The National Oceanic and Atmospheric Administration (NOAA) will use the DOD CAC Program. The CAC is a DOD smartcard issued as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel.   https://www.cac.mil/Home.do

- USPTO will use a PIV conformant solution that will leverage its current architecture.

Under the current card issuance process there are two DOC procedures for card issuance.  The first is an in-person card issuance facility where DOC personnel could receive enrollment and issuance services from a DOC controlled site/location. The other process is for personnel to receive services at remote facilities, (non-DOC). The GSA MSO SSP shared service locations and for NOAA personnel DOD facilities will serve as DOC's remote enrollment and issuance facilities. During the transition timeframe the current PIV-I procedures will be maintained until the specific programs are implemented.

DOC, Director for Security will accredit card issuing locations in accordance with NIST Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations.[1]  NIST SP 800-79 outlines the certification and accreditation information to base card issuance facility certification and accreditation decisions.

Finally, this document will outline an interoperability procedure called the "Principles of Trust". DOC will accept the validity of the PIV cards issued by other agencies.  The essence of HSPD-12 is interoperability. PIV standards and guidelines include protective measures and precautions that facilitate trust in the PIV Card.  The Office of Security (OSY) will assure that agencies trusted by DOC are conformant the reliability tenet of HSPD-12.  This tenet states: "… (The PIV Card) is issued only by providers whose reliability has been established by an official accreditation process…" The Principles of Trust are based on the following SP 800-79 citation:

*"…If one agency would like to use the services of a PCI[2] of a second agency, the first agency should review the second agency's PIV policies and the PCI's operations plan, accreditation package, and Authorization to Operate. If acceptable the client agency may utilize the services of the server agency's PCI without re-accreditation…"*

[1] Additional questions and answers may be found on the following links: Questions & Answers, Part 1 (PDF) Questions & Answers, Part 2 (PDF)

[2] PIV Card Issuer (PCI)

# 1. Introduction

## 1.1 Background

On August 27, 2004, a Homeland Security Presidential Directive, HSPD-12 - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" was issued. HSPD-12 directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In response to this directive, the NIST published a FIPS 201-1 – "*Personal Identity Verification (PIV) for Federal Employees and Contractors*" on February 25, 2005. FIPS 201-1 and its associated publications provide detailed specifications for Federal agencies and departments, in order for them to issue PIV cards to their personnel. FIPS 201-1 standard and related publications can be obtained from the NIST website at http://csrc.nist.gov/piv-program.

Once implemented and issued by Federal agencies, the PIV card is envisioned to provide the attributes of security, authentication, trust and privacy using this commonly accepted identification credential.

Federal agencies have been planning to implement their compliance models since August 2004 using draft and/or interim guidance from OMB, GSA, and the National Institute of Standards and Technology (NIST). Final documents published recently that affected DOC's implementation strategies were:

- August 27, 2004 - Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*
- February 25, 2005 – (Document Updated June 26, 2006), Federal Information Processing Standard (FIPS) 201-1, *Personal Identity Verification of Federal Employees and Contractors*
- July 31, 2005 - Special Publication (SP) 800-79, *Guidelines for Certification and Accreditation of PIV Card Issuing Organizations*.
- August 5, 2005 - OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – *Policy for a Common Identification Standard for Federal Employees and Contractors*.
- June 23, 2006 – OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
- June 30, 2006 – OMB Memorandum M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*
- January 11, 2007 – OMB Memorandum M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*

- October 23, 2007 – OMB Memorandum M-08-01, *HSPD-12 Implementation Status*

### 1.2 Purpose and Scope

This document provides DOC's implementation instructions for compliance with HSPD-12 and the FIPS 201-1 Standard requirements. FIPS 201-1 is composed of two parts. The first part (PIV-I) describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance, but does not address the interoperability of PIV cards and systems among departments and agencies. The second part (PIV-II) completes the FIPS 201-1 conformance criteria, which states:

"The identity proofing, registration and issuance processes used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements stated in the FIPS and approved in writing by the head of the Federal department or agency." The Deputy Secretary Sampson approved the Department's accredited program on October 26, 2005.

The card issuing facility management will use this planning guidance to develop a local plan fulfilling requirements. Adherence to this guidance will provide the certification and accreditation (C&A) team with sufficient information to base an accreditation decision, including:

- The specific requirements for issuing PIV cards;
- The processes used for meeting the PIV card requirements;
- Adaptation of a specific PIV Card issuance solution's requirements and guidance
- The supporting materials and identity management related documents such as the PIV Card Issuer's (PCI) privacy policy for applicants, descriptions of management procedures for assuring continued reliable operations and all agreements with agencies using the services of the PCI; and
- Post-accreditation requirements for maintaining a reliable PCI.

The guidance in this document illustrates the intended methods of incorporation of HSPD-12 into the Department and PCI Facility (PCIF) credential issuing organizations plans, procedures, policies, and training programs.

### 1.3 Timelines

This implementation guidance requires PCIFs and Bureaus to develop internal operating processes and procedures as mandated by FIPS 201-1 and SP 800-79 and will comply with this document 30 days from the issue date.

# 2. Roles and Responsibilities

This section discusses the roles and responsibilities of key organizational participants for the implementation of Commerce's PIV card issuance system.

## 2.1 Governance

### 2.1.1 Office of the Secretary

In accordance with FIPS 201-1, PIV-I, the Department shall approve in writing the identity proofing and registration process used when verifying the identity of the applicant satisfying the requirements of FIPS 201-1.

### 2.1.2 Office of Security

The Office of Security, (OSY) will make policy recommendations and develop the Department's Credential Management Program. The Chief Financial Officer (CFO) and Assistant Secretary for Administration shall appoint the following role:

- **Senior Agency Official** - The Senior Agency Official (SAO) is responsible for the establishment, budget, and oversight of the PIV functions and services for the DOC.

  The *Director for Security* is the Senior Agency Official (SAO).

The SAO shall appoint the following roles:

- **Designated Accreditation Authority** - The Designated Accreditation Authority (DAA) is a senior agency official within the DOC with the authority to formally accredit the reliability of the PCIF in accordance with SP 800-79 guidelines.

  The *Deputy Director for Security* is the Designated Accreditation Authority (DAA).

- **Agency Identity Management Official** - The Agency Identity Management Official (AIMO) is responsible for ensuring that all services specified in FIPS 201-1 are provided reliably and that PIV cards are produced and issued in accordance with its requirements through the DOC PCIFs. The AIMO is the agency's Role Administrator (RA), in accordance with SP 800-79 guidelines.

  The *Chief,* CMPO is the AIMO.

- **Certification Agent** - The Certification Agent (CA) is responsible for establishing and ensuring reliability of the PCIF in accordance with SP 800-79. Performs certifications (comprehensive assessments) of the PCIF. The CA is independent from the PCIF operation and identifies discrepancies between the current status of the PCIF and the requirements of FIPS 201-1, and presents them to the PCIF Manager who will prepare recommended corrective actions to reduce or eliminate the discrepancies.
  The A*ssistant Director of the Anti-terrorism Division* is the CA.

- **PIV Card Applicant Representative** - A PIV Card Applicant Representative is responsible for representing the interests of current or prospective Federal employees and contractors who are the applicants for PIV credentials. The representative should represent the privacy concerns of applicants and assist an applicant who is denied a PIV card because of missing or incorrect information in an identity source document. An employee may be represented by a union representative in these matters if she or he so chooses. This designation is in accordance with SP 800-79 guidelines. The AIMO will appoint an agency Card Applicant Representative.

As stated above, The AIMO is the agency's Role Administrator (RA) for the GSA MSO Solution. The AIMO will designate the initial roles in the GSA MSO USAccess® System. (NOAA and USPTO do not have these roles in their solution.) Card Issuing Facility Managers of the GSA MSO USAccess® System will appoint the following roles:

- Role Administrator (RA)
- Agency/Enrollment Center Security Officer
- Sponsor Role - The PIV Sponsor
- Registrar Role
- Adjudicator Role
- PCIF Issuer / Activator Role

These roles are further explained in section 12 of this document.

OSY is responsible for the following:

- Adhering to the OSY/OHRM Memorandum titled "*Issuance of New Policy and Procedure for Processing of Suitability and National Security Investigations.*"

- Revising and maintaining the Department Security Manual and other Department publications that integrate the requirements of the FIPS 201-1 Standard and its related publications.

### 2.1.3 Office of the Chief Information Officer

The Office of the Chief Information Officer (OCIO) is the Department's primary HSPD-12 point of contact. The OCIO shall appoint the following role:

- Agency Official for Privacy (AOP): - The AOP is responsible for overseeing privacy-related matters in the PIV system and works with the PIV Card Applicant Representative to ensure that the rights of Applicants and PIV Subscribers (approved Applicants who have been issued a PIV credential) are protected. The role of the AOP is defined in FIPS 201-1 and may not assume any other operational role in the PIV system.

The Office of Chief Information Officer is responsible for the following:

- Is responsible for the development and maintenance of the OMB required Departmental HSPD-12 Implementation Plan;
- Coordinates the OMB required quarterly reporting requirements;
- Provide the primary and alternate Department representative on the Federal Identity Credentialing Committee;
- Recommend approval/disapproval waiver requests for the use of solutions other than the GSA MSO solution
- Provides oversight of E-Authentication Line-of-Business initiatives pertaining to HSPD-12; and

### 2.1.4 Office of Acquisition Management and Financial Assistance

The Office of the Acquisition Management and Financial Assistance (OAMFA) shall appoint the following role:

- **PIV Sponsor for Contractors** - The individual who substantiates the need for a PIV card to be issued to the contractor-Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV card to the contractor-Applicant.
  The *Contracting Officer's Representative (COR) or Contracting Officer's Technical Representative (COTR)* is the sponsor for all contractor employees.

The Office of Acquisition Management (OAMFA) is responsible for the following:

- Include language implementing the Standard in applicable new contracts. All new contracts, including exercised options, requiring contractors to have long-term access (greater than six months) to federally controlled facilities or access to federally controlled information systems shall include a requirement to comply with the Directive and Standard for affected contractor personnel. Include contract language in all contracts requiring the contractor to maintain a roster of all contractor employees who have a National Agency Check with Inquiries, (NACI) or higher investigation and those employees who currently possess a Federal Government issued PIV Card.

- For current contractors, develop a plan and begin the required background investigations for all those who do not have a successfully adjudicated investigation on record.

- Adhere to the OSY/OAMFA Memorandum titled: Guidance for Implementation of Homeland Security Presidential Directive (HSPD) 12 in Contracts.

- Adhere to the OAM Memorandum titled: Guidance for Implementation of Homeland Security Presidential Directive (HSPD) 12 in Grants.

- Contracting Officers will assure that each COR/COTR or Grants Liaison will include in the contract/grant language requiring the COR/COTR or Grants Liaison to provide a copy of the appointment memorandum to the servicing security officer. Additionally, the memorandum inform the COR/COTR or Grants Liaison of the requirement to comply with GSA MSO sponsorship and training requirements and/or other PIV-Card issuing sponsorship program requirements.

- The servicing Head of the Contracting Office (HCO) Contracting Officers are responsible for assuring the appointment of COR/COTR personnel. The Contracting Officer will appoint PIV sponsors for Contractors.
- Identify all contracting cross-bureau service agreements to OSY.

### 2.1.5 Office of Human Resources Management

The Office of the Human Resources Management (OHRM) shall appoint the following role:

- **PIV Sponsor for Employees** - The individual who substantiates the need for a PIV card to be issued to the Federal employee-Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Federal employee-Applicant.

The Office of Human Resources Management is responsible for the following:

- Adhere to the OSY/OHRM Memorandum titled "*Issuance of New Policy and Procedure for Processing of Suitability and National Security Investigations.*"
- Promulgate and maintain guidance that will assure compliance with 5 CFR 731, Suitability
- The servicing human resources office is responsible for appointing the PIV Sponsor for employees. The servicing human resources office is also responsible for adjudicating low risk DOC federal positions.
- Integrate PIV-Card Program required training requirements into the Commerce Learning Center, (CLC). (GSA MSO USAccess® System roles, only)
- Identify all Human Resources Management cross-bureau service agreements to OSY.

### 2.1.6 General Sponsorship not previously covered

A Sponsor is the individual who substantiates the need for a PIV credential to be issued to an applicant, enters the applicant's required sponsorship data elements into the system, and remains aware of the applicant's status and continuing need for holding a PIV credential. The Sponsor is responsible for managing the employment status of the cardholder in the managed service system through a web interface (for example, an employment/contract status may change when a cardholder retires, terminates, transfers to another department/agency/contractor, or for another reason no longer requires a PIV card). The Sponsor is the only person who can make corrections or changes to an applicant's information in the system.

## 2.2 Organization

OSY will maintain a list of all DOC operated PCIF/card issuing locations. DOC has implemented a manual (role-based) system to comply with PIV-I of FIPS 201-1. PCIFs are required to maintain this process until such time that their PCIF is fully integrated with a PIV-Card program, their operations plan will be revised to include all transitional activities and forwarded to OSY for the certification agent's review and accreditation assessment. The operational plan will provide details on the steps carried out as part of the processes to be employed at their facility.

The DOC PCIF managers may oversee facilities with multiple roles.  These roles will depend upon the client base they serve.

During the transition period the PCIF managers will need to maintain the current badging operation (the "PIV-I" system) to allow personnel to use existing automated access control systems. In locations where an automated access control system is not used, the PIV Card will be used to gain access via visual personal identity verification procedures. These verification procedures will adhere to the local security plan or other facility security procedure.

The roles of PCIFs will be based on the bureau's PIV-Card program solution.

### 2.3 Principles of Trust

PIV standards and guidelines include protective measures that establish a reasoned basis for trust of PIV Cards within the federal government.  Inter/intra-organization trust of PIV Cards is crucial to the DOC's implementation of HSPD-12.  This section describes the four levels of inter/intra-organizational acceptance of PIV Cards.  DOC has adopted the following levels of trust for our credentialing program: These levels are:

- Level 1 Internally (within Commerce) issued PIV Cards

- Level 2 Cards issued by the GSA MSO client organizations and DOD

- Level 3 Cards issued by go-it-alone Federal organizations where the DOC DAA has accepted that agency's accreditation.

- Level 4 Cards issued by commercial entities where the Federal PKI authority has certified its Certificates with the Federal bridge, where the organization follows FIP 201-1, and the federal government has approved their C&A and finally, where the DOC DAA has accepted that organization's accreditation.

The DOC CA will review the accreditation status of Levels 3 and 4 organizations annually.  The DAA will take the CA recommendations and determine whether to accept or deny the organization's accreditation.

Contractor employee credentials issued under one of these program levels will not require re-investigation or re-badging.  The RA/PCIF Manager will develop and annotate within their respective operations plans how they will enroll, track and revoke physical access.  This will not preclude the RA/PCIF Manager issuing non-PIV cards. The following are benefits the principle of trust will provide to DOC:

- Reduction of duplicate card issuance

- Seamless interoperation at DOC
- Use of the single Department-wide standard
- DOC cost savings and efficiencies
- Easier and faster processing
- Standard card procedures across DOC Bureaus

### 2.4 Temporary Duty and Local Travel

Where local or non-local travel is required to obtain a PIV card or Common Access Card, DOC will comply with all regulatory requirements for payment while in a duty status, including compensatory time off for travel (5 CFR Part 550), and all travel regulations. Bureau travel regulations will be applied to all Federal Employees who require travel in incidence to the enrollment, issuance and activation of PIV Cards. If the nearest enrollment, issuance and activation station for an employee is located outside of the local commuting area, normal travel authorization procedures will be followed: requests for travel will be approved by the employee's management official(s). DOC reserves the right to determine the most cost-effective and efficient means by which to ensure issuance of the PIV card, including potential use of mobile workstations, combining other official travel with issuance of the PIV card at a enrollment, issuance and activation site nearby the temporary duty station, etc.

## 3. Documentation

This section discusses the documentation requirements in terms of development, submission and storage requirements.

### 3.1 Development

#### 3.1.1 Operations Plan

Per the requirements of SP 800-79, each PCIF will develop an Operations Plan that must be included in the Accreditation Package submitted to the DOC DAA. Appendix A is the general format for this plan. Although some Regional Security Officer's will not issue PIV-Cards, it is important that they continue to outline their role in one or more of DOC's PIV-Card programs.

The plan will specify all the requirements for issuing PIV cards and describe the processes in place or planned for meeting those requirements. The plan will contain supporting material and related documents such as the privacy policy for applicants, descriptions of management procedures for assuring continued reliable operations, and all agreements with agencies regarding using the services of the PCIF.

PCIF will use the outline provided in Appendix B as a template for developing their individual operations plan.

If the system is not part of the DOC/Organizational Enterprise architecture, PCIFs must provide a determination and finding memorandum indicating the reason.

### 3.1.2 System Privacy Impact Assessment (PIA)

A PIA is a process for determining the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting information in identifiable form (IIF).

In accordance with Section 2.4 of FIPS 201-1, PCIFs are expected to currently have, or to conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal IIF for implementing PIV, consistent with the E-Government Act of 2002 (E-GOV) and the OMB Memorandum M-03-22 (M322), *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.

If the access control system does not have or is not covered by a PIA, the PCIF Manager must provide a determination and finding memorandum from the servicing privacy official indicating why the system does not have a PIA.

At locations where the GSA MSO is the SSP, their PIA sign will be physically posted within the PICF. The sign can be found at the following link: USAccess® Privacy Sign.

### 3.1.3 Corrective Action Plan

As part of the certification phase outlined in SP 800-79, a DOC CA will perform a comprehensive assessment of the PCIF in order to determine the extent to which the requirements of FIPS 201-1 are being achieved. The CA will use pre-selected assessment methods and will verify that PCIF controls are implemented correctly, operating as intended, and producing the desired outcomes.

The CA is responsible for identifying discrepancies between the current status of the PCIF and the requirements of FIPS 201-1, and presenting them to the PCIF Manager who will then prepare recommended corrective actions to reduce or eliminate the discrepancies.

The CAP prepared by the PCIF Managers, describes the measures being implemented and includes the following:

- Corrected deficiencies noted during the assessment; and
- Reduce or eliminate vulnerabilities to the creation and issuance of secure PIV credentials.

## 3.2 Submission

### 3.2.1 Accreditation Package

The *accreditation package* documents the results of the certification phase and provides the DAA with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the PCIF. The PCIF Manager is responsible for the assembly, compilation, and submission of the accreditation package. The accreditation package contains the following documents:

- PCIF’s operational plan, including all necessary attachments (privacy policies, standards, guidance, etc);
- PCIF’s assessment reports; and
- PCIF’s corrective action plan.

The local PCIF Manager then submits the accreditation package to the DAA.

### 3.3 Storage

A PCIF is required to collect, organize, store, and disseminate many documents important to its operations. All documentation must be kept current.

- **Plans -** Include PCIF’s operational plan and corrective action plan resulting from certification activities.
- **Policies -** Include the PIV Privacy requirements as specified in this document and information security policies relevant to the PCIF.
- **Standards and Guidelines -** Include all FIPS and NIST guidelines relevant to the PCIF, international, national, and industry standards applicable to the services and operations of the PCIF, especially those related to issuance of PIV cards.
- **Identity Source Documents -** PIV Card Applicants supply identity source documents specified in FIPS 201-1 so a PCIF can prove that the claimed identity is indeed that of the Applicant. These documents must be stored in a manner that assures their contents are protected, used only for authorized purposes, and be retrievable later for re-verification if needed. GSA and DOD have not yet determined the time of retention for these documents.
- **Forms/Reports -** Forms will be used to obtain information and reports will be produced to provide information. PCIFs may obtain or provide information without resorting to developing new forms whose formats may require prior approval.
- **Memoranda -** Personnel (employees and/or contractors) will be designated to perform duties as needed in the PCIF. Individuals and their delegates may be appointed via memoranda issued from RA. If designated by memorandum, it must be retained on file by the RA or outlined in the PCIF operation plan to demonstrate conformance with the organizational structure necessitated by SP 800-79.

## 4. Privacy Requirements

This section describes privacy requirements to be compliant with FIPS 201-I.

### 4.1 General

The following outlines general requirements to be adhered to by local PCIFs in order to be compliant:

- Ensure that personal information collected for employee identification purposes is handled consistent with the Privacy Act of 1974.
- Coordinate with appropriate officials to define consequences for violating privacy policies of the PIV system.
- Collect information using only forms approved by OMB under the Paperwork Reduction Act (PRA) of 1995. Agencies are encouraged to use Standard Form 85, Office of Personnel Management (OPM) *Questionnaire for Non-Sensitive Positions*, when collecting information. If information is collected using a newly developed form, OMB approval of the collection under the PRA process must be obtained. All background check and investigative packages will use OPM's Electronic Questionnaires for Investigations Processing (e-QIP) Gateway. e-QIP is part of an E-Government initiative sponsored by OPM. e-QIP allows applicants to electronically enter, update, and transmit their personal investigative data over a secure internet connection to DOC for review and approval.[3]
- Assure technologies used in the implementation of PIV allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program. For those using the GSA-MSO shared solution, this requirement is met by following procedures established by GSA documentation and the execution of an Interagency Security Agreement.
- Ensure technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of IIF. For those using the GSA-MSO shared solution, this requirement is met by following procedures established by GSA documentation and the execution of an Interagency Security Agreement.

### 4.2 Privacy Policy

- Sponsors must provide PIV Applicants with a full disclosure of the intended uses of the PIV card and the related privacy implications by referring them to the *Privacy Act Routine Usage* section of the SF85, 85P, or 86, and if requested, the system PIA may be made available.
- PCIFs will make available to all applicants the Department's privacy policy located at http://www.osec.doc.gov/cio/oipr/ITPrivacypol.html and GSA MSO privacy policies Privacy Impact Assessment and the USAccess® Privacy Sign .

[3] Census will use standard forms (SF) 85, 85P, and 86 until the e-QIP program is fully implemented within the bureau.

- NOAA will make available to all applicants the Department's privacy policy located at http://www.osec.doc.gov/cio/oipr/ITPrivacypol.html and DOD CAC privacy policies.

- USPTO will make available to all applicants the Department's privacy policy located at http://www.osec.doc.gov/cio/oipr/ITPrivacypol.html and the USPTO privacy policies.

The GSA MSO PIA covers the information that is collected from Personal Identity Verification (PIV) Applicants, the individuals to whom a PIV card is issued. The PIV Applicant may be a current or prospective Federal employee or contractor. As required by FIPS 201-1, GSA will collect biographic and biometric information from the PIV applicant in order to:

(i) Complete the identity proofing and registration process;

(ii) Create a data record in the PIV Identity Management System (IDMS); and

(iii) Issue a PIV Card. This information is collected, processed, maintained and destroyed by the General Services Administration's system and system personnel.

Therefore, PIA for the GSA MSO can not cover the activities of systems outside of GSA control. Examples are: Physical Access Control Systems, our system to track security activities (Foreign Nationals, Information and Personnel Security Functions) and e-mail exchange serves. These systems will need to maintain specific PIAs to show privacy impacts. Thus these system PIAs are of the out-of-scope of the GSA MSO PIA. The same may hold true for the NOAA and USPTO implementations. NOAA and USPTO will include all privacy policies within their respective operations plans.

## 5. Training

All PIV Card role holders are required to take the training respective to their role to orient them to the program.

The Commerce Learning Center will provide access to courses developed by the GSA MSO for all role holders. Bureaus not using the GSA MSO solution will develop training based on the solution's requirements. Personnel needing training should contact your servicing Security Officer for PIV-Card training requirements.

## 6. Certification

The CA provides recommendations to the DOC DAA with the information necessary to make credible decisions on whether to authorize the PCIF to issue PIV cards.

The DOC CA will assess the PCIF by evaluating attributes and operations of the organization to determine the extent to which the requirements of FIPS 201-1 have been achieved using the pre-selected assessment methods. CA shall verify that plans have been implemented correctly, operate as intended, and produce the desired outcomes. Recommended actions to be taken to correct deficiencies and discrepancies found during the assessment shall be made available to each PCIF.

Upon successful completion of this activity, the risk associated with the PCIF operations will have been determined, documented, and a recommendation made to the DOC DAA by the CA regarding accrediting the capability and reliability of the PCIF.

## 7. Accreditation Decision

Accreditation recommendations resulting from certification processes will be conveyed to the DAA by the CA. To ensure the business and operational needs of Bureaus, Organizations or Regional Offices are considered, the DAA will meet with the CA and the AIMO prior to issuing an accreditation decision to discuss the certification findings and the terms and conditions of the authorization.

The accreditation decision letter transmits the accreditation decision from the DAA to the PCIF Manager. The accreditation decision letter contains the following information:

- Accreditation decision;
- Supporting rationale for the decision; and
- Terms and conditions for the authorization.

The accreditation decision letter shall indicate to the PCIF Manager whether the PCIF is— (1) authorized to operate; (2) authorized to operate on an interim basis; or (3) not authorized to operate. The supporting rationale includes the justification for the DAA's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the PCIF. The accreditation decision letter is attached to the original accreditation package and provided to the PCIF Manager. A copy of the decision letter and the transmittal letter should be e-mailed to PIVaccreditation@nist.gov by the DAA.

Upon receipt of the accreditation decision letter and accreditation package, the PCIF Manager should review the terms and conditions of the authorization. The DAA should also retain a copy of the accreditation decision letter and accreditation package. The certification and accreditation-related documentation (especially information dealing with vulnerabilities) should be— (1) marked and protected appropriately in accordance with DOC policy; and (2) retained in accordance with the DOC's records retention policy.

All PCIFs must undergo a C&A determination prior to when the Department issues written approval that the process is compliant with FIPS 201-1. A matrix will be prepared to summarize the status of DOC PCIFs.

# 8. PCIF Monitoring

A critical aspect of the certification and accreditation processes is the post-accreditation period involving the monitoring of the operations and status of the PCIF. An effective monitoring program requires:

- Configuration management processes;
- Review and analysis of changes to the PCIF's procedures and practices; and
- Assessment and reporting of status changes to appropriate DOC officials.

It is important to document proposed or actual changes to the overall operation of the PCIF and to determine the impact of those changes to its reliability. The following sub-sections outline the tasks that will be implemented and carried out by the PCIF as part of a successful monitoring phase.

## 8.1 PCIF Management and Control

Documenting changes and assessing their potential impacts on an ongoing basis is an essential aspect of maintaining accreditation. As part of this activity, the PCIF Manager shall:

- Use established management and control procedures, document any changes that may be significant with respect to service offerings, PIV card issuing operations, or the PIV support automated system (including hardware, software, firmware, and surrounding environment); and
- Analyze the proposed or actual changes to (including hardware, software, firmware, and surrounding environment) the services and operations and analyze them to determine the impact of such changes.

## 8.2 PCIF Status Monitoring

The monitoring activity helps to identify potential problems during operations that are not identified during the certification phase. As part of this activity, the PCIF Manager shall:

- Select the attributes of the PCIF to be monitored; and
- Assess the required and selected attributes to determine the extent to which they are exhibited by the PCIF in all aspects of providing services to the bureau, Organization or Regional Office and producing the desired outcome with respect to meeting the requirements specified in FIPS 201-1.

## 8.3 Status Reporting and Documentation

The information in the status reports should be used as part of the determination of the need for re-accreditation and to satisfy DOC policy and specified requirements. As part of this activity, PCIF Managers shall:

- Update the PCIF’s operations plan based on documented changes to the PCIF’s operational requirements, personnel, facilities, equipment, and technology available to implement PIV systems and components and the results of the monitoring process;
- Update the CAP based on the documented changes to the operations plan and the results of the monitoring process; and
- Report the status of PCIF's accreditation to the DAA.

## 9. Bureau/Operating Unit Reporting Requirements

An important part of our PIV card issuance initiative is to understand the geographic attributes of bureau personnel points of presence. Personnel levels and locations are a dynamic reality. To assist OSY with assuring each DOC applicant is afforded the opportunity to obtain services from the most convenient location each bureau/operating unit will send to OSY, the following report:

This report will inform the AIMO and OSY where PIV-Card support is needed. The titles, are for the most part, are self explanatory. The below guide will assist the preparer with completing the form.

**Human Resource (HR) Support**: Indicate the bureau providing HR services

**Contract Support:** Most bureaus/operating units provide Contracting Officer Representative, (COR) and/or Contracting Officer Technical Representative, (COTR) from within the bureaus/operating unit. Contracting Officer's are those individuals with the authority to enter into, administer, and or terminate contracts and make related determinations and findings.

**Bureau/Operating Unit Points of Presence Report**

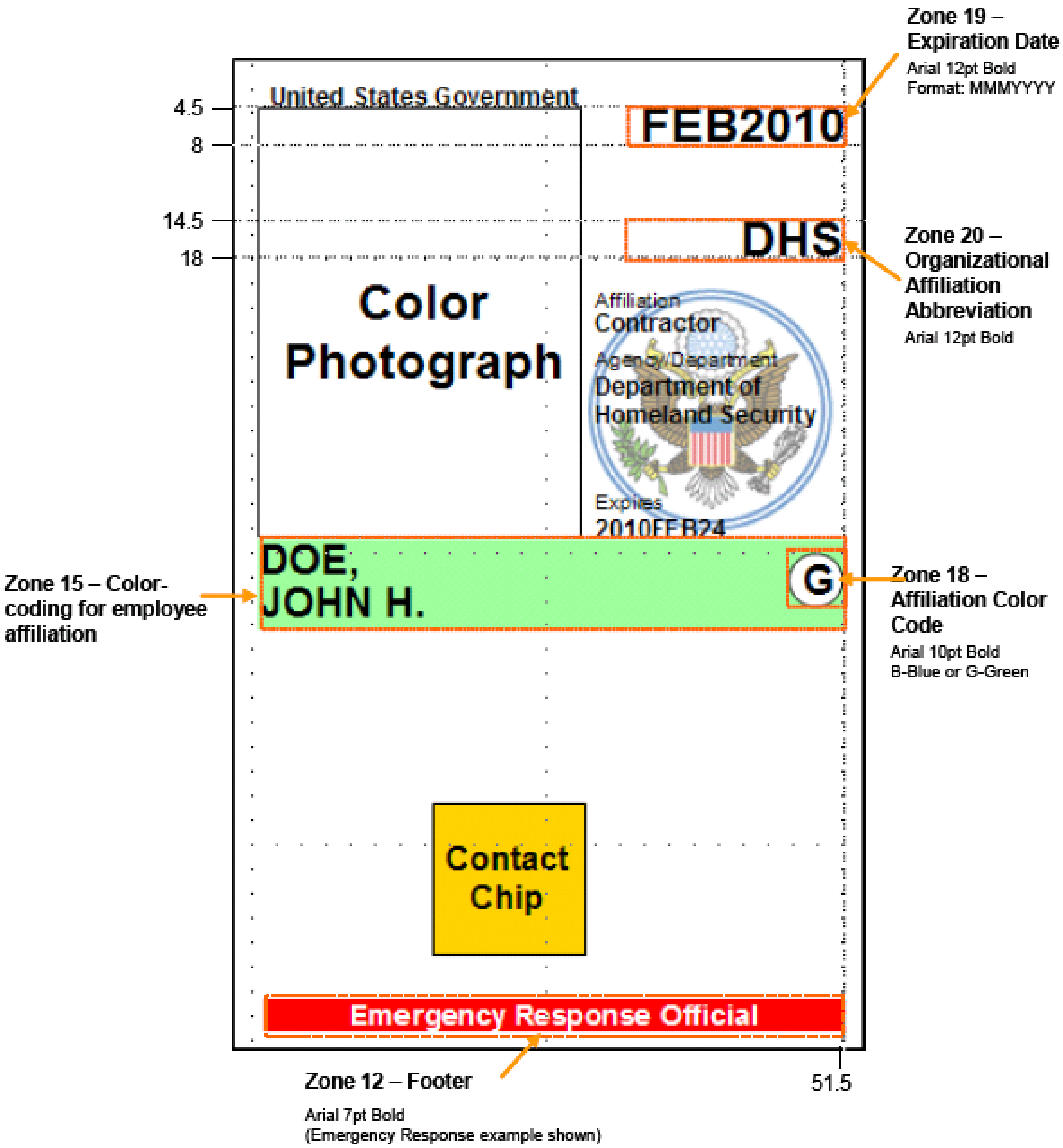
**BUREAU/Operating Unit:** ______________________________
**As of Date:** ______________________________
**Point of Contact:** ______________________________
**Email:** ______________________________
**Phone Number:** ______________________________

| | | | PERSONNEL | | | | HR | Contract | Security |
|---|---|---|---|---|---|---|---|---|---|
| **Facility Address** | **State** | **Facility Number** | **Federal** | **Contractor** | **Grantees** | **Others** | **Support** | **Support** | **Support** |

**Security Support:** The Director for Security provides access, medium and high risk adjudication and other services for the department. NIST and Census have a split security function. The Client Services Security Division provides security services for the occupants of the HCHB, Census, NOAA Headquarters and regional clients.

## 10. PIV Card Topography

Unless otherwise stated the DOC PIV Card will conform to Special Publication (SP) 800-104 Titled: A Scheme for PIV Visual Card Topography. The below figure shows the card characteristics. (NOAA use of the CAC will use Topography designated by DOD)



### 10.1 Bureau Affiliation PIV Card Zone 20 designations

Each bureau/operating unit will have a two to six letter designation indicating the bureau/operating unit of the badge holder. The letter code designations are:

| | |
|---|---|
| Office of the Secretary | OS |
| Office of the Deputy Secretary | OS |
| Office of the Inspector General | OIG |
| National Oceanic & Atmospheric Administration | NOAA |
| National Institute of Standards and Technology | NIST |
| Bureau of the Census | CENSUS |
| National Telecommunications & Information Administration | NTIA |
| Bureau of Economic Analysis | BEA |
| Bureau of Industry and Security | BIS |
| Economic Development Administration | EDA |
| Economic and Statistics Administration | ESA |
| International Trade Administration | ITA |
| Minority Business Development Agency | MBDA |
| Office of Civil Rights | OS |
| Patent and Trademark Office | USPTO |

The applicant sponsor will denote the above affiliation at the time of enrollment sponsorship.

### 10.2 Emergency Response Official

The color-coding for Emergency Response Official (ERO) is optional. The ERO color-coding, when used, shall be depicted at the footer location of Zone 12 and must print "Emergency Response Official" with white lettering on a red background. No other color-coding is permitted in Zone 12 when implementing SP 800-104.

Bureaus/operating units should designate positions (not people) that will have the Emergency Response Official red stripe badge annotation. The designation of people, only may incur increased cost to the government. Personnel duties may change more frequently than positions change. Therefore, sponsors will designate the Emergency Response Official at the time an employee is being sponsored in the PIV-card System. These positions and appointed personnel will be designated in accordance with the following criteria:

- The hierarchical priorities of SP 800-104 will be followed

- Positions and appointed personnel with Department Continuity of Operations Plan program responsibilities
- Positions and appointed personnel with National Response Plan and/or National Infrastructure Protection Plan responsibilities
- Positions and appointed personnel who are Law Enforcement, Security and Facility Management with contingent response responsibilities

All bureaus/operating units require this designation, the bureaus/operating units will forward a request from their emergency coordinator through the servicing security office to the Director of Security for approval.

Those personnel, who are designated as EROs, should be recipients of the annual letter required by the OPM. These individuals should have their specific duties noted and state that they will be in receipt of an appropriately designed credential so designating them. They and their supervisor are responsible to relinquish, (or cause relinquishment) this credential and the ERO PIV card, when their duties no longer require this designation.

Contractors with positions requiring the ERO designation will have the designations identified within the contract local language provisions.

Foreign National color-coding has precedence over government employee and contractor color-coding. Foreign National, Government Employee, and Contractor color-coding has precedence over ERO color-coding (this implies that Red will never be visible in Zone 15).

When Zone 15 indicates Foreign National affiliation and the department or agency does not need to highlight ERO status, the footer location of Zone 12 may be used to denote the country or countries of citizenship. If so used, the department or agency shall print the country name or the three letter country abbreviation (alpha-3 format) in accordance with ISO 3166-1, Country Codes [ISO 3166].

## 11. Issuing PIV Cards to Foreign National Personnel

HSPD 12 requires the establishment of a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal government to its employees and contractors. The National Agency Check with Written Inquiries (NACI)[4] or an equivalent background investigation is the minimum requirement to establish an individual's right to a claimed identity and determine their suitability to hold a compliant identity credential. On behalf of Federal departments and agencies, the OPM conducts NACI background investigations.

Some contractor and other personnel requiring HSPD-12 compliant identity credentials will not be United States (US) Citizens; Therefore, DOC will conduct the below identified activities to

[4] The National Agency Checks include the Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, FBI National Criminal History Fingerprint Check, National Credit Search (when requested), and Military Personnel Records Search (when applicable). The Written Inquiries portion includes records searches and checking references in related to an individual's background during the past five years. Inquiries are only made within the U.S. and its territories.

confirm that non-citizens are in a lawful immigration status and that the non-citizen is eligible for employment within the U.S.

DOC will conduct a check with U.S. Citizenship and Immigration Services' (USCIS) Verification Division, a component of the Department of Homeland Security (DHS), to ensure the individual is in a lawful immigration status and that they are eligible for employment within the US. During the check, Federal agencies will also be able to compare the photograph, or other biometric (e.g. fingerprints) if available, on immigration documents (e.g., Employment Authorization Document or Permanent Resident Card issued by USCIS) presented by the non-citizen against the biometric DHS has in their systems.

DOC will implement the following background check policy for non-U.S. citizens.

1. Verify immigration status or employment authorization.

Any non-US citizen working in the US and employed by the federal government, assigned to a government contract, or working in a partnership with the federal government, must be in a lawful immigration status and authorized employment. OPM will provide more detailed implementing guidance so agencies may verify immigration and employment eligibility.

Acceptable DHS credentials to prove employment authorized immigration status are:

Unexpired Permanent Resident Card (I-551)
Unexpired Employment Authorization Document (I-766)
Unexpired foreign passport with a valid I-94 or I-94A for a class of admission that permits employment

2. Verify biometrics taken at enrollment match the biometrics held by DHS.

To provide assurance of identity, the biometrics taken during the PIV enrollment process are to be matched against the biometrics maintained by DHS USCIS, where available and made available as part of determination of employment eligibility and/or lawful immigration status. This check applies to all non-US citizens requiring PIV credentials, regardless of length of time spent in the US. DOC will provide to OPM information that will permit OPM to conduct biometrics matching.

3. Complete a NACI Background Investigation. Once immigrant status and employment authorization records are verified, the following additional checks are required:

- For immigrant or non-immigrant visa holders in the US for 3 years or more, a NACI background investigation must be initiated.
- For immigrant or non-immigrant visa holders in the US less than 3 years, an FBI fingerprint check must be completed prior to credential issuance but the NACI background investigation may be delayed until the individual has been in the U.S. for 3 years.

4. Complete adjudication process.

DOC will adjudicate according to the standards found in title 5 CFR part 731, except for those individuals whose NACI's are delayed until such time as they have resided in the US for 3 years. As part of the adjudication process for non-US citizens, agencies must take into account the results of the US-VISIT database checks, FBI fingerprint checks, and NACI.

Department Administration Order 207-12, Titled: Foreign Visitor and Guest Access Program, is the governing policy for issuing PIV Cards to foreign visitors. OSY will provide to the Department additional requirements in a Standard Operating Procedure at a later date.

## 12. Implementation of the General Services Administration (GSA) Managed Service Office (MSO) Roles

Unless otherwise indicated, Departmental Bureaus will use the services of GSA MSO. The current implementation strategy calls for each bureau/operating unit to enter into annual interagency agreements with the MSO. In some instances the agreement will lease enrollment stations. These leased stations are dedicated (leased) to the leasing organization and are not required to, but may provide services to other MSO customers. The personnel not co-located with DOC leased enrollment centers will use the GSA MSO Shared Enrollment Center closest to the DOC applicant or such solution as may be provided the individual from their Bureau.

Until GSA MSO can provide credentialing services to DOC, applicants will continue to be credentialed using the current PIV-I process.

The AIMO will be the Agency RA for DOC. This role will be a focal point for GSA MSO (concerning SP 800-79 issues) for PCIF Managers operating GSA Leased Enrollment Centers. The Agency RA is responsible for authorizing and managing the Agency's Sponsor, Adjudicator, Registrar, and Activator roles and ensuring those personnel have been properly trained in the PIV process. Additional duties and responsibilities will be determined at a later date.

The Census PCIF Manager of the GSA Leased Enrollment Centers will appoint the Role Administrator for that center.

- **Role Administrator** - The Role Administrator is responsible for authorizing and managing the Enrollment Center's Sponsor, Adjudicator, Registrar, and Activator roles. The RA will assure that those personnel have been properly trained in the GSA MSO PIV process. (Census PCIF Managers may appoint the Role Administrator)

- **Agency/Enrollment Center Security Officer -** The Security Officer is the individual authorized to physically collect and revoke cards, and the daily contact for Agency employees who lose their PIV Cards. It is also the only role that has the ability to reactive a PIV Card.[5]

[5] This Security Officer function should not be confused with DOC's Regional or Servicing Security Officers. Nor should it be confused with the information Technology (IT) Security Program Officers. This role is strictly

- **Sponsor Role** - The **PIV Sponsor** acts on behalf of DOC or agency to substantiate the need for a PIV credential to be issued to an Applicant, enters the Applicant's required sponsorship data elements into the system, and remains aware of the Applicant's status and continuing need for holding a PIV credential.

- **Registrar Role** - **PIV Registrar** will adhere to the GSA MSO Registrar User Guide to enroll an applicant into the PIV system, ensures completion of a background check, and approves the issuance of the PIV card. The Registrar is the individual responsible for enrollment, which includes identity proofing the Applicant and collecting biographic information, a facial image, and fingerprints.

- **Adjudicator Role** - The **Adjudicator** is an individual who is authorized to record the adjudication result for an Applicant. A positive adjudication result will initiate the PIV Card issuance process.

- **PCIF Issuer / Activator Role -** The person who initializes and personalizes PIV cards at the PIV Card Issuing Facility (PCIF) and delivers PIV cards to authorized Applicants (directly) after completion of appropriate identity authentication and background checks is called the **PCIF Issuer.**

## 13. Implementation of the PIV Card Program using DOD Infrastructure

NOAA will use the DOD PIV-II compliant CAC to meet the PIV card requirements under HSPD-12. NOAA employees will receive PIV cards in accordance with the DODS implementation plan on a phased schedule for deployment of the software and hardware upgrades required to issue the PIV-II compliant CACs. Initial issuance of the new badges is expected to begin on or after March 12, 2008. NOAA employees will receive their CACs from one of the Real-Time Automated Personnel Identification System (RAPIDS) stations located around the country, including NOAA-operated RAPIDS stations in Silver Spring, MD and Seattle, WA. The CAC issued to NOAA employees will have a NOAA logo to differentiate NOAA employees from active duty military personnel. The process is summarized below. NOAA and the two OSY managed RAPIDS locations will develop an operations plan.

**NOAA New Employee Processing:**
1. New employees must complete NOAA's existing PIV-I processing including security checks, fingerprint checks, initiating a NACI or providing proof of NACI completion. The NOAA database file will be transmitted to DMDC for uploading to Defense Enrollment Eligibility Reporting System (DEERS)[6] on a periodic timeframe (anticipated to be daily) to add new employees and delete employees who have left the agency. The file will include fingerprints (where available in the format and quality necessary). At the time of transmittal, NOAA will

prescribed in the GSA MSO USAccess® System Operational Plan. This designation does not apply to those organizations that do not use the GSA MSO USAccess® System.

[6] To receive a CAC, all eligible personnel must be entered into DEERS – the authoritative source for CAC issuance. NOAA employees that have successfully completed PIV-I identity vetting requirements will be entered into DEERS.

verify to DMDC that all PIV-I requirements have been met, including a NACI being complete or initiated, and fingerprint checks complete.

2. Upon notification, the new employee is required to go to a RAPIDS station to be issued the CAC. Two forms of identification (I-9 documents) are required.

3. At card issuance, an employee can expect to provide the following:
   a. Digital photo
   b. Fingerprints (primary and secondary forefinger)
   c. A six to eight digit personal identification number (PIN) created by the Cardholder
   d. Signed acknowledgement of card receipt

**NOAA Existing Employee Processing:** Existing employees need only complete steps 2 and 3 above.

## 14. Implementation of the PIV Card Program: internal Infrastructure

Card issuing facilities will outline in their specific operations plans all portions of their PIV card issuing operations not covered by the GSA MSO. For example, The USPTO will use its own Federal Bridge PKI. This bureau operation plan will show how this PKI portion of card management will impact their card issuance process.

## 15. Affiliates, Short Term Visitation and Special Appointments

OMB M-05-24 provides guidance to agencies for temporary employees and contractors. The requirements for short term, temporary employees and contractors (foreign or domestic) should be viewed as the minimum requirements, dependent on risk and other factors. All PCIF Managers/Role Administrators/Servicing Security Officers (SSO) will consider this guidance in their operations plan.

If employed greater than six months, DOC will apply all sections of FIPS 201-1 and OMB M-05-24, including the background investigation requirements in the FIPS 201-1 standard.
If employed six months or less, DOC will apply the following factors and investigative requirements:

a) Apply adequate controls to systems and facilities (i.e. ensuring temporary staff has limited/controlled access to facilities and information systems).

b) Provide temporary employees and contractors with clear documentation on the rules of behavior and consequences for violation before granting access to facilities and/or systems.

c) Document any security violations involving these employees, and report them to the appropriate authority within 24 hours.

d) Identity credentials issued to these individuals must be visually and electronically distinguishable from identity credentials issued to individuals to whom the standard does apply.

DOC SSOs/PCIF Managers will not develop policies which overlap or contradict FIPS 201-1 or OMB directed processes for identity proofing and issuance.

Investigative requirements matrix outline general requirements for personnel requiring physical access to DOC facilities.  The PCIF/Role Administrators/SSOs will consult the DOC Security Manual for additional physical access control requirements.

The DOC Information Technology (IT) Security Policy outlines logical Access investigative requirements. Paragraph 17.2 states: “DOC requires that the IT Security Program Manager and operating units as necessary, develop, disseminate, and periodically review/update: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.”  PCIF/Role Managers will consult with their servicing IT Security Officer (ITSO) for logical access control investigative requirements.

The ITSO must monitor compliance of the system with applicable Departmental and Federal requirements and ensure the conduct of annual system self-assessments of security controls. The ITSO also monitors the timely completion of corrective actions to resolve control weaknesses identified in self-assessments or external reviews of controls and coordinates with the Department ITSPM on security issues and reporting on the security posture of the system.

## 16. Servicing Security Officer (SSO) Roles

**Servicing Security Officers**[7]

DOC Servicing Security Officers (SSO) implements Departmental security program activities in operating units on behalf of the Director of Security. SSOs provide security guidance, service, and support to the bureaus, operating units, and Departmental offices under their jurisdiction; implement security policies and procedures issued by the Office of Security; and coordinate any safeguarding requirements that specifically pertain to an operating unit with the appropriate head of an operating unit.

SSOs may formulate and issue supplementary instructions for their servicing area concerning personnel, information, and physical security matters. Each SSO must actively administer education and inspection programs for each office within their service area that processes, handles, or stores national security information.

Currently there are three types of SSOs.  The first is the SSO with location responsibilities.  The second is a SSO with regional responsibilities. The final SSO type has bureau-wide responsibilities only.  These SSOs will be referred to as Regional Security Officers (RSO). Under PIV-I, SSOs served as PCIF Managers.

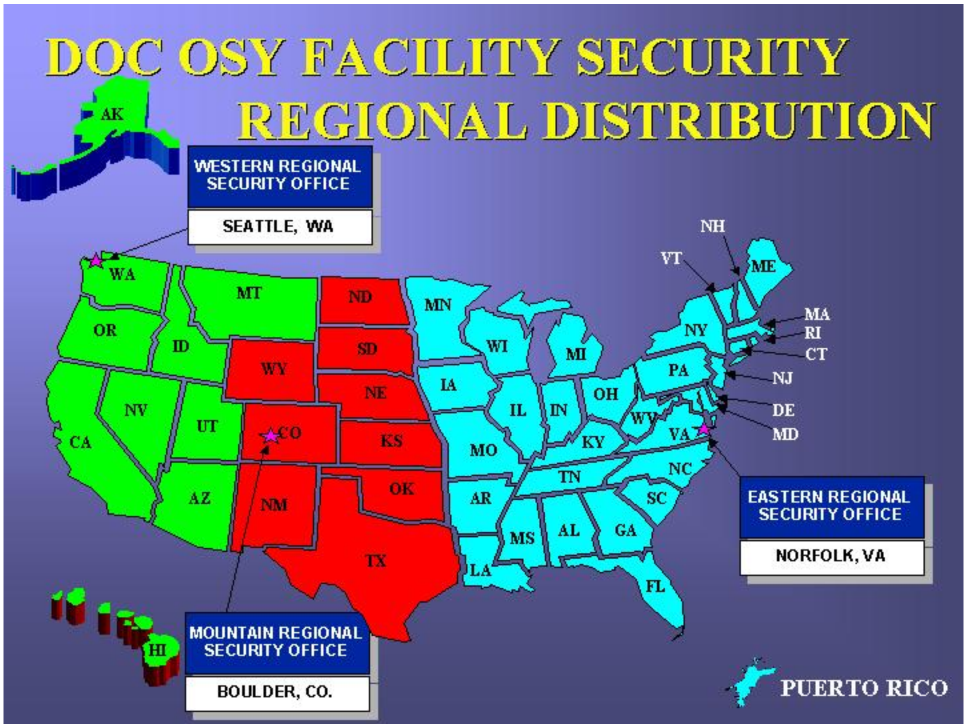
The SSO with location responsibilities are:

- The National Oceanic and Atmospheric Administration, (NOAA) Headquarters, Silver Spring, MD,
- The National Institute of Standards and Technology (NIST), Gaithersburg, Maryland
- Security Officer for the Herbert C. Hoover Building, (HCHB)

[7] U.S. DEPARTMENT OF COMMERCE, MANUAL OF SECURITY, POLICIES AND PROCEDURES Section I, Chapter 2, Subparagraphs D 1 and 2

- Census and The Patent and Trade Office (USPTO) have bureau security officers
- The Eastern Regional security Office (ERSO), Mountain Regional Security Office (MRSO)
- Western Regional Security Office (WRSO).

These SSOs managed compliant and accredited PCIFs. Under PIV-II the SSO functions will change based on the location and the area of SSO responsibilities. Each SSO will prepare an operations plan using the format shown in Appendix A. For those SSOs who do not have a PIV card, issuing responsibility will outline in the plan their support roles. Typical support roles may include physical security planning recommending PIV compliant components, suitability and adjudication support. The following is a general overview of PIV-II responsibilities for each SSO. The RSO will provide suitability and adjudication results to the GSA MSO web portal, in accordance the jointly signed policy titled: Issuance of New Policy and procedures for the processing of Suitability and National Security Access Investigations.



The above map shows the regional geographical areas of responsibilities.

**<u>The SSO for NOAA Headquarters, Silver Spring, MD:</u>** NOAA received approval from DOC and DOD to use the CAC. These credentials will be PIV-II compliant and were approved by the OMB. NOAA will align its implementation with the timelines approved for DOD by OMB. DOD has promulgated manuals and processes for the issuance of CAC credentials at over 2,000 locations world wide. Because of the location status, SSO NOAA HQ will issue DOD CAC PIV-II Credentials only. Non-PIV Cards will be issued in accordance with DOC Security Manual and the SSO's operations plan. Not all DOD RAPIDS sites currently contain the necessary software upgrades to issue PIV-II cards. DOD is installing PIV-II software at its RAPIDS sites in a phased approach, with nationwide implementation completed by January, 2009. NOAA will ensure that a listing of PIV-II compliant RAPIDS sites is made available to employees via NOAA's website prior to implementation to ensure that sites identified contains the needed software to issue PIV-II compliant badges.

**WRSO, Seattle, WA:** WRSO will issue PIV-II compliant credentials under the DOD CAC credential program and provide referrals to NOAA personnel requesting DOD CAC Credentials who are not co-located near WRSO Offices. DOD has established an interactive web site to assist with these referrals. This Website: http://www.dmdc.osd.mil/rsl/owa/home allows the applicant to enter his/her location on the site. The results will show the closest DOD CAC Credential issuance location with the approximate mileage. Not all DOD RAPIDS sites currently contain the necessary software upgrades to issue PIV-II cards. DOD is installing PIV-II software at its RAPIDS sites in a phased approach, with nationwide implementation completed by January, 2009. NOAA will ensure that a listing of PIV-II compliant RAPIDS sites is made available to employees via NOAA's website prior to implementation to ensure that that site identified contains the needed software to issue PIV-II compliant cards.

Furthermore, WRSO's regional responsibilities that the RSO has are the adjudication responsibilities for non-NOAA bureaus in the regions area of responsibility. The RSO will provide suitability and adjudication results to the GSA MSO web portal, in accordance the jointly signed policy titled: Issuance of New Policy and procedures for the processing of Suitability and National Security Access Investigations. To accomplish these tasks the RSO adjudicators will need to access GSA MSO Web portal. This will require each adjudicator to take GSA's required training located on the Commerce Learning Center's web portal and be enrolled in GSA's system. Non-PIV Cards will be issued in accordance with DOC Security Manual and the SSO's operations plan. Commerce has adopted the GSA MSO as the department PIV-II solution.

**ERSO, Norfolk, VA and MRSO, Boulder, CO:** ERSO/MRSO will not issue PIV-II Compliant credentials. ERSO will provide referrals to NOAA personnel requesting DOD CAC Credentials within ERSO geographical area of responsibility. DOD has established an interactive web site to assist with these referrals. This Website: http://www.dmdc.osd.mil/rsl/owa/home allows the applicant to enter his/her location on the site. The results will show the closest DOD CAC credential issuance location with the approximate mileage. Not all DOD RAPIDS sites currently contain the necessary software upgrades to issue PIV-II badges. DOD is installing PIV-II software at its RAPIDS sites in a phased approach, with nationwide implementation completed by January, 2009. NOAA will ensure that a listing of PIV-II compliant RAPIDS sites is made available to employees via NOAA's website prior to implementation to ensure that that site identified contains the needed software to issue PIV-II compliant badges.

Furthermore, ERSO's regional responsibilities that the RSO has are the adjudication responsibilities for non-NOAA bureaus in the regions area of responsibility. Commerce has adopted the GSA MSO as the department PIV-II solution. The RSO will provide suitability and adjudication results to the GSA MSO web portal, in accordance the jointly signed policy titled: Issuance of New Policy and procedures for the processing of Suitability and National Security Access Investigations. To accomplish these tasks the RSO adjudicators will need to access GSA MSO Web portal. This will require each adjudicator to take GSA's required training located on the Commerce Learning Center's web portal and be enrolled in GSA's system. Non-PIV Cards will be issued in accordance with DOC Security Manual and the SSO's operations plan.

**SO, Census Suitland, MD:** The SO for Census has bureau-wide security responsibilities. The Bureau is participating with the GSA MSO solution for its PIV-II Credential. The Client Services Security Division, (CSSD) *and servicing HRD Office* will provide suitability and adjudication results to the GSA MSO web portal, in accordance the jointly signed policy titled: Issuance of New Policy and procedures for the processing of Suitability and National Security Access Investigations.[8]

**SO, NIST Gaithersburg, MD:** Because of the location status, the SO for NIST Gaithersburg will issue GSA MSO PIV-II Credentials only. Non-PIV Cards will be issued in accordance with DOC Security Manual and as supplemented by the SO's operations plan. CSSD will provide suitability and adjudication results to the GSA MSO web portal, in accordance the jointly signed policy titled: Issuance of New Policy and procedures for the processing of Suitability and National Security Access Investigations.

**SO HCHB, Washington, D.C.:** Because of the location status, the SO for HCHB will issue GSA MSO PIV-II Credentials only. Non-PIV cards will be issued in accordance with DOC Security Manual and as supplemented by the SO's operations plan. The SO, HCHB will service the bureaus located at the HCHB, except NOAA. The OSY Counter Espionage Division will provide suitability and adjudication results to the GSA MSO web portal, in accordance the jointly signed policy titled: Issuance of New Policy and procedures for the processing of Suitability and National Security Access Investigations.

**SO, USPTO, Alexandria, VA:** The SO for USPTO has bureau-wide security responsibilities. The Bureau will create its own solution for its PIV-II Credential. The SO will develop a comprehensive operations plan that will cover all elements of the PIV Card program management. This plan will be the basis of USPTO accreditation. Non-PIV Cards will be issued in accordance with DOC Security Manual and as supplemented by the SO's operations plan.

[8] NOTE: the decennial is not subject to the requirements of PIV Card implementation. The length of employment for these numerators is under 180 days. *If such appointment is extended beyond 180 days, it will be treated as a new appointment for purposes of HSPD-12.* Temporary employees for the decennial census will not adhere to the PIV Card Issuance Standards.

## 17. Facility Access Control

The DOC Security Manual Chapter 31 Titled: “Physical Security Planning” outlines how physical security programs will be planned. Chapter 34 Titled: “Identification and Admittance to Facilities,” provides DOC policy for facility access control. Chapter 36 Titled: “Guard Services” is the policy for acquisition and deployment of these services. Over the next year these and other security manual chapters will be realigned to conform to the tents of HSPD-12 requirements.

As DOC transitions to smart card technologies there will be a period of time the Security Officers/Guards will be challenged to determine which identification (ID) card is valid for general entry. PIV-II look-alike test cards are available today in great numbers. Some commercial firms have adopted PIV-II look-alike cards as their company access card and others have provided these cards to participants at trade shows and events. Security Officers/Guards must be vigilant to ensure the authenticity of the presented card is valid, to the greatest extent possible.

Therefore, implementing FIPS 201-1 smart card system will make extended use of flash-then-pass procedures until such time as the marketplace provides less costly entry systems and the Federal fiscal situation will allow system and entry-way upgrades. Until these issues are resolved, DOC’s servicing RSO will provide or recommend efficient ingress and egress control of personnel. Over the next 2-3 years, many facilities will use the PIV-II card as a flash-then-pass access control medium. The convergence of PACS into the enterprise architecture will eventually allow for the verification of Federal bridge PKI Certificates. This verification, initially, will be on an exception basis and at facilities that can fund the infrastructure.

Each RSO will develop a regional security plan identifying all Department of Justice Level III and IV facilities where physical access control (Security Officers) and/or physical access control systems are recommended and/or installed. The plan will consist of the following attributes:

- Two architectures identifying the current access control status and a target access control posture.
- Perform a gap analysis between these architectures and develop a transition plan that will bring the region to the target architectural state.

Security system migration requirements should be derived from an agency’s Physical Security Enterprise Architecture Program. The basic framework is contained in the Federal Enterprise Architecture Program[9]. The two basic components of this type of architecture are the current and target architectures. The Current Architecture is a blueprint of the organization, as it exists now. It is the starting point for all planning activities. The Target Architecture is a blueprint of the organization, as it needs to be to support the protection profile of the agency. For the purposes of this implementation guidance, physical access will be the focus. Once the two architectures types are developed, a Gap Analysis is performed. The Gap Analysis examines the Current state and the Target state, determining for each of the four levels what needs to change

[9] Federal Enterprise Architecture Program http://www.whitehouse.gov/omb/egov/a-2-EAModelsNEW2.html

or is required to achieve the Target.  This would include any organizational changes, enhanced business processes, data requirements, applications, and infrastructure components.

Finally, a migration plan must be developed to chart the course of reaching the target, architecture.  The Migration Plan builds off of the Gap Analysis and breaks it down into manageable projects. The structure of this planning is:

- Overall strategy - define priorities and dependencies, show linkage to project management
- Funding - once a project is identified, show linkage to the OMB A-11 Capital investment process (Ex 300 or similar for smaller projects)
- Collaboration - evaluate opportunities to build from existing components and/or identify others doing similar projects and combine resources
- Implementation Timeline – if a detailed project plan exists, link to it. If not, provide completion dates and major milestone dates where possible.

The convergence of Physical Security and IT systems requires a framework to organize our approach to the implementation of HSPD-12. The enterprise architecture will identify the inventory of all Security “Specific” programs and automated systems that will be impacted by the implementation of HSPD-12. The fundamental part of the Physical Security Enterprise Architecture is the modeling of enterprise security services throughout DOC.  This architecture will inventory all systems in a baseline Architecture, define security business processes, develop target architectures (three to five years out), and create a migration plan that will identify the gap between the baseline (current) and target architectures.

The information reported in these plans is sensitive and the OSY Anti-Terrorism Division will consolidate them into one comprehensive plan. RSO’s will take care to restrict access to these plans.

***This page intentionally left blank***

# Appendix A—PCIF Operations Plan Annotated Outline

PCIF Operations Plan Annotated Outline

## COVER PAGE

# Personal Identity Verification (PIV)

## Operations Plan
## For

# <<Name of the PCI Facility>>

<<Publication Date>>

Contact Point
<Name of >
<Title>
<Bureau/Organization/Regional Office>
<Phone>

## INTRODUCTION

### BACKGROUND

*<Provide a brief background/project description on the plan>*

### PURPOSE AND SCOPE

*<Provide the purpose and scope of this document>*

### ASSUMPTION AND CONSTRAINTS

*< Enter any assumptions or constraints used to develop this operations plan>*

### APPLICABLE LAWS, DIRECTIVES, POLICIES, REGULATION & STANDARDS

*<List any specific laws and regulations that are applicable to the information processed by the PIV system, which establish specific requirements for confidentiality, integrity, availability, (CIA) auditability and accountability of information in the system.>*

## PCI FACILITY DETAILS

### UNIQUEPCIFIDENTIFIER

*<Unique Identifier for the PCI>*

### NAME OF THE ORGANIZATION SPONSORING THE PCI

*<Sponsoring Organization Information>*

### OPERATION PLAN STATUS

*< Provide the current status of the PIV Card Issuer operations: i) N/A initial C&A not performed, ii) ATO , iii) IATO, iv) DATO.>*

### ORGANIZATION

#### *ORGANIZATION STRUCTURE/CHART*

*<Provide with the help of a chart/illustration the PIV issuing organization>*

#### *CONTACT INFORMATION*

*<Provide the names along with the contact information for the following personnel>*

PCI Facility Manager
Designated Accreditation Authority
Authorized Sponsors for the PCI

## PROCESS DESCRIPTION

### IDENTITY PROOFING AND REGISTRATION

*< Discuss in detail the processes used to perform identity proofing and registration. Include details such as how vital and sensitive applicant's information is stored, transfer process between various roles etc. Refer to Appendix C for particulars on what needs to be included in this section>*

### ISSUANCE

*< Discuss in detail the processes used to perform issuance of the PIV credential. Refer to Appendix C for particulars on what needs to be included in this section>*

### MAINTENANCE

*< Discuss in detail procedures used when PIV credentials are lost, stolen, damaged or have expired. Also discuss termination procedures in the event, employees or contractors no longer require the identity credential >*

## TECHNICAL SYSTEM DESCRIPTION

### SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

*<Provide a (1-3 paragraphs) general technical description of the automated system(s) used by the PCIF in performing the required services, including the distributed, collaborative computing environments comprising the PIV System. Discuss any environmental factors that raise special security concerns (e.g., internet connectivity, dial-up access) and document the physical location of the system. Provide a network diagram or schematics to help identify, define, and clarify the system boundaries for the system. Provide a description of the system and sub-applications and other software intra-dependencies.>*

### SYSTEM INTERCONNECTIONS / INFORMATION SHARING

*< Provide a description of the network used for communicating with information systems and the PIV System, including any system interconnections and/or information sharing (inputs/ outputs) outside the scope of this plan. Show how the various components and sub-networks are connected and/or interconnected to any other system. Include information on the authorization for connections to other systems or the sharing of information.>*

### SYSTEM INVENTORY

*<Provide a complete list of inventory (hardware and software) of all the components that comprise the PIV credential issuance system. Include information on the system name, its purpose and the system owner.>*

## PCI FACILITY MANAGEMENT

*<Descriptions of management procedures, including configuration management processes, review and analysis of changes to the PCI's procedures and practices, assessment and reporting of status changes to appropriate organization officials etc., for assuring continued reliable operations. Describe any configuration management procedures for the system including; testing and/or approving system components prior to production, impact analyses to determine the effect of proposed changes on existing security controls and change identification, approval, and documentation.>*

## APPENDIX-A: ACRONYMS AND ABBREVIATIONS

## APPENDIX-B REFERENCES

## ATTACHMENT A

*<PCI's Privacy policy for applicants>*

## ATTACHMENT B to …

*<Agreements with other agencies regarding using the services of the PCI>*

*This page intentionally left blank*

# Appendix B—Sample Memoranda and Accreditation Decision Letters

## B.1 Certification/Accreditation Package Transmittal Letter

Date:
To:
From:
RE:

A certification of the [PCI NAME] located at [LOCATION] has been conducted in accordance with NIST Special Publication (SP) 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations* and the [DoC] policy on PCIF accreditation. The attached accreditation package contains— (i) the PCIF operations plan; (ii) the assessment report; and (iii) a corrective action plan (CAP).

The PCIF operations plan, its procedures, and its attributes have been assessed by [CERTIFICATION AGENT] using the assessment methods and procedures defined in SP 800-79 and specified in the assessment report to determine the extent to which the required and desired attributes of a capable and reliable PCIF are exhibited and if the PIV Card issuing procedures are operating as intended and producing the desired results. The CAP describes the corrective actions that we plan to perform to remove or reduce any remaining deficiencies detected in the PCI's procedures and attributes.

Signature

Title

•

## B.2 Accreditation Decision Letter (Authorization to Operate)

Date:
To:
From:
RE:

---

After reviewing the results of the certification and accreditation package of the [PCI] and it's supporting automated PIV system support components located at [LOCATION] and the evidence provided in the associated accreditation package, I have determined that the PCI's plan and procedures and capabilities are in compliance with FIPS 201-1 and our privacy and security policies and are acceptable. Accordingly, I am issuing an *authorization to operate* (ATO) the PCI's services in its existing or specified operating environment. The PCIF is accredited without any significant restrictions or limitations. This accreditation is my formal declaration that adequate attributes are being exhibited by the PCI, that a satisfactory level of capability and reliability is present, and that the PCIF is expected to this maintain this capability, reliability, and operational status for at least the next three years or until a major change is made to its operation.

This accreditation and ATO will remain in effect as long as— (i) the required monitoring is performed and status reports for the PCIF are submitted to this office every [TIME PERIOD – ONE YEAR IS RECOMMENDED]; (ii) the problems detected during the monitoring process do not result in organization-level risks that are unacceptable; and (iii) the capability and reliability of the PCIF is re-accredited within the lesser time of three (3) years or the re-accreditation requirements established by organization policy.

A copy of this letter with all supporting certification and accreditation documentation should be retained in accordance with the organization's record retention schedule.

________________________________

Signature

Title

### B.3 Accreditation Decision Letter (Interim Authorization to Operate)

Date:
To:
From:
RE:

---

After reviewing the results of the certification of the [PCI] and its supporting automated PIV system support components located at [LOCATION] and the evidence provided in the associated accreditation package, I have determined that the required attributes exhibited by the [PCI] are *not* acceptable. However, I have determined that there is an overarching need for the PCIF to provide the needed services due to mission necessity and other considerations. Accordingly, I am issuing an *interim authorization to operate* (IATO) the PCIF services in its existing operating environment. Operation of the PCIF must be performed in accordance with the enclosed terms and conditions during the IATO period and all detected risks of operation and problems encountered during operation should be documented. The PCIF is *not* considered accredited during the IATO period.

Reliability of the PCIF operations and security of the PCI's automated support systems must be monitored rigorously during the IATO period. Monitoring activities should focus on the specific areas of concern identified during the certification assessments. Significant changes in the status of the operations during the IATO period should be reported immediately. All PIV Cards issued by the PCIF during this period should be marked in the PIV System so that agencies accepting the Cards for access control decisions are aware they were issued by the PCIF during an IATO period. Once accreditation is obtained by the PCI, these Cards should be examined and the marking removed for the Cards that are determined to meet the requirements of the accredited PCI.

This interim authorization to operate is valid for a maximum of three (3) months. The limited authorization will remain in effect as long as— (i) the required status reports for the system are submitted to this office every month; (ii) the problems or deficiencies reported during the monitoring process do not result in additional risk which is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating the deficiencies in accordance with the CAP. At the end of the IATO period, the PCIF must be certified, accredited and authorized to operate or the authorization for further operation will be denied. A second IATO will be granted only under extenuating circumstances. This office will review the CAP submitted with the accreditation package during the IATO period and monitor progress on removal or reduction of concerns and discrepancies before re-accreditation is initiated.

A copy of this letter and all supporting certification and accreditation documentation should be retained in accordance with the organization's record retention schedule.

________________________________

Signature

Title

### B.4 Accreditation Decision Letter (Denial of Authorization to Operate)

Date:
To:
From:
RE:

---

After reviewing the results of the certification of the [PCI] located at [LOCATION] and the supporting evidence provided in the associated accreditation package, I have determined that the attributes exhibited by the PCIF are unacceptable. Accordingly, I am issuing a denial of authorization to operate (DATO) the PCIF in its planned or existing operating environment. The PCIF is *not* accredited and [MAY NOT BE PLACED INTO OPERATION or ALL CURRENT OPERATIONS MUST BE HALTED].

The Corrective Action Plan (CAP) should be pursued immediately to ensure that proactive measures are taken to correct the deficiencies found during the assessment. Re-certification and re-accreditation should be initiated at the earliest opportunity to determine the effectiveness of correcting the deficiencies.

A copy of this letter with all supporting certification and accreditation documentation should be retained in accordance with the organization’s record retention schedule.

______________________________

Signature

Title

•

## Appendix C—Acronyms and Abbreviations

| | |
|---|---|
| AIMO | Agency Identity Management Official |
| AOP | Agency Official for Privacy |
| ATO | Authorization to Operate |
| BEA | Bureau of Economic Analysis |
| BIS | Bureau of Industry and Security |
| CA | Certification Agent |
| C&A | Certification and Accreditation |
| CAC | Common Access Card |
| CAP | Corrective Action Plan |
| CAR | Card Applicant Representative |
| CFO | Chief Financial Officer |
| CLC | Commerce Learning Center |
| CMPO | Credential Management Program Office |
| CO | Contracting Officer |
| COR | Contracting Officer Representative |
| COTR | Contracting Officer Technical Representative |
| DAA | Designated Accreditation Authority |
| DATO | Denial of Authorization to Operate |
| DMDC | Defense Manpower Data Center |
| DOD | Department of Defense |
| DOC | Department of Commerce |
| DOS | Department of State |
| EDA | Economic Development Administration |
| E-QIP | Electronic Questionnaires for Investigation Processing |
| ESA | Economic and Statistics Administration |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| GSA | General Services Administration |
| HSPD | Homeland Security Presidential Directive |
| IATO | Interim Authorization to Operate |
| IDMS | Identity Management System |
| IIF | Information in Identifiable Form |
| ITA | International Trade Administration |
| MBDA | Minority Business Development Agency |
| MOU | Memorandum of Understanding |

| | |
|---|---|
| MSO | Managed Service Office |
| NAC | National Agency Check |
| NACI | National Agency Check with Inquiries |
| NIST | National Institute for Standards and Technology |
| NOAA | National Oceanic and Atmospheric Administration |
| NTIA | National Telecommunications & Information Administration |
| OAM | Office of Acquisition Management |
| OCIO | Office of Chief Information Officer |
| OHRM | Office of Human Resource Management |
| OMB | Office of Management and Budget |
| OIG | Office of the Inspector General |
| OMO | Office of Management and Organization |
| OPM | Office of Personnel Management |
| OSY | Office of Security |
| PCI | PIV Card Issuer |
| PCIF | PIV Card Issuer Facility |
| PIA | Privacy Impact Assessment |
| PIV | Personal Identity Verification |
| PKI | Public Key Infrastructure |
| PRA | Paper Reduction Act |
| RA | Role Administrator |
| RAPIDS | Real-Time Automated Personnel Identification System |
| RSO | Regional Security Office |
| SAO | Senior Authorizing Official |
| SF | Standard Form |
| SHRO | Servicing Human Resource Office |
| SOP | Standard Operating Procedures |
| SOR | System of Records |
| SP | Special Publication |
| SSP | Shared Service Provider |
| USPTO | United States Patent and Trade Office |
| USVIS | United States Visit database |

## Appendix D—References

[1] HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004.

[2] NIST FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* NIST, February 25, 2005

[3] NIST Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, NIST, July 2005.

[4] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST, May 2004.

[5] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, NIST, February 2005.

[6] FICC, *Federal Identity Management Handbook* (draft), GSA, July 2005

[7] NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, NIST, February 2005.

[8] *Privacy Act of 1974*, U.S. Public Law 93-579, 1974.

[9] *E-Government Act of 2002*, U.S. Public Law 107-347, 2002.

[10] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB, September 26, 2003.