



## PIV Card Issuer Operations Plan

Version 1.0

August 1, 2007

CM # GSA-DI-0000129-1.4.0

## Revision Chart

---

Version	Primary Author(s)	Description of Version	Date Completed
0.1	Kevin Doty/Jim Galie	Initial Draft	07/20/07
0.2	Kevin Doty	Updated draft based on comments provided by GSA	07/23/07
0.3	Kevin Doty	Added section 4.0	07/25/07
0.4	Kevin Doty	Updated Initialization figures and wording; expanded renewal and reissuance into Section 2.5	7/26/07
0.5	Kevin Doty	Updated SP-800-79 pertinent controls info (Issuance, Renewal, Destruction, etc) and GSA/Agency role function comments	7/29/07

# Table of Contents

---

- 1.0 INTRODUCTION..... 1**
- 1.1 PURPOSE ..... 1
  - 1.1.1 *PCI Operations* ..... 1
  - 1.1.2 *PCI Operations for Certification and Accreditation* ..... 1
- 1.2 SCOPE..... 2
  - 1.2.1 *PCI Operations* ..... 2
  - 1.2.2 *PCI Operations for Certification and Accreditation* ..... 2
- 1.3 MSO BUSINESS STRATEGY OPERATIONS ..... 3
- 1.4 MSO ALIGNMENT WITH HSPD-12 CONTROL OBJECTIVES ..... 3
- 1.5 MSO ASSUMPTIONS AND CONSTRAINTS ..... 4
- 1.6 DOCUMENT ORGANIZATION ..... 5
- 1.7 PLAN MAINTENANCE ..... 5
- 2.0 PCI OPERATIONS ROLES, REQUIREMENTS AND PROCEDURES..... 6**
- 2.1 MSO SYSTEM LEVEL ROLE ADMINISTRATION..... 6
  - 2.1.1 *MSO System Level Role Requirements, Duties, and Interfaces*..... 8
    - 2.1.1.1 MSO System Role Administrator..... 8
    - 2.1.1.2 MSO System Security Officer ..... 10
    - 2.1.1.3 MSO System Facility Officer ..... 11
  - 2.1.2 *MSO Organizational Reporting Structure and Role Assignment Hierarchy*..... 12
- 2.2 AGENCY LEVEL ROLE ADMINISTRATION ..... 13
  - 2.2.1 *Agency Role Exclusivity Policy*..... 15
  - 2.2.2 *Agency Role Structure*..... 16
  - 2.2.3 *Agency with Sub-Agencies Structure* ..... 16
  - 2.2.4 *Agency Level Role Requirements, Duties, and Interfaces* ..... 17
    - 2.2.4.1 Agency Role Administrator..... 17
    - 2.2.4.2 Agency Security Officer Role ..... 19
    - 2.2.4.3 Agency Sponsor Role ..... 24
    - 2.2.4.4 Registrar Role ..... 29
    - 2.2.4.5 Agency Adjudicator Role ..... 33
    - 2.2.4.6 Issuance Process ..... 35
    - 2.2.4.7 Agency Activator Role ..... 37
    - 2.2.4.8 Applicant ..... 41
- 2.3 ROLE MANAGEMENT HIERARCHY ENFORCEMENT ..... 42
- 2.4 MSO AND AGENCY PROGRAM INITIALIZATION OPERATIONS ..... 44
  - 2.4.1 *MSO System-Specific Initialization*..... 44
  - 2.4.2 *Agency System-Specific Initialization* ..... 46
  - 2.4.3 *Enrolling Additional Agency Personnel* ..... 49
- 2.5 PIV CARD LIFECYCLE OPERATIONS ..... 49
  - 2.5.1 *Re-Issuance* ..... 49
  - 2.5.2 *Termination*..... 49

2.5.3	<i>PIV Card Renewal</i> .....	50
2.5.4	<i>PIV Card Certificate Renewal</i> .....	50
2.5.5	<i>PIV Card Destruction</i> .....	51
2.5.6	<i>PIV Card Holder Daily Usage Operations</i> .....	52
2.6	PRIVACY POLICY .....	53
2.7	BACKGROUND INVESTIGATION REQUIREMENTS.....	54
<b>3.0</b>	<b>PCI OPERATIONS CERTIFICATION AND ACCREDITATION</b> .....	<b>57</b>
3.1	INTRODUCTION.....	57
3.1.1	<i>Assessment / Methodologies</i> .....	58
3.1.2	<i>Status</i> .....	58
3.1.3	<i>References</i> .....	59
3.2	SP 800–79 ASSESSMENT REPORT .....	59
3.2.1	<i>Organization Description</i> .....	59
3.2.2	<i>Review, Analyze and Record Supporting Documents</i> .....	63
3.2.2.1	Defined Process and Policy Inventory.....	63
3.2.3	<i>PIV Sub-System Inventory</i> .....	65
3.2.3.1	PIV System Automated System Inventory .....	65
3.2.4	<i>Observed PCI Demonstration and Performed Interview</i> .....	66
3.2.5	<i>Process Flow Diagram</i> .....	68
3.2.6	<i>Perform SP 800-79 Attributes Assessment</i> .....	68
3.3	CERTIFICATION AND ACCREDITATION.....	72
3.3.1	<i>Initiation Phase</i> .....	72
3.3.2	<i>Certification Phase</i> .....	74
3.3.3	<i>Accreditation Phase</i> .....	75
3.4	C&A SUMMARY.....	78
<b>4.0</b>	<b>SUPPORTING DOCUMENTATION</b> .....	<b>79</b>
4.1	PIV IMPLEMENTATION GUIDANCE .....	79
4.1.1	<i>Introduction</i> .....	79
4.1.2	<i>Card Production</i> .....	79
4.1.2.1	Process Overview .....	79
4.1.2.2	Actors.....	79
4.1.2.3	Process Description .....	80
4.1.3	<i>Expiration Date Requirements</i> .....	80
4.1.4	<i>Audits and Records Management</i> .....	80
4.1.5	<i>Reporting Requirements</i> .....	80
4.2	TRAINING .....	81
4.2.1	<i>Training Sources</i> .....	81
4.2.2	<i>Instructor-Led Training</i> .....	81
4.2.3	<i>Virtual Classroom/Web Seminar Training</i> .....	82
4.2.4	<i>Web-based Training</i> .....	82
4.2.5	<i>Learners Roles and Responsibilities</i> .....	83
4.3	GSA TECHNICAL REQUIREMENTS FOR MANAGING ROLES .....	85

**APPENDIX A – TERMS AND ACRONYMS..... 96**

**APPENDIX B – DEFINITIONS..... 98**

**APPENDIX C – MSO APPROVED IDENTITY DOCUMENTS GUIDE..... 100**

**APPENDIX D – OMB MEMO M-05-24..... 102**

**APPENDIX E – PIV CARD USAGE PRIVACY ACT NOTICE ..... 104**

**APPENDIX F – BACKGROUND INVESTIGATION SCHEDULING..... 106**

**APPENDIX G – APPEAL RIGHTS FOR DENIAL OF A CREDENTIAL ..... 107**

## List of Figures

---

Figure 2-1: MSO Roles Governing Agencies.....	7
Figure 2-2: MSO Top Level Organization.....	13
Figure 2-3: Agency without Sub-Agencies Structure.....	16
Figure 2-4: Agency With Sub-Agency PIV Roles.....	17
Figure 2-5: Suspend PIV Card Process Diagram.....	22
Figure 2-6: Revoke and Destroy PIV Card Process Diagram.....	23
Figure 2-7: Reactivate PIV Card Process Diagram .....	24
Figure 2-8: Sponsorship Process Diagram.....	26
Figure 2-9: Update Applicant Sponsorship Information Process Diagram .....	27
Figure 2-10: Request PIV Card Re-issuance or Reprint Process Diagram.....	28
Figure 2-11: Enrollment Process Diagram .....	32
Figure 2-12: Adjudicator Process Diagram .....	35
Figure 2-13: Issuance Process Diagram.....	37
Figure 2-14: Attended Activation Process Diagram.....	40
Figure 2-15: Unattended Activation Process Diagram .....	41
Figure 2-16: MSO System Initialization.....	45
Figure 2-17: Identifying Key Agency Personnel .....	47
Figure 2-18: Creating the Initial Agency Role Environment.....	48
Figure 3-1: MSO PCI Process Flow Diagram .....	68

## List of Tables

---

Table 2-1: MSO Role Descriptions.....	6
Table 2-2: Agency Role Definitions within the MSO PIV Process.....	14
Table 2-3: Enrollment Tasks.....	29
Table 2-4: PCI Role Management Hierarchy Enforcement.....	42
Table 3-1: PIV Role Name and Personnel.....	59
Table 3-2: MSO PIV Roles Contact Information .....	62
Table 3-3: Process and Policy Inventory .....	63
Table 3-4: Document Inventory .....	64
Table 3-5: PIV Project System Inventory .....	65
Table 3-6: Automated System Inventory .....	65
Table 3-7: PIV Card Enrollment Process.....	66
Table 3-8: PCI 800-79 Required Attributes.....	69
Table 3-9: PCI-79 Desirable Attributes .....	71
Table 4-1: WBT Working Titles.....	83
Table 4-2: WBT Roles and Responsibilities.....	84
Table 4-3: Implementing Technical Requirements for Managing Roles.....	85

# 1.0 INTRODUCTION

---

Homeland Security Presidential Directive 12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors,” established the requirement for a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. As a result, the National Institute of Standards and Technology (NIST) released “Federal Information Processing Standard (FIPS) 201: Personal Identity Verification (PIV) of Federal Employees and Contractors” on February 25, 2005. FIPS establishes the technical requirements and business processes for the development of PIV contact/contact-less smart cards.

The USAccess Program, powered by the EDS Assured Identity™ solution, provides a managed service to produce compliant PIV credentials and to maintain associated identity accounts. The USAccess mission under the U.S. General Services Administration (GSA) HSPD-12 Shared Services Provider II contract is to serve as the executive Agent for government-wide acquisition of information technology to implement HSPD-12. That mission includes the effort to provide 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.

## 1.1 Purpose

### 1.1.1 PCI Operations

The primary purpose of this PIV Card Issuer (PCI) Operations Plan is to describe the operations and procedures at the MSO and Agency levels, including the assignment of PIV roles and responsibilities. It is important to understand the overall PCI operations and workflows, beginning with Applicant sponsorship by an approved authority, and Applicant participation in the identity proofing and registration process to create the record of demographic and biometric information in the MSO Identity Management System (IDMS). Following favorable background investigation and adjudication results, the PCI operations result in the Applicant’s receipt and activation of the PIV Card for authorized daily usage.

### 1.1.2 PCI Operations for Certification and Accreditation

The secondary purpose of this document is to provide the GSA Certification Agent with sufficient PCI operations information to make a PIV Certification and Accreditation (C&A) decision. The GSA C&A team uses this PCI Operations Plan as input for establishing the reliability of the MSO component organization and operation with regard to the PIV technical and business requirements in FIPS 201-1, and the C&A requirements in NIST 800-79,

“Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations”, National Institute of Science and Technology (NIST) July 2005.

## 1.2 Scope

### 1.2.1 PCI Operations

This PCI Operations Plan covers MSO and all Shared Services Agency employees, contractors, affiliates, and volunteers who require long-term, routine access to federal facilities, systems, and networks. The personal information to be collected in the enrollment process will consist of data elements necessary to verify the identity of the individual, and to perform background check or other investigations.

This document describes the overall PCI operations, including roles and responsibilities and hierarchical controls governing assignment of those roles, and the workflow processes performed by PIV personnel in these roles.

There are three core sets of GSA Shared Services user role populations:

1. Users with administrative and operational responsibilities.
2. Trusted agents of the MSO solution, both at the Agency and MSO level, as applicable, e.g., Sponsor, Adjudicator, Registrar, Activator, Security Officer, and Role Administrator.
3. MSO Applicants.

The functions and relationships within core populations (2) and (3) are discussed with respect to PCI Operations and role assignment duties, while core population (1) is discussed in the C&A portion of this document as part of the operations C&A verification.

### 1.2.2 PCI Operations for Certification and Accreditation

In order to confirm the reliability of the PCI operations required for C&A verification, this PCI Operations Plan reviews the following:

- The specific requirements for issuing PIV Cards
- The processes in place or planned for meeting the PIV Card requirements
- The supporting materials and identify management related documents
- The PIV Card Issuer’s privacy policy for Applicants
- Descriptions of management procedures for assuring continued reliable operations
- All agreements with agencies regarding the use of the PIV Card Issuer services
- The certification agent findings and recommendations summary

## 1.3 MSO Business Strategy Operations

The HSPD-12 mandate reinforced the vetting requirements for government employees, contractors and affiliates, and it also mandated the development of a secure infrastructure that supports a secure smart token with embedded identity information. The investment to build, maintain, and operate this new capability was recognized to be substantial; and in many cases, too expensive for smaller agencies and business units of the government to afford or operate alone. The reality of that investment propelled the concept of a Shared Services that would federate many government agencies under a single credential provider to the forefront. The U.S. General Services Administration (GSA) sponsored Managed Services Office (MSO) (herein after GSA MSO is referred to as MSO) has joined together over multiple agencies and commissions, and more than 550,000 resulting identities under a single credentialing umbrella at the inception of the program.

The MSO is the only pure federated system serving multiple agencies, and has a tiered structure that consists of:

1. The MSO for system operations, security, and credential deliver.
2. Agency Leads who assign responsible parties to operate and administrate the identities of their respective employees.

The MSO has developed supporting material which describes management procedures for assuring continued reliable operations, to include Privacy Policies, MSO Contingency Plan, and all necessary agreements with agencies regarding using the services of the PCI, to include Interconnection Service Agreements (ISAs) and Inter-Agency Agreements (IAAs). Responsibility for Privacy Policies is assigned to the Agency Privacy Officers.

## 1.4 MSO Alignment with HSPD-12 Control Objectives

The HSPD-12 directive identified several control objectives for achieving secure and reliable identification, and these objectives are:

- 1. The identification is issued based on sound criteria for verifying the Applicant's identity.**

The MSO has implemented an approved, controlled and reliable process for verifying the Applicant's identity (see Appendix C for a list of MSO approved identity documents). This model is based upon using the identity assets of agencies and organizations participating in the MSO Shared Services, who are best aware of the affiliation of their employees and contractors, and implementation of FIPS 201-1 into a role-based/separation of duties system that technically embeds an identity aboard an approved FIPS 201-1 credential. Business rules such as sponsorship and adjudication remain within the Agency and abide by the same Agency specific business rules in terms of suitability and privacy protection. The MSO acts as an electronic conduit with the individual agencies retaining control of the fingerprint process to include adjudication and suitability. Implementation of the Federal Identity Credentialing Committee (FICC)

standard for automated transfer of identity information from an Agency system of records to the MSO operated identity store.

**2. The identification is strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation.**

Separating the Enrollment Officer/Registrar from the organization that provides the PIV Cards (i.e., Centralized Printing Services) is a strong deterrent to fraud, abuse, and identity theft. Use of card topology security features to raise the bar in terms of visual recognition of the credential and to reduce the ease of counterfeiting. Examples of this are the use of Optically Variable Ink (OVI) of the Great Seal of the United States embedded in the center of the card, as well as micro-printing as an effective deterrent to photocopying, or attempts to use inexpensive card printers to fraudulently reproduce the credential.

**3. The identification can be rapidly authenticated electronically.**

PKI digital certificates (encoded on the PIV Card via the MSOs Card Management System (CMS) and federally approved Federal PKI SSPs) allows access to credential services and the management of those credentials. The capability to do a ‘positive check’ of an identity within the MSO identity system, via a proposed government standard for authentication, sponsored by the Federal Identity Credentialing Committee (FICC), while still in the process of definition.

**4. The identification is issued by providers whose reliability has been established by an official accreditation process.**

The GSA PIV System is currently undergoing the C&A process. Additionally, this process will provide the basis and sufficient evidence for the GSA Designated Approval Authority (DAA) to officially accredit the PCI process.

## 1.5 MSO Assumptions and Constraints

The PIV initiative is focused on implementing and ensuring a consistent and reliable registration and issuance process, and includes the background investigation process. The PIV process is focused on implementation of the FIPS 201-1 standard, with the goal to have interoperable an ID that can be easily recognized and used for access to both physical and logical assets within subscribing agencies.

Per HSPD-12, FIPS 201-1, and OMB Memorandum 05-24, provided in Appendix D, all Agencies must create and begin implementation on a PIV-II-compliant system for new employees and contractors beginning no later than October 27, 2006. GSA accomplished this task under an initial vendor contract and met the October 27<sup>th</sup> 2006 deadline. Subsequently, a decision to re-compete the contract to obtain wider service offerings and better pricing options was made with a follow-on contract award on 23 April 2007. An updated implementation plan was provided to OMB based upon this action. The MSO will work to meet the dates specified by OMB with a goal of credentialing all MSO Agency personnel by October 27<sup>th</sup>, 2008.

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

## 1.6 Document Organization

The remainder of this document is organized in two interdependent parts:

**Section 2.0:** Provides a detailed description of the overall MSO operations, to include PCI roles, technical requirements, duties, PCI organization initialization steps, and the process workflows for the individual PIV operations. These descriptions are provided at both the MSO and Agency levels, and explain the interaction between both entities and their personnel in order to initialize, launch, and maintain daily PCI operations.

**Section 3.0:** In accordance with documented NIST SP 800-79 requirements, this section provides verification of all PCI operations that are required to attain and maintain C&A status for the MSO Authority to Operate (ATO).

**Section 4.0:** Provides supporting documentation and technical information related to FIPS 201-1 compliant MSO Operations.

## 1.7 Plan Maintenance

The PCI Manager develops and maintains the PCI Operations Plan. This Plan falls under Configuration Management (CM) as outlined in the CM Plan. This document has been reviewed against NIST Special Publications, Government security documents and other client specific security documents, and is commensurate with those requirements. This document is periodically reviewed by responsible parties within the USAccess organization and updated as necessary.

## 2.0 PCI Operations Roles, Requirements and Procedures

The MSO ensures that the mandatory hierarchical system structure is enforced in the overall management operations for Role Administration. Adhering to this structure allows the system to effectively manage the administrative responsibilities for MSO system and Agency level roles in the areas of role assignment, role membership, and other administrative policies and procedures, as defined in the technical requirements.

The PIV process for issuing and activating an Applicant’s PIV Card contains critical administrative roles and responsibilities such as Sponsors, Registrar, Adjudicator, Issuance, Activator, and Security Officer. The following subsections describe these roles in detail as they pertain to the MSO System Level Role Administration and the Agency Level Role Administration.

Training and certification are required for the Sponsor, Registrar, Adjudicator, Activator, Security Officer and Role Administrator roles. More information regarding training can be found in the USAccess Training Plan.

### 2.1 MSO System Level Role Administration

The MSO is responsible for starting, administrating, and auditing the PIV chain-of-trust for the entire federation of Agency customers and meeting FIPS 201-1 requirements.

To facilitate the structure the MSO has administrative supervision over the system that is embedded in a few select roles. Some of these roles are only in operation at specific times (i.e., MSO System Role Administrator to aid in startup and adding an Agency) and some of the roles are maintained as normal operation (i.e., the MSO System Security Officer and MSO Facility Manager). These roles are described in Table 2-1: MSO Role Descriptions.

**Table 2-1: MSO Role Descriptions**

Role	Description
MSO System Role Administrator	The GSA designated individual responsible for assigning the initial Agency primary roles in the USAccess System. The MSO Role Administrator creates the initial accounts for the Agency Role Administrator, Sponsor, and Adjudicator per the role management policies described in Section 2.4.2. After the initial creation of the PIV roles only the Agency Role Administrator will continue to be managed by the MSO Role Administrator. The Agency Role Administrator will be responsible for managing the PIV roles.
MSO System Security Officer	The GSA designated individual responsible for overall security of the system and for managing audit reporting and specific issues relating to security. The MSO Security Officer shall have a minimum of a TOP SECRET Clearance and will be the single point of contact for security issues across the MSO.

Role	Description
MSO Facility Manager	The GSA designated individual responsible managing all the facilities and who administrates the selections and verifies the training of all Registrars. This is a management oversight role to assist with routine operations.

An example of the MSO role structure which oversees Agency role administration is shown in Figure 2-1: MSO Roles Governing Agencies and includes an example of an Agency, in this case the Department of Commerce, providing role administration over its sub-agencies. For simplicity, the Agency level Activator role is not depicted in Figure 2-1.

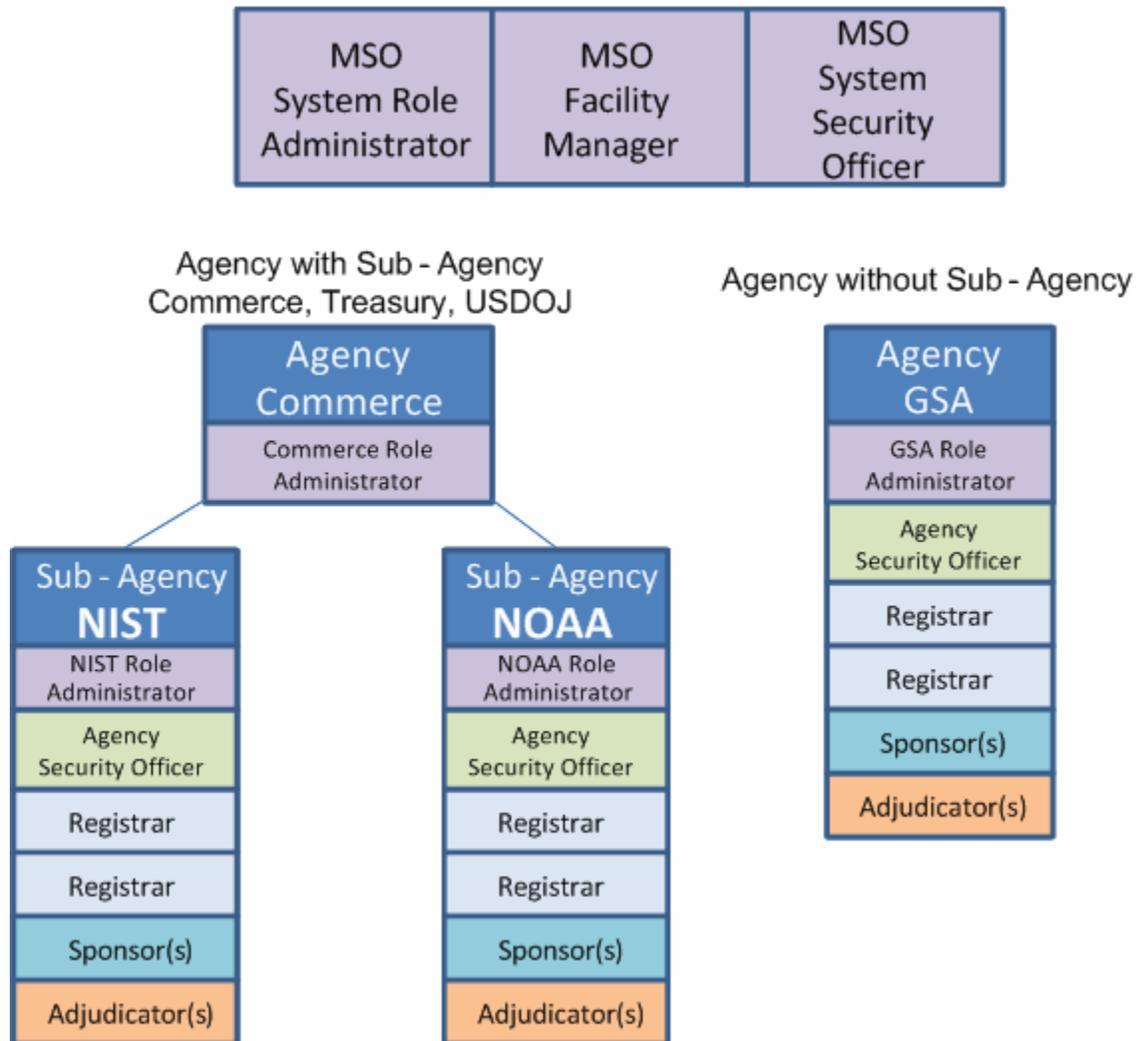


Figure 2-1: MSO Roles Governing Agencies

## 2.1.1 MSO System Level Role Requirements, Duties, and Interfaces

The MSO credentialing organization consists of the MSO employees who manage the system and have roles that provide service across the entire Shared Services federation. As an Agency is brought into the Shared Services, the MSO manages the Agency configuration (unique topology and data concerns); it validates the initial Agency roles and provides the vehicle for these personnel to receive their training, role assignments, and initial cards; and it manages any unique Agency data requirements that may interface to the shared service. Each role described in this section affects the integrity and security objectives of HSPD-12 with regard to issuance of a PIV Card. The roles listed below are the hierarchy that would exist within an Agency structure as a customer of the MSO. This section describes the three major roles that the MSO uses in administration, startup, and maintenance of the PIV issuance infrastructure.

### 2.1.1.1 MSO System Role Administrator

The MSO designated individual is responsible for managing the initial Agency Sponsor, Adjudicator, Registrar, Security Officer, and Activator roles to commence administration of a chain-of-trust. The scope of the MSO Role Administrator is verifying and loading the initial Agency roles and personnel as required and in administration of a change in the Agency Role Administrator during system operation. Once a customer has a satisfactory structure in place for administrating their own organization, the MSO Role Administrators relinquish their duties to the customer organization. The MSO shall have two MSO System Role Administrators assigned at a minimum to ensure dual control and oversight of system loading.

The MSO System Role Administrators are GSA designated officials that will be allowed to sponsor and adjudicate a limited number of the following Agency roles, and are responsible for creating the following initial accounts for the subscribing Agency:

- Agency Role Administrator
- Agency Sponsor
- Agency Adjudicator
- Registrar
- Security Officer
- Agency Activator

It is the responsibility of the MSO Role Administrator that all account assignment requests shall be documented and signed for auditing purposes and certified that the appropriate training and identity proofing has been completed on the individual.

#### **2.1.1.1.1 MSO System Role Administrator Requirements**

- Be designated in writing by a senior level Agency official (need designation letter)
- Load and administrate the initial Agency roles when an Agency joins the MSO
- Shall receive training and be certified via the MSO PIV Training Program
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of Agency/Commission structure, including populations and missions of Agency sites as well as MSO operating rules and requirements
- Be familiar with PKI, the PIV issuance process, and the Service/Agency's Sponsor/Role process
- Have not been convicted of a felony offense
- Have had, as a minimum, a suitable NACI background investigation performed.
- Have not knowingly been denied a security clearance or had a security clearance revoked

#### **2.1.1.1.2 MSO System Role Administrator System Interfaces**

- Web interface with work queue for roles
- System allows privilege grant, privilege revoke

#### **2.1.1.1.3 MSO System Role Administrator Other Possible System Roles**

- MSO Security Officer

#### **2.1.1.1.4 MSO System Role Administrator Duties**

- Adjudicate separation of roles within the Agency
- Approves privileges for new role holders, verifying separation of duties and training
- Ability to revoke role privileges for Agency Role Administrators
- Helps onboard new roles from other agencies

### **2.1.1.2 MSO System Security Officer**

The MSO System Security Officer can suspend or terminate an Applicant's PIV Card. In addition, the Security Officer is responsible for validating MSO operations and has access to run reports and view system audit logs.

#### **2.1.1.2.1 MSO System Security Officer Requirements**

- Be designated by a senior official responsible for the MSO
- Shall receive training and be certified as Security Officer with a Top Secret Clearance
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of Agency/Commission structure, including populations and missions of Agency sites as well as MSO operations and Agency interfaces
- Be familiar with PKI, the PIV issuance process, and the Service/Agency's Sponsor/Role process

#### **2.1.1.2.2 MSO System Security Officer System Interfaces**

- Processes require web interface, PIV Cards and digital signature
- Allows suspend card, revoke card, reinstate card, card destroyed notice, audit trail reporting
- Training must be received

#### **2.1.1.2.3 MSO System Security Officer Other Possible System Roles**

- MSO Role Administrator

#### **2.1.1.2.4 MSO System Security Officer Duties**

- Audit and report capabilities for monitoring Shared Services activities within the respective Agency
- PIV Card suspension/reactivation/and revocation capabilities. The MSO Security Officer shall not administrate any credential action except in extreme circumstances or in the event of an emergency. However, the MSO Security Officer is the only official who can

process an emergency revocation notification, as necessary. In general, the Agency Security Officer shall be the primary means of managing their own employees.

- Audit physical revocation and destruction of PIV Card at termination of Cardholder employment
- Act as an interface for the USAccess System and MSO for any inquiries on specific identity issues as they relate to law enforcement activities. If a security breach is discovered, the MSO Security Officer is required to notify the MSO Program Manager and law enforcement personnel within 45 minutes of its discovery. All activities shall be coordinated with the affected Agency.

### **2.1.1.3 MSO System Facility Officer**

The MSO System Facility Officer role is defined as an MSO management agent to provide PIV operations oversight. It is the responsibility of this MSO agent to provide guidance to enrollment facilities to establish and maintain enrollment station requirements, ensure that Registrars are trained and certified, and to manage the Registrar operations from a management-only perspective.

#### **2.1.1.3.1 MSO System Facility Officer Requirements**

- Be designated by a senior official responsible for the MSO
- Shall receive training as a registrar and be familiar with registrar operations
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of Agency/Commission structure, including populations and missions of Agency sites as well as MSO operations and Agency interfaces
- Be familiar with PKI, the PIV issuance process, and the Service/Agency's Sponsor/Role process
- Have not been convicted of a felony offense
- Have had, as a minimum, a NACI background investigation performed
- Have not knowingly been denied a security clearance or had a security clearance revoked

### **2.1.1.3.2 MSO System Facility Officer System Interfaces**

- None

### **2.1.1.3.3 MSO System Facility Officer Other Possible System Roles**

- None

### **2.1.1.3.4 MSO System Facility Officer Duties**

- Manages the location of enrollment assets via meetings with customer agencies
- Verifies Registrar assignments
- Ensures that Registrars are properly trained and monitors their training status
- Monitors the usage of enrollment assets to ensure access by members of the MSO customer agencies

## **2.1.2 MSO Organizational Reporting Structure and Role Assignment Hierarchy**

Agency representatives assume responsibility for the process within their organization upon the assignment of an Agency Role Administrator, and subsequent role assignments, as will be explained later in this document, to commence operations.

The MSO Security Officer is a system specific role that is not defined in FIPS 201-1. It is the only role in the MSO organization that has the ability to access all identities within the MSO identity store for all agencies. This individual has Security Officer counterparts in respective agencies or sub-agencies; but this MSO level role has access to all data on the system for revocation and credential management. This assignment requires a minimum of a Top Secret Clearance. Note, although the Security Officer (MSO and Agency level) can manage identities, he/she cannot create, sponsor, enroll, activate, or adjudicate, and therefore maintains the separation of duties required within FIPS 201-1.

An additional role that is unique to the MSO is the role played by the MSO Facility PCI Manager. This MSO role manages the deployment of enrollment assets across multiple members of the Shared Services Federation. Additionally, because of the importance of the Registrar and their training requirements, all Registrar functions shall be approved by the MSO. This includes MSO contracted assets, government employees, or contractor assets provided by shareholder agencies.

Once the individual agencies have been established, the MSO organization can manage the Agency functions and ongoing role oversight and assignments, including management of Agency Role Administrators. Figure 2-1: MSO Roles Governing Agencies presents the top level organizational diagram for this structure showing that Registrars report to the MSO Registrar, as depicted by the arrowed lines, while the span of Security Officer access control is shown by the dashed circles. However, the MSO Security Officer has access to all identity accounts in the

USAccess System. Individual agency and sub-agency Security Officers may only see personnel within their own organizational business unit.

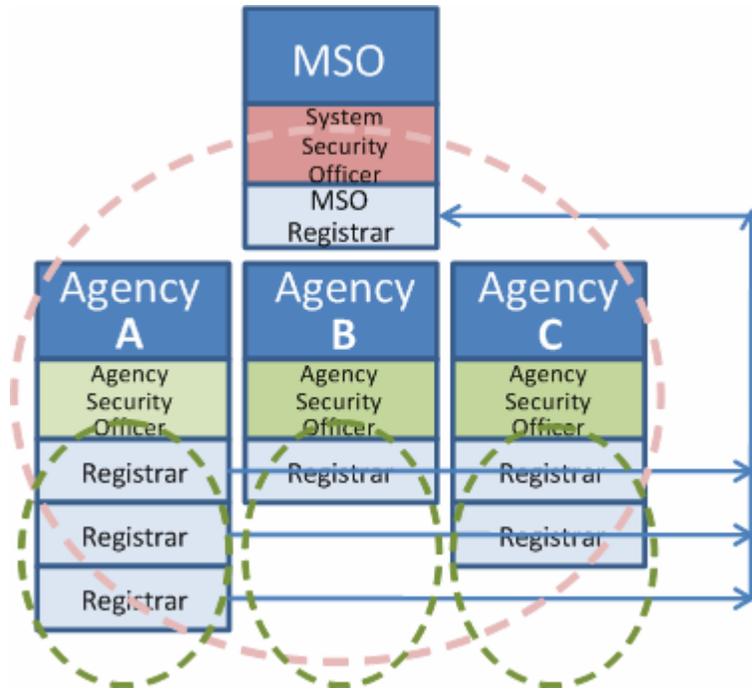


Figure 2-2: MSO Top Level Organization

## 2.2 Agency Level Role Administration

The agency level roles are defined for organizations that are MSO customers. Each role described later in this section affects the integrity and security objectives of HSPD-12 with regard to issuance of a PIV Card. The roles listed in *Process* are the hierarchy that would exist within an Agency structure as a customer of the MSO. Additional supervisory roles exist within both the MSO and systems operations. These roles shall be defined in separate sections to emphasize their supervisory role. However, within the MSO customer base, there are multiple business approaches across agencies as well as service structures within agencies that support varied business approaches such as:

- Government Owned/Contractor Operated (GOCO) laboratories with minimal government sponsorship.
- Contracted services for human resources or adjudication within an Agency and between Agencies, such as Human Resource Lines-of-Business (HR-LOB).
- Large agencies with dedicated personnel with defined functions that map to the requirements of FIPS 201-1 as well as very small Agencies and Commissions who have few personnel to accomplish the range of duties in the IPS process.

The MSO system is based upon the strength of a single person who is designated as a senior official for the personnel who receive identity cards in the FIPS process. This individual at the Agency level is the Agency Role Administrator, and should make every attempt to separate roles and duties within the system to ensure that ‘no single individual’ may bypass the requirements of FIPS 201-1 and commit fraud to issue a credential.

To that end, there will always be separation between the Agency Role Administrator, the Agency Security Officer, and the Registrar to meet the separation of roles required by FIPS 201-1. The Agency Role Administrator shall attempt to have separate individuals perform each of the duties as defined in Table 2-2. However, combination of roles is permitted by Agency Role Administrators in the performance of PIV Sponsorship and Adjudication.

All system access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Separation of duties means the delegation of authority in a manner that spreads responsibility among people and creates checks and balances for those who have the authority to make changes, additions, and modifications. “Least privilege” means giving Shared Services Solution users access to only the minimal information required to perform their job functions (it also applies to the ability to add, modify, or delete data).

Each role assignment requires approval by Agency Role Administrator at the individual level. That means the Agency Role Administrator cannot approve individual roles for the entire Human Resources (HR) office as a sweeping approval. Each individual has to be approved. This also means that the Agency Role Administrator can approve every individual in the HR office through this process and when a new individual is assigned to the HR office, that new individual need to be approved by the Agency Role Administrator. Any overlap will require the Role Administrator to document their justification and approval for having combination of roles.

**Table 2-2: Agency Role Definitions within the MSO PIV Process**

Role	Description
Agency Role Administrator	The Agency designated individual responsible for managing the Agency’s Sponsor, Adjudicator, Registrar (if applicable), and Activator roles. The scope of the Agency Role Administrator is bound to the Agency configuration in the managed service system. The Agency Role Administrator will verify that the appropriate separation of duties are followed and will verify that all training certification requirements have been met.
Agency Security Officer	The Security Officer can suspend or terminate an Applicant’s PIV Card. In addition, the Security Officer is responsible for validating identity documents in question and authorizing the process to continue. The Security Officer has the ability to run reports and view system audit logs. The Security Officer may not fill any other role within the organizational unit.

Role	Description
Agency Sponsor	The individual who substantiates the need for a PIV Card to be issued to the Applicant. (Once the Applicant has been issued a PIV Card the Applicant is referred to as the PIV Cardholder.) The Sponsor is also the individual responsible for entering the Applicants' primary biographic information as well as required sponsorship data elements. The Sponsor remains aware of the Applicant's status and associated continuing need for holding a PIV Card. The Sponsor is responsible for managing the employment status of the PIV Cardholder in the managed service system through a web interface when a PIV Cardholder retires, terminates, or for another reason no longer requires a PIV Card. The Sponsor can make corrections or changes to an Applicant/Cardholders primary biographic information in the system.
Agency Adjudicator	The individual who is authorized to record the adjudication result for an Applicant. The Adjudicator enters or updates the status of adjudication result for all Applicants through a web enabled interface in the managed service system. A positive adjudication result will initiate the PIV Card issuance process.
Registrar	The individual responsible for identity proofing the Applicant and collecting biographic information, a photo, and fingerprints. This role does not specifically contain the title "AGENCY". Registrars may be provided by the MSO, may be a government employee of an Agency, or may be a contract employee of an Agency. All Registrars are controlled and supervised by the MSO in terms of their qualifications and ability to act in this role. The Registrar confirms that the individual present at time of enrollment is sponsored, inspects two identity source documents, see Appendix C, in original form and scans the documents into the system. The Registrar then captures the Applicant's photo and captures both flat and rolled images of all ten of the Applicant's fingerprints. The photo and fingerprints are captured in accordance with FIPS 201-1 specifications. The system automatically generates a primary and secondary biometric minutia template, which is verified by the Applicant. The enrollment package is digitally signed and saved into the IDMS using certificates from the Registrar's PIV Card. The Registrar cannot make changes to a completed enrollment record without authorization from a Sponsor to re-enroll.
Agency Activator	The individual responsible for processing PIV Card activations. The Activator verifies that the Applicant is the person to whom the PIV Card is to be issued and guides the Applicant through the activation process.
Applicant	The individual who has a need for a federal credential under the requirements of FIPS 201-1. The Applicant is responsible for providing proper identity information at sponsorship and enrollment and for expeditiously performing the PIV process of enrollment and activation. Applicants shall surrender their credentials when they are no longer eligible in accordance with local Agency policy.

### 2.2.1 Agency Role Exclusivity Policy

In general, the MSO role policy does not allow for more than one role to be assumed and performed by a single person from an agency. However, there are exceptions which shall be authorized by the Agency role Administrator. Unlike other agency roles which are exclusive roles, the Registrar may also perform a secondary role as Activator, at the discretion of the Agency, with a documented chain of approval.

All role assignments require approval by Agency Role Administrator at the individual level. The policy requires a fully documented approval process authorized by the Agency Security Officer

per individual. In addition, the Agency Security Officer defines the policies for role assignments, also allowing another role exception, with the combination of Sponsor and Adjudicator as necessary.

### 2.2.2 Agency Role Structure

The Agency role structure for medium to small agencies that perform their own HR and adjudication functions is shown in Figure 2-3: Agency without Sub-Agencies Structure. For billing purposes, this unit is treated as a specific billable unit. A single Agency Role Administrator manages the subordinate roles and the security structure as shown (GSA is used as an example). For simplicity, the Agency level Activator role is not depicted in Figure 2-3.

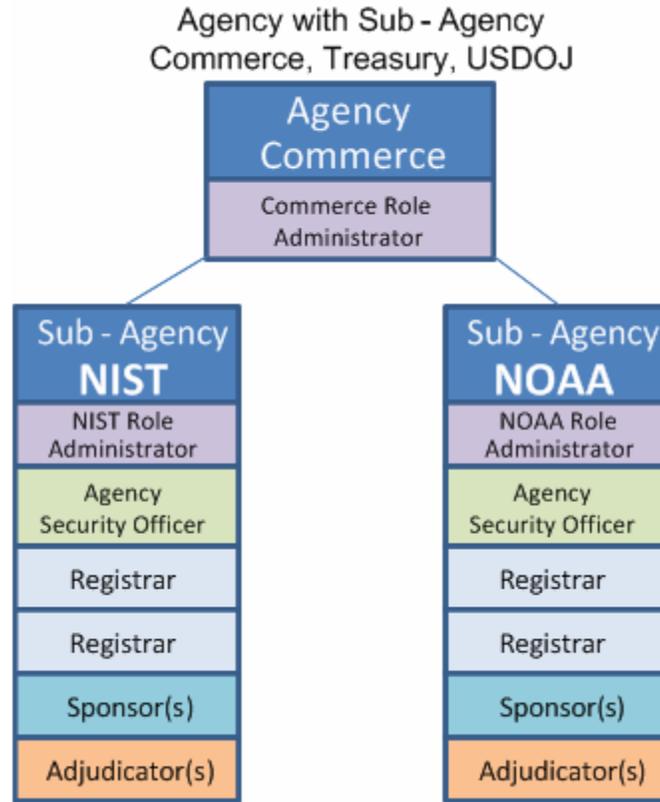
Agency without Sub - Agency



Figure 2-3: Agency without Sub-Agencies Structure

### 2.2.3 Agency with Sub-Agencies Structure

This Agency structure is recommended for large diverse organizations that have multiple operating units that act as independent units and that may have separate billing structures. This structure may be used with multiple billing and administrative units to maintain separation of roles. It is aligned to existing HR and billing systems, and it ensures that Applicants are as closely aligned to their Sponsors as possible. Note that the MSO will only manage the Agency-role structure to two levels (Agency and Sub-Agency) in order to maintain an efficient billing and administrative structure. Figure 2-4: Agency With Sub-Agency PIV Roles shows the structure of a large Agency with multiple independent operating units (Commerce is used as an example). For simplicity, the Agency level Activator role is not depicted in Figure 2-4.



**Figure 2-4: Agency With Sub-Agency PIV Roles**

The following subsections will detail each Agency role with an overview of the role and a list of the requirements, system interfaces, and duties.

## 2.2.4 Agency Level Role Requirements, Duties, and Interfaces

### 2.2.4.1 Agency Role Administrator

The Agency designated individual responsible for managing the Agency’s Sponsor, Adjudicator, Registrar (unless MSO managed), Security Officer and Activator roles. The scope of the Agency Role Administrator is bound to the Agency configuration in the managed service system. The Agency Role Administrator will verify that the appropriate separation of duties are followed and will verify that all training certification requirements have been met.

Each Agency shall designate a primary and secondary Agency Role Administrator. The Agency Role Administrator will be allowed to assign PIV roles for his/her own Agency, following the MSO initial Agency account assignments for Sponsor, Adjudicator, Security Officer, and Registrar. The following additional PIV roles can then be assigned and managed by the Agency Role Administrator:

- Sponsor
- Registrar

- Adjudicator
- Activator
- Security Officer

The Agency Role Administrator will not be allowed to sponsor, enroll, adjudicate, and/or activate PIV Cards for Applicants. This role is an account assignment only role, preventing the ability to both assign and perform the roles, adhering to the separation of duties requirement.

**2.2.4.1.1 Agency Role Administrator Requirements**

- Be designated in writing by a senior level Agency official (need designation letter)
- Designate the Sponsors across his/her organization
- Designate his/her organization’s Security Officer who shall have access to Personally Identifiable Information (PII) of all the Organization’s enrollees
- Designate the Adjudicators across his/her organization
- Shall receive training and be certified via the MSO PIV Training Program
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of Agency/Commission structure, including populations and missions of Agency sites
- Be familiar with PKI, the PIV issuance process, and the Service/Agency’s Sponsor/Role process
- Have not been convicted of a felony offense
- Have had as a minimum, a NACI background investigation performed
- Have not knowingly been denied a security clearance or had a security clearance revoked

**2.2.4.1.2 Agency Role Administrator System Interfaces**

- Web interface with work queue for role assignments
- System allows privilege grant, privilege revoke

### **2.2.4.1.3 Agency Role Administrator Other Possible System Roles**

- None

### **2.2.4.1.4 Agency Role Administrator Duties**

- Adjudicate separation of roles within the Agency
- Approves privileges for new role holders, verifying separation of duties and training
- Ability to revoke role privileges for users within the Agency

### **2.2.4.2 Agency Security Officer Role**

It is noted that there are two levels of security officers: Agency Security Officers and MSO System Security Officers. Agency Security Officers, discussed here, can only access records for his/her designated Agency, while only System Security Officers can access all records across all agencies. However, Agency Security Officers shall have access to System logs relevant to activities specific to their Agency.

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.

At least one Security Officer should be designated by each Agency participating in the MSO. This person is responsible for the suspension and/or revocation of PIV Cards and/or PIV certificates loaded onto the cards that result from personnel-related reasons. These reasons may include temporary suspension from work-related duties, maternity/paternity leave, leave of absence, resignation, and retirement, among other personnel situations. The Security Officer should also investigate any potential identity impersonation events.

In addition, the Security Officer is responsible for validating identity documents in question and authorizing the process to continue. The Security Officer has access to run reports and view system audit logs. The Security Officer is the designated role with access to the bulk upload capability.

#### **2.2.4.2.1 Agency Security Officer Requirements**

- Be designated by the Agency Role Administrator
- Shall receive training and be certified as Security Officer
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder

- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of Agency/Commission structure, including populations and missions of Agency sites
- Be familiar with PKI, the PIV issuance process
- Have not been convicted of a felony offense
- Have had as a minimum, a NACI background investigation performed
- Have not knowingly been denied a security clearance or had a security clearance revoked

#### **2.2.4.2.2 Agency Security Officer System Interfaces**

- Processes require web interface, PIV Cards and digital signature
- Administrates and signs for bulk upload requests
- Allows PIV Card suspension, revocation, reinstatement, card destruction notice, audit trail reporting
- Training must be received

#### **2.2.4.2.3 Agency Security Officer Other Possible System Roles**

- None

#### **2.2.4.2.4 Agency Security Officer Duties**

- A Security Officer has multiple duties within the system, and they include:
- Auditing and reporting capabilities for monitoring Shared Services activities within the respective Agency
- Audit physical revocation and destruction of PIV Card at termination of Cardholder employment
- Liaison for Agency inquiries on specific identity issues related to law enforcement activities. If a security breach is discovered, the Security Officer is required to notify the Role Administrator and the MSO Security Officer.
- Batch import new Applicants
- Suspend a PIV Card for security related threats
- Terminate a PIV Card for security related threats
- Revoke and destroy PIV Cards from terminated Cardholders
- Reactivate a PIV Card
- Document that a PIV Card was destroyed

- Log a security event
- Provide audit logs to designated government representatives on-demand
- Resolve issues/invalidate enrollments involving fraudulent source documents or variables
- Allow enrollment of previously enrolled applicant if deemed necessary
- Approve/Disapprove activation continuance
- Approve/Disapprove rollback
- Determine specifics of file modification event

2.2.4.2.5 Security Officer Process Diagrams

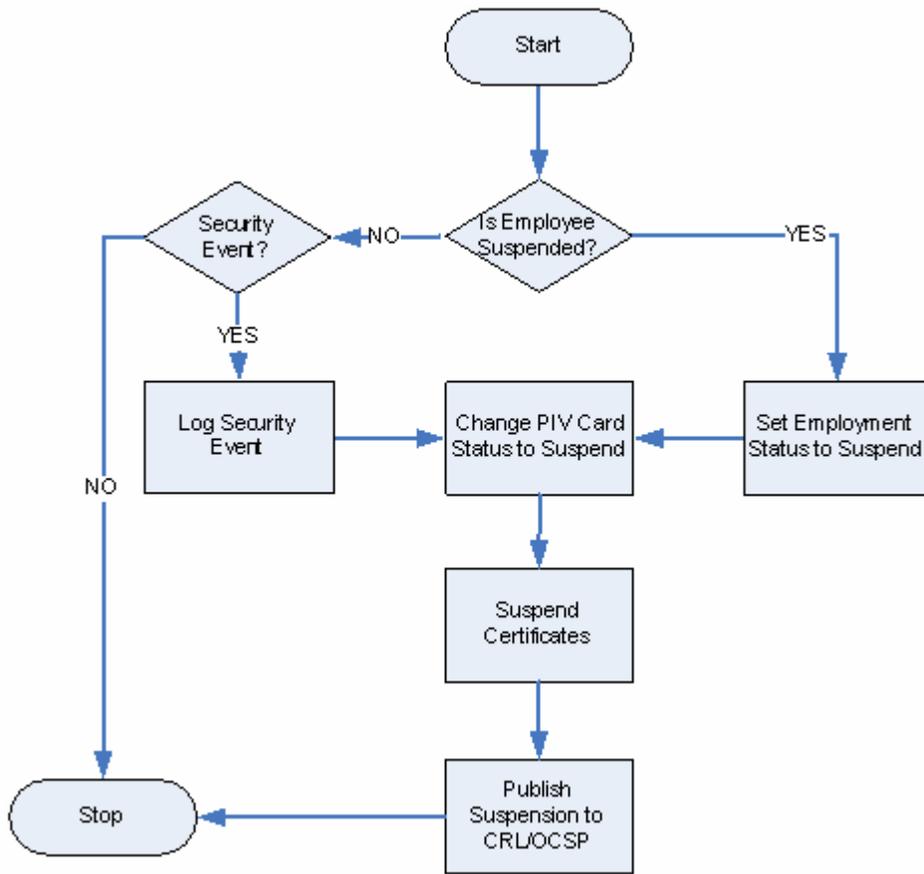


Figure 2-5: Suspend PIV Card Process Diagram

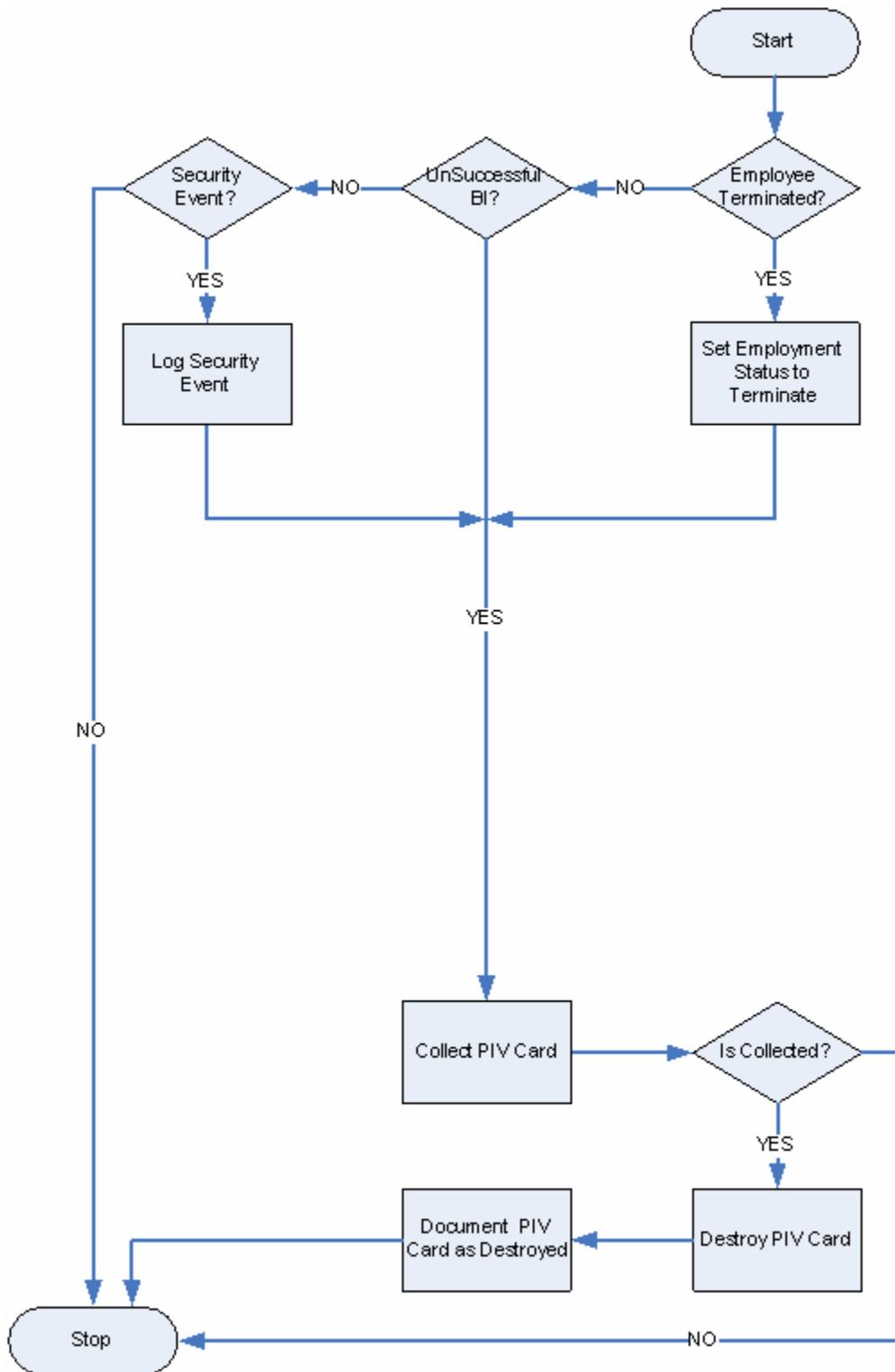
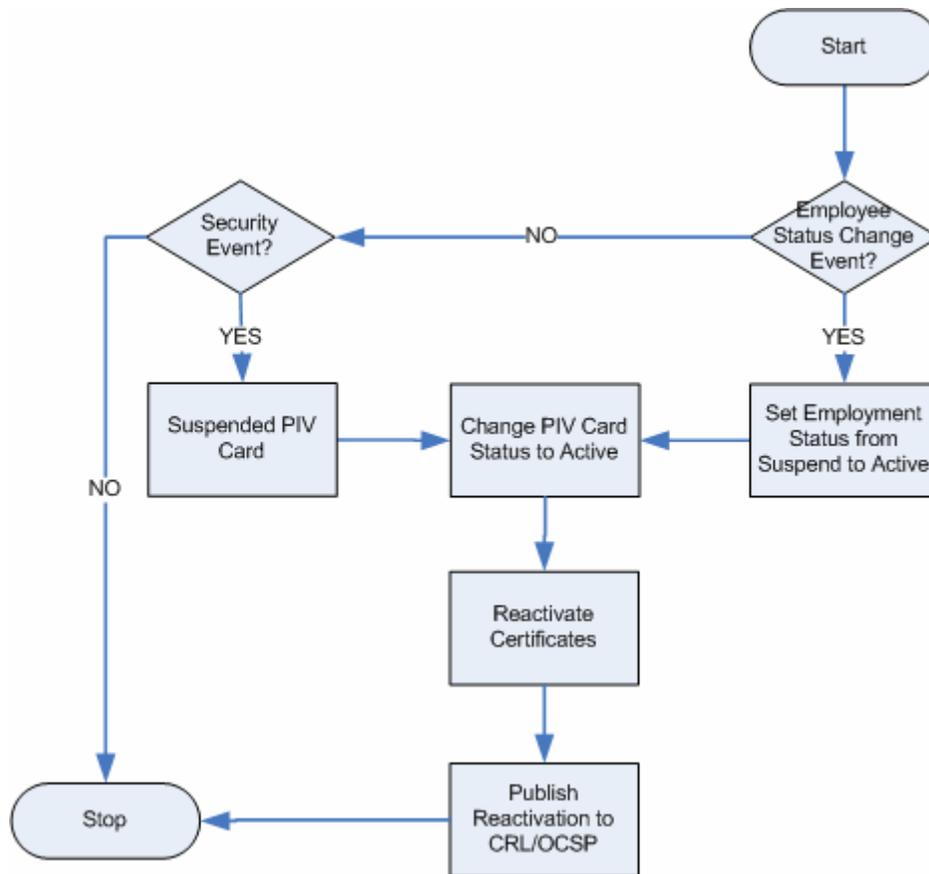


Figure 2-6: Revoke and Destroy PIV Card Process Diagram



**Figure 2-7: Reactivate PIV Card Process Diagram**

### 2.2.4.3 Agency Sponsor Role

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 status may change when a Cardholder retires, terminates, transfers to another department/Agency, 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.

#### 2.2.4.3.1 Agency Sponsor Requirements

- Be designated by the Agency Role Administrator
- Shall receive training and be certified as Sponsor
- Shall not download or remove PII from the system
- Be a U.S. Citizen

- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of Agency/Commission structure, including populations and missions of Agency sites
- Be familiar with PKI, the PIV issuance process, and the Service/Agency's Sponsor/Role process
- Have not been convicted of a felony offense
- Have had, as a minimum, a NACI background investigation performed
- Have not knowingly been denied a security clearance or had a security clearance revoked

#### **2.2.4.3.2 Agency Sponsor System Interfaces**

- Processes require web, or HRLOB interface, PIV Cards and digital signature
- Allows access to indicate vetted status, pre-adjudication, for existing background check records
- Allows search function, card reissuance, and card renewal. In addition, the Sponsor may change the employment status.
- Provides template topology and other details automatically selected for Applicants based on inputted information
- Training must be received

#### **2.2.4.3.3 Agency Sponsor Other Possible System Roles**

- Adjudicator, if designated by the Agency Role Administrator.

#### **2.2.4.3.4 Agency Sponsor Duties**

- A Sponsor has multiple duties within the system, and they include:
- Determines Applicant need for a PIV Card
- Uploads Applicant information into system based on HR database or enter information manually
- Updates record for Applicant based on user status and relevant information
- Ability to change employment status which may result in card suspension or revocation.
- Re-issue or reprint a new card for existing Cardholder
- Initiates re-enrollments for current or previous Cardholders

Sponsorship Process Diagrams

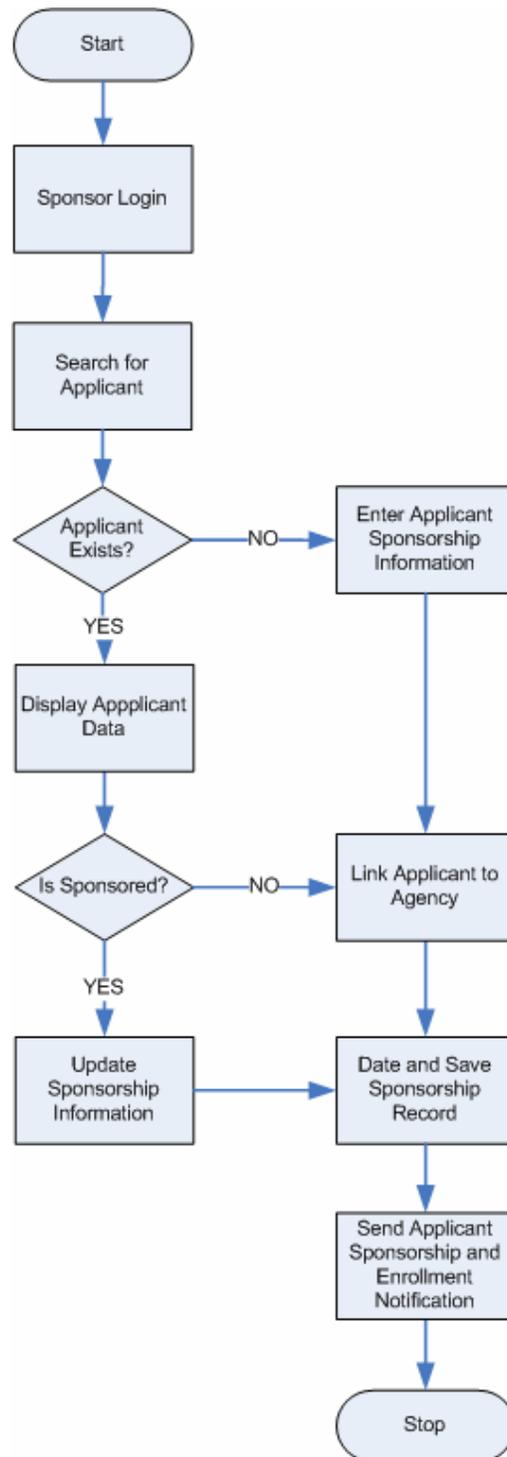


Figure 2-8: Sponsorship Process Diagram

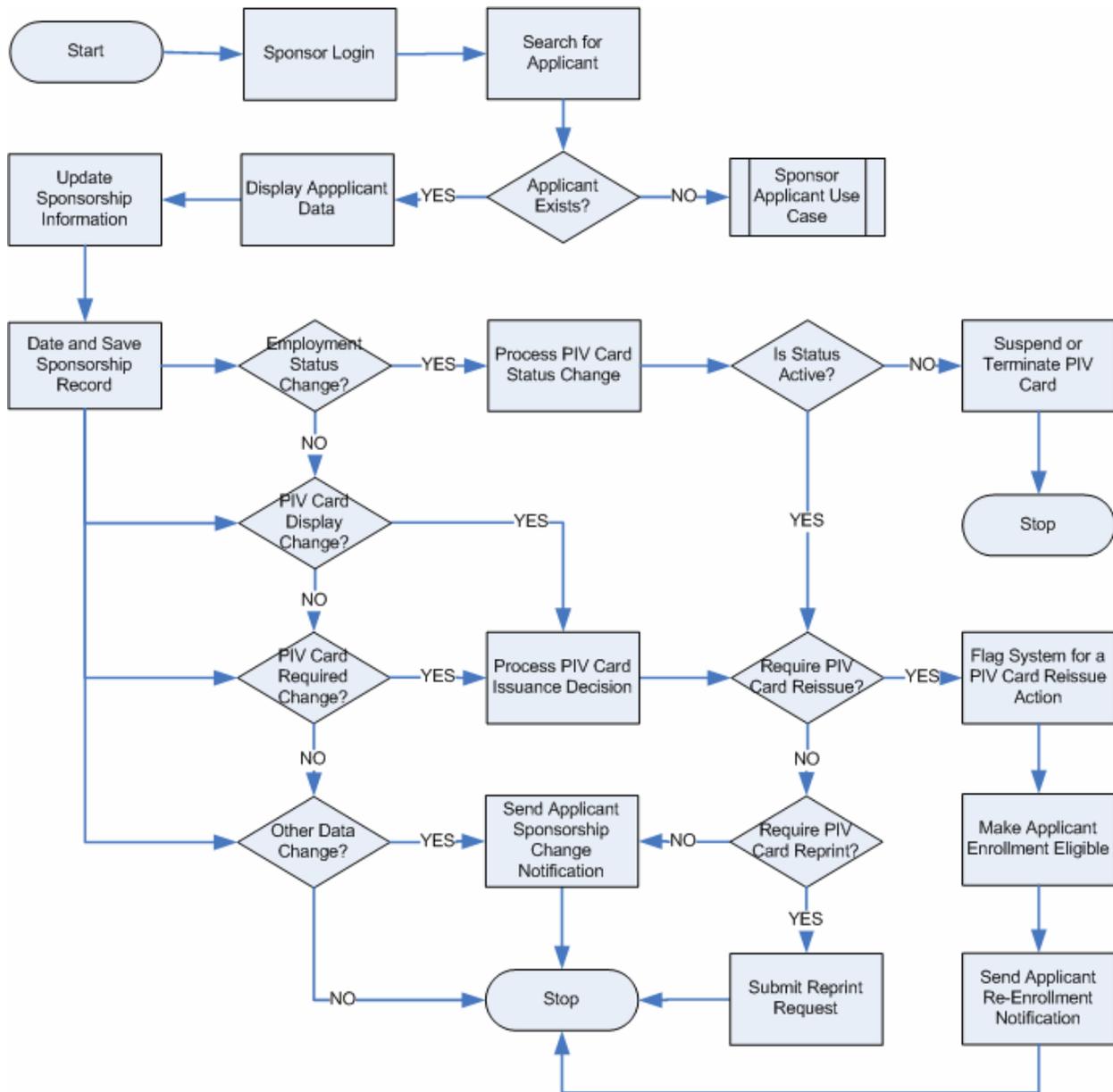


Figure 2-9: Update Applicant Sponsorship Information Process Diagram

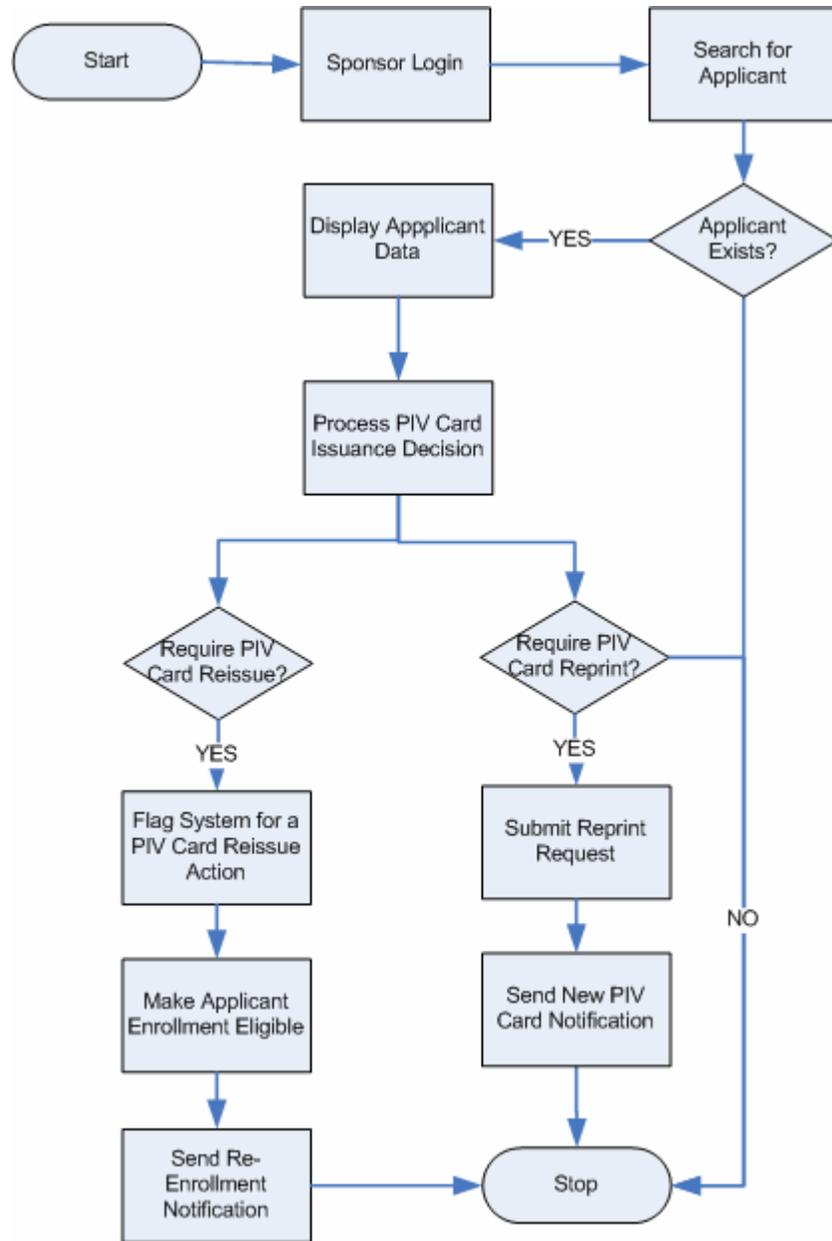


Figure 2-10: Request PIV Card Re-issuance or Reprint Process Diagram

### 2.2.4.4 Registrar Role

Note that this role does not specifically contain the title “AGENCY”. Registrars may be provided by the MSO, may be a government employee of an Agency, or may be a contracted employee of an Agency. All Registrars are controlled and supervised by the MSO in terms of their qualifications and ability to act in this role. The Registrar is the individual responsible for enrollment, which includes identity proofing the Applicant and collecting biographic information, a facial image, and fingerprints.

There are two types of enrollments that must be supported by the Registrar, (1) a new enrollment for an Applicant that has never been enrolled before, and (2) a re-enrollment required when a Cardholder needs a new card issued because of theft, loss, defective card, personal information update, or biometric changes.

- The Registrar confirms that the Applicant present at time of enrollment is sponsored, inspects two identity source documents in original form and scans the documents into the system. The Registrar then captures the Applicant’s photo and captures both flat and rolled images of all ten of the Applicant’s fingerprints. The photo and fingerprints are captured in accordance with FIPS 201-1 specifications. The system automatically generates a primary and secondary biometric minutia template, which is verified by the Applicant. The enrollment package is digitally signed and saved into the IDMS using certificates from the Registrar’s PIV Card. The Registrar cannot make changes to mandatory FIPS 201-1 identity fields within the enrollment record without authorization from a Sponsor to re-enroll. Non-mandatory fields may be updated as required. Unlike other roles, the Registrar may also perform a secondary role, as Activator, at the discretion of the Agency, with a documented chain of approval. The Registrar also manages enrollment workstation schedule in case of scheduling conflicts.

The basic enrollment tasks are provided in the following Table 2-3: Enrollment Tasks, in sequential order.

**Table 2-3: Enrollment Tasks**

Enrollment Tasks
1. Ensure the Applicant has the appropriate identity documentation (Appendix C)
2. Pull up the demographics information, fill in the remaining fields, and ensure it is correct
3. Validate the authenticity of identity documents (Appendix C)
4. Scan two valid identity documents (Appendix C)
5. Obtain slap images of Applicant’s fingerprints using the fingerprint scanner
6. Obtain rolled images of Applicant’s fingerprints using the fingerprint scanner
7. Verify that Applicant’s fingerprints can be matched to the scanned images that will be used to create the biometric template
8. Take the Applicant’s photograph
9. Validate that all information is correct and complete

Enrollment Tasks
10. Digitally sign the enrollment Application
11. Return all identity documentation to the Applicant

#### ***2.2.4.4.1 Registrar Requirements***

- Government employee or approved contractor
- Shall receive training and be certified as Registrar and pass a certification test
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of HSPD-12 policy and document properties
- Have not been convicted of a felony offense
- Have had, as a minimum, a NACI background investigation performed
- Have not knowingly been denied a security clearance or had a security clearance revoked

#### ***2.2.4.4.2 Registrar System Interfaces***

- Processes require web interface, dedicated enrollment station, PIV Cards and digital signature
- Verifies sponsorship automatically
- Training must be received

#### ***2.2.4.4.3 Registrar Other Possible System Roles***

- Activator

#### ***2.2.4.4.4 Registrar Duties***

- Provides re-enrollment functions
- Provides new enrollment functions
- Searches and retrieves the Applicant's record
- Scans and identifies authentic source documents
- Captures color photo

- Captures twenty fingerprints (ten flat and ten rolled)
- Verifies minutiae templates
- Flags any issues during enrollment
- Signs and send enrollment packet
- Informs Applicant of next steps

2.2.4.4.5 Enrollment Process Diagram

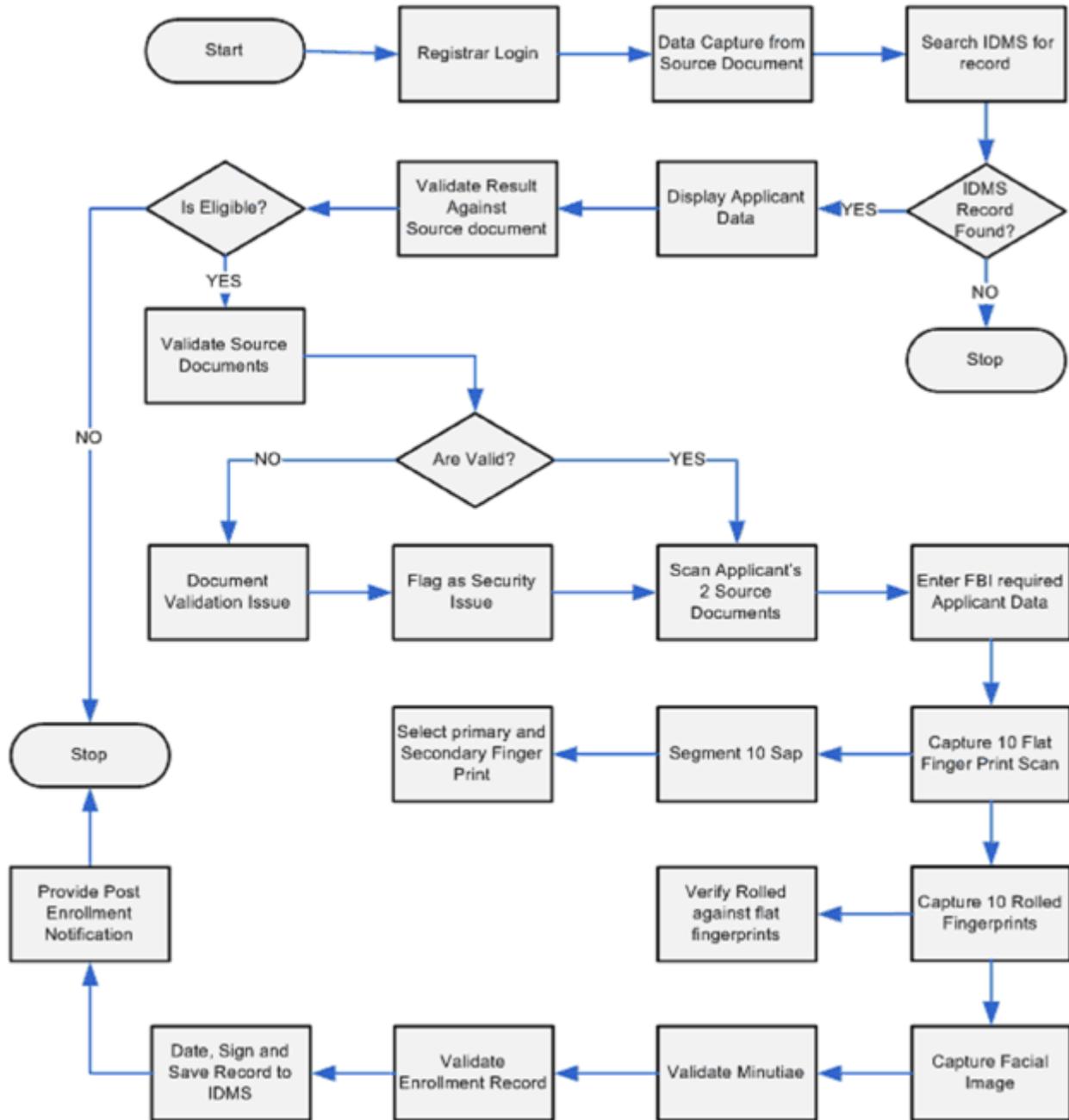


Figure 2-11: Enrollment Process Diagram

### **2.2.4.5 Agency Adjudicator Role**

The individual who is authorized to record the adjudication result for an Applicant. The Adjudicator enters or updates the status of adjudication result for all Applicants through a web enabled interface in the managed service system. A positive adjudication result will initiate the PIV Card issuance process.

After an Applicant is sponsored and has enrolled in-person with a Registrar at an enrollment workstation, a completed enrollment package is submitted for adjudication. The Adjudicator initiates the process of the system submitting the enrollment package to for a OPM/FBI background check. The required background checks for a PIV Card include a NCHC fingerprint check, and a NACI. The NCHC typically takes one to several days for adjudication, while the NACI may take several months for adjudication. Each Agency participating in the MSO is responsible for the background investigation checks required for each Applicant. After receiving background investigation results from the FBI or OPM, the Agency Adjudicator will enter in the Adjudicator portal and provide a decision that will be recorded as part of the Applicant's enrollment record. The Adjudicator provides an "approve" or "denied" decision in the system.

#### **2.2.4.5.1 Agency Adjudicator Requirements**

- Be designated by the Agency Role Administrator
- Shall receive training and be certified as Adjudicator
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Have a working knowledge of Agency/Commission structure, including populations and missions of Agency sites
- Be familiar with PKI, the PIV issuance process, and the Service/Agency's Sponsor/Role process
- Have not been convicted of a felony offense
- Have had as a minimum, a NACI background investigation performed
- Have not knowingly been denied a security clearance or had a security clearance revoked

#### **2.2.4.5.2 Agency Adjudicator System Interfaces**

- Processes require web interface, PIV Cards and digital signature

- Completes pending cases, recent status changes and unapproved cases are automatically queued for Adjudicator response
- Adjudicator input allows notification to print, suspend card, reinstate card, search for users within the Agency
- Training must be received

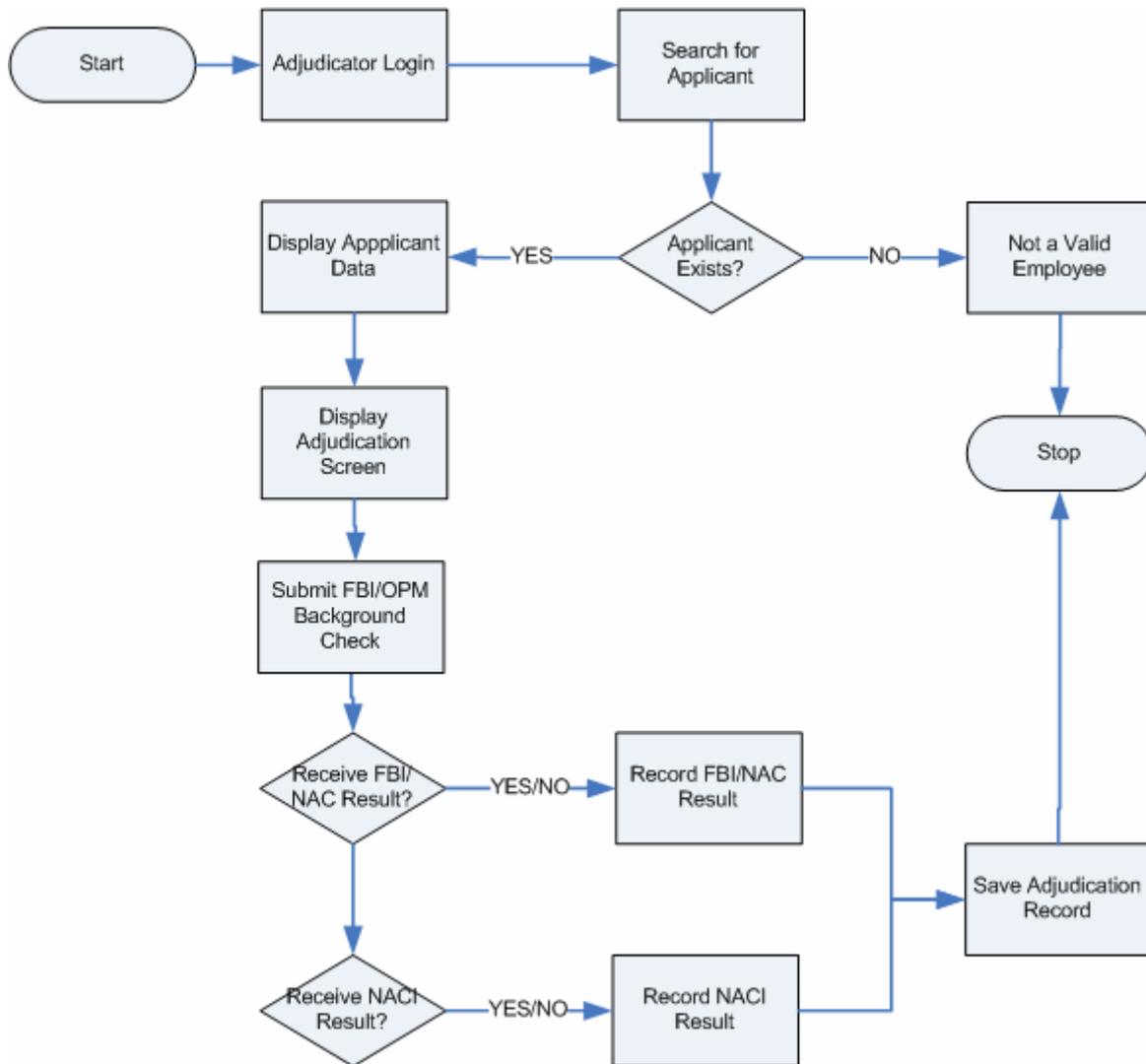
#### **2.2.4.5.3 Agency Adjudicator Other Possible System Roles**

- Sponsor, if officially approved by Agency Security Officer

#### **2.2.4.5.4 Agency Adjudicator Duties**

- Accesses web portal interface
- Receives manual reports on background checks
- Selects the required Submitting Office Number (SON) / Submitting Office Identifier (SOI) / Office of Payment and Collections – Account Lookup Code (OPAC-ALC).
- Responds to any inquiry by Applicants as to the status or reason for suspension or revocation based on background checks
- Can manage adjudication status, whereby upon positive/negative adjudication, the System can suspend cards, or reinstate cards previously suspended for an unsatisfactory background check

**2.2.4.5.5 Adjudication Process Diagram**



**Figure 2-12: Adjudicator Process Diagram**

**2.2.4.6 Issuance Process**

The MSO Issuance Process is handled at the system level, so there is not an Issuer role. However, there are some issuance workflows that shall be discussed.

In the issuance process, the MSO system processes the credential request, produces the PIV Card, and sends (issues) the PIV Card to the Applicant for activation. First, the system validates that all prerequisites are met for printing a card, which includes Applicant sponsorship, a successfully adjudicated background investigation, a complete validated enrollment, a biometric duplicate check, a full enrollment package, and an active employment status.

After these criteria have been verified, a card production pre-issuance package is built in the system,. A card production package print request is then submitted to the centralized printing facility whereby a card is printed and pre-personalized with the printed Applicant information and photo at the printing facility, and accuracy verified via establishes Quality Assurance (QA) processes. The card is now sent to a designated agency person for delivery to the Applicant. Finally, the Activator receives card from the Applicant and performs a 1:N identity check before attended activation.

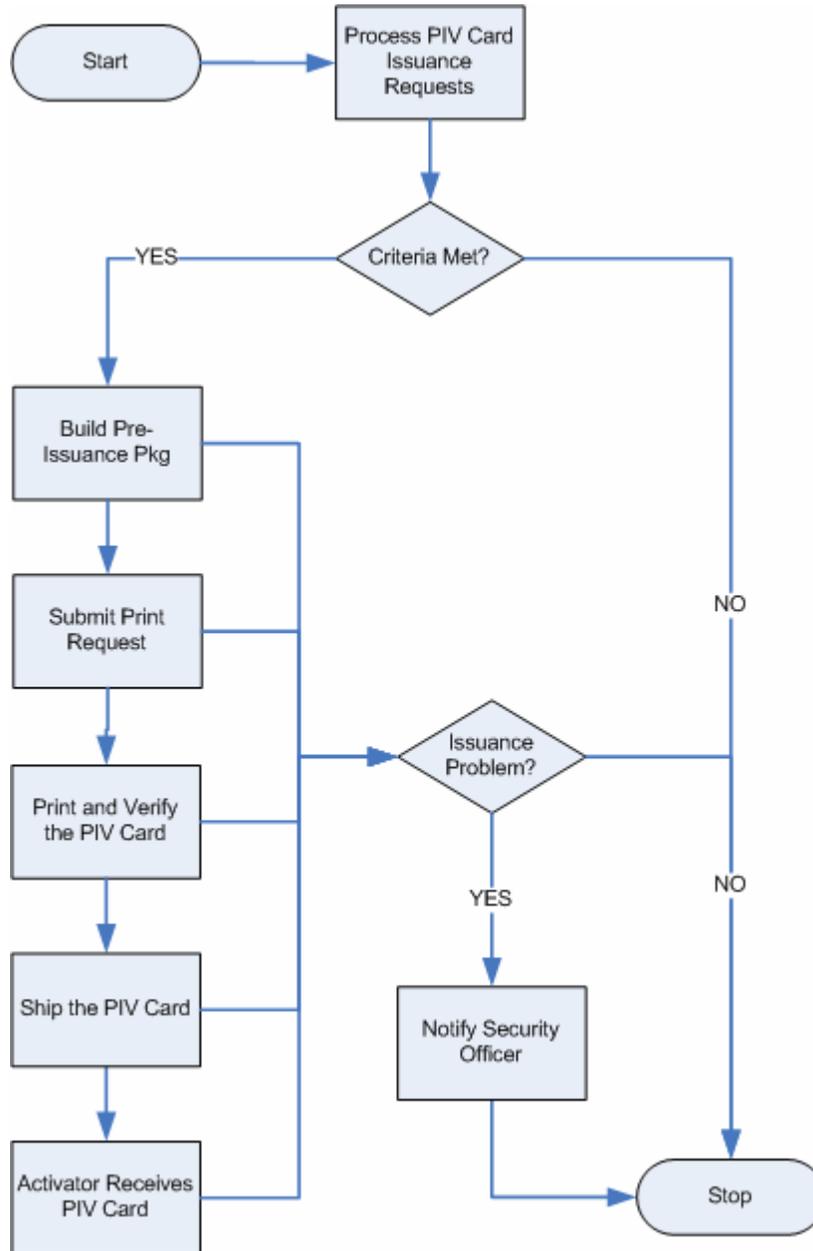
#### **2.2.4.6.1 Actors**

There are no actors for issuance. It is entirely an automated process.

#### **2.2.4.6.2 Issuance Use Cases**

- The following issuance use cases shall be supported:
- Normal Valid Card Issuance Process
- Pre-issuance Request with Security Issues
- Pre-issuance Request with Criteria Issues
- Invalid Card Printing Check
- Invalid Address
- Wrong Cards Shipped to Valid Address
- No Applicant Match for a Shipped Card

**2.2.4.6.3 Issuance Process Diagram**



**Figure 2-13: Issuance Process Diagram**

**2.2.4.7 Agency Activator Role**

The Activator is the individual responsible for processing PIV Card activations. The Activator verifies that the Applicant is the person to whom the PIV Card is to be issued via identity documentation verification, and guides the Applicant through the activation process. The Activation process starts when the Applicant receives the PIV Card and goes through the steps of

identification, loading of the certificates, activating and signing for the PIV Card. To activate the PIV Card, there is a two step process of unattended or attended activation. The Applicant's identity will be verified and biometrically authenticated, which unblocks the PIV Card. Subsequently, the system finalizes the personalization of the PIV Card by allowing the Applicant to set the Personal Identification Number (PIN) and by loading the required certificates. The Applicant then signs for the PIV Card, and the system sets the PIV Card status to active.

#### **2.2.4.7.1 Agency Activator Requirements**

- Be designated in writing by the Agency Role Administrator
- Shall receive training and be certified as Activator
- Shall not download or remove PII from the system
- Be a U.S. Citizen
- Be a Federal government civilian employee or designated personnel in the case of GOCO operated facilities
- Be a PIV Cardholder
- Be capable of sending and receiving digitally signed and encrypted email after initial enrollment
- Be familiar with PKI, the PIV issuance process, and the Service/Agency's Sponsor/Role process
- Have not been convicted of a felony offense
- Have had, as a minimum, a NACI background investigation performed
- Have not knowingly been denied a security clearance or had a security clearance revoked

#### **2.2.4.7.2 Agency Activator System Interfaces**

- Processes require web interface, PIV Cards and digital signature
- Dedicated workstation
- Updates new information processed by Activator (i.e., PIV Card status)
- Allows card activation, PIN reset
- System notifies Applicant of card ready for activation via email once the card is delivered to the site. Notification email also contains the Applicant's temporary system generated password used during the activation process.
- Training must be received

#### **2.2.4.7.3 Agency Activator Other Possible System Roles**

- Registrar

#### **2.2.4.7.4 Agency Activator Duties**

- Receives PIV Cards from the Card Production Facility (CPF), signs for packages
- Logs in PIV Cards
- Controls secure storage of PIV Cards in safe, logging all actions to items taken into or out of safe based on Agency specific policy and procedures
- Ensures Applicant identity through picture and biometric check
- Facilitates the activation of PIV Cards
- Verifies PIV Card has been activated properly
- Informs Applicant about PIV Card usage using Agency specific policy and procedures
- Performs PIN reset in CMS

#### **2.2.4.7.5 Agency Activator Use Cases**

- Attended Activation with Fingerprint Biometrics
- Attended Activation without Fingerprint Biometrics
- Attended Failed Activation
- The following use cases are within the Activation process but are the responsibility of the Applicant, and not the Activator:
- Unattended Activation with Fingerprint Biometrics
- Unattended Failed Activation

2.2.4.7.6 Activation Process Diagrams

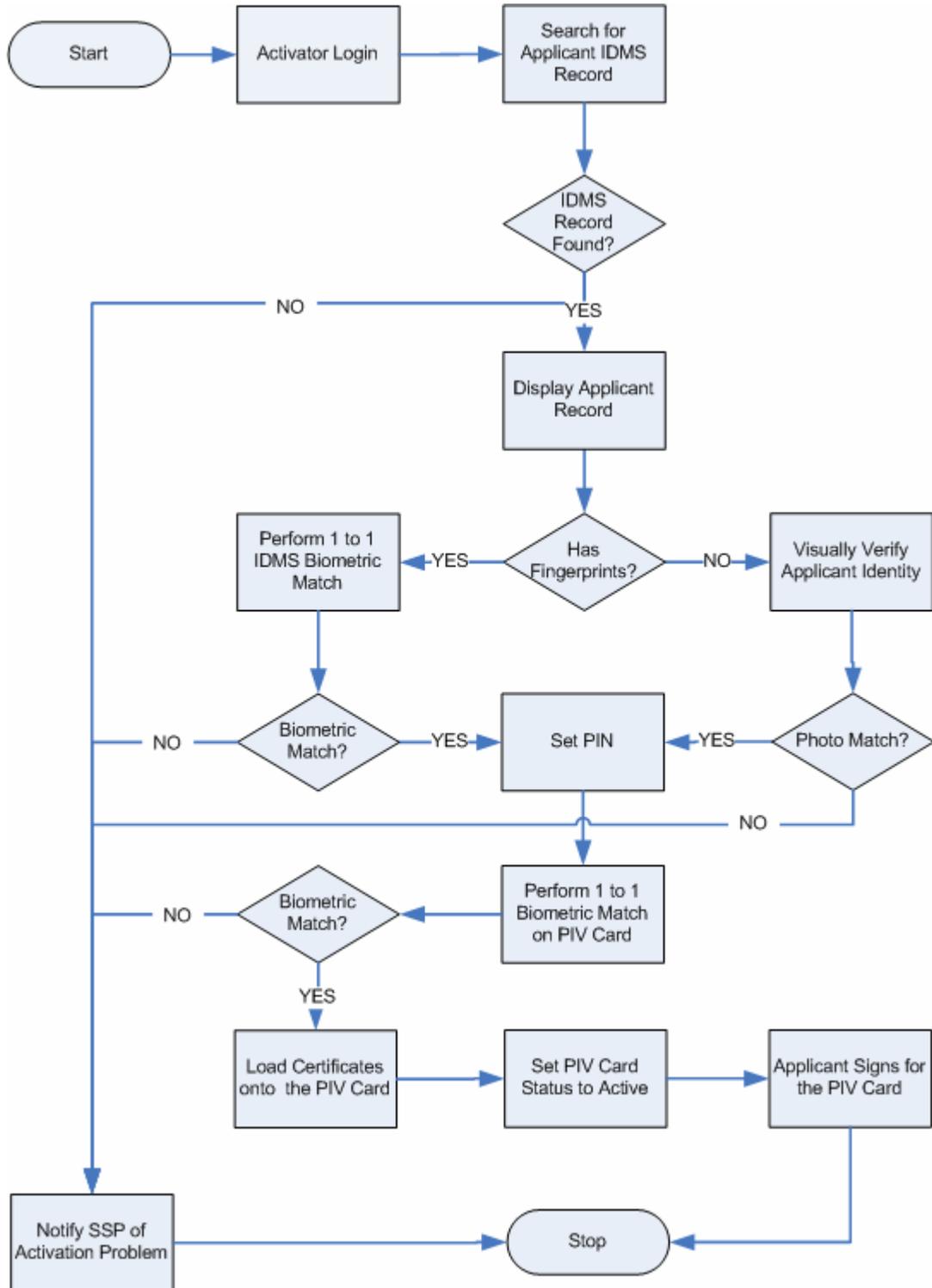


Figure 2-14: Attended Activation Process Diagram

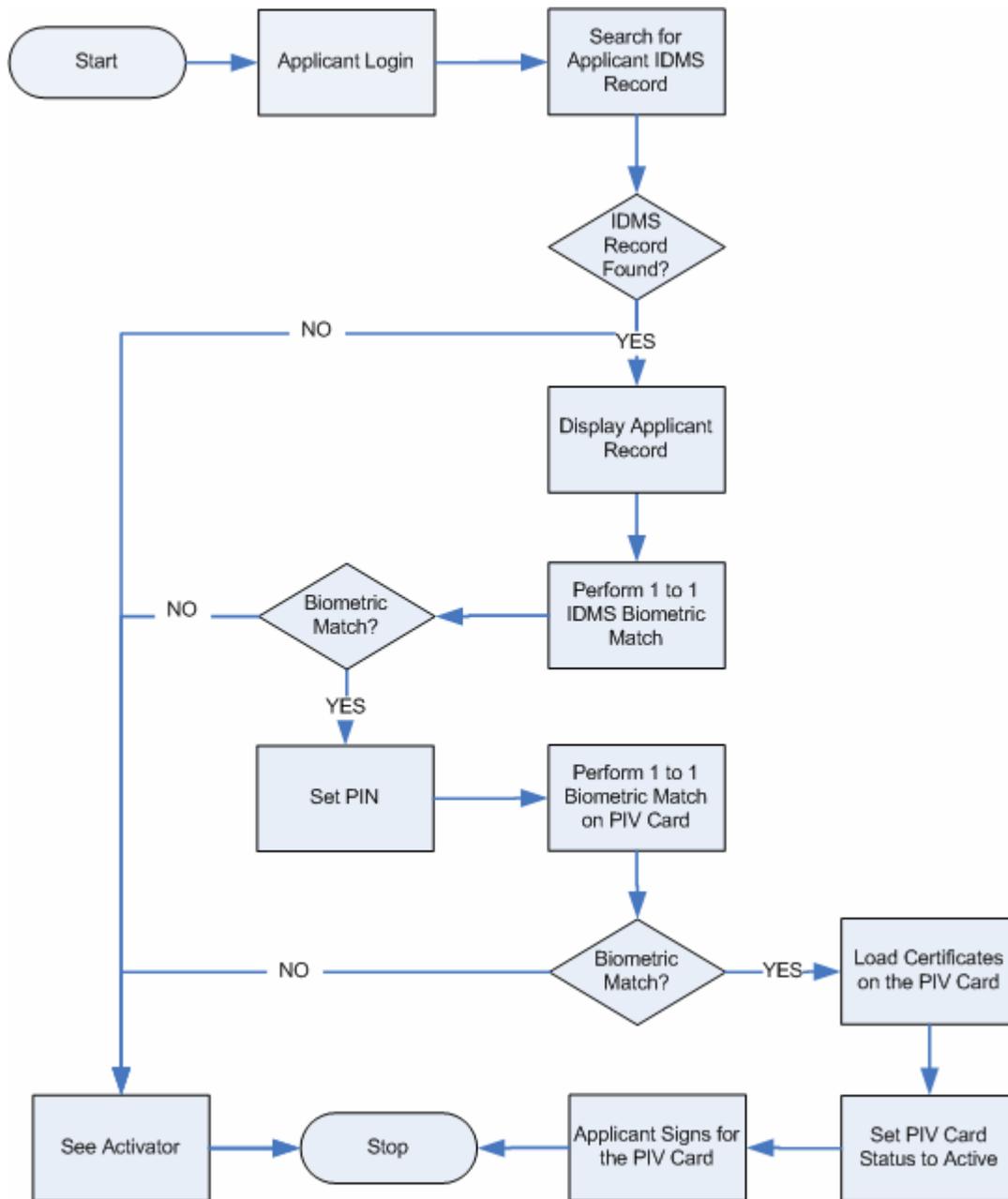


Figure 2-15: Unattended Activation Process Diagram

### 2.2.4.8 Applicant

#### 2.2.4.8.1 Applicant Requirements

- Government employee or affiliated contract employee
- Meet policy guidelines for a PIV credential

- Applicant System Interfaces
- No private user interface to records
- Access to scheduling tool on website
- Public website for FAQ
- Training is available for Applicants, with requirement left to Agency policy

**2.2.4.8.2 Applicant Other Possible System Roles**

- None

**2.2.4.8.3 Applicant Duties**

- Informs Sponsor of changes to personal information
- Schedule Enrollment and Activation appointments as required
- Arrives for enrollment with identity documents (see Appendix C)
- Arrives at activation station
- For unattended activation, provide username and password (provided when notified card was ready for activation).
- Sets new PIN
- Maintains the PIV Card in accordance with all security and privacy regulations
- Returns PIV Card for revocation upon separation or if no longer affiliated with sponsoring organization

**2.3 Role Management Hierarchy Enforcement**

The MSO system and Agency level role hierarchy is displayed in Table 2-4: PCI Role Management Hierarchy Enforcement Rules, or constraints, as defined in the technical requirements, provide the separation of duties, both static and dynamic based on the situation, providing effective GSA policy enforcement. Enforcing these policies allows certain combinations of PCI business functions to be performed; prevents certain combinations from being performed by the same person; and/or prevents certain functions from being carried out if role memberships are terminated.

**Table 2-4: PCI Role Management Hierarchy Enforcement**

ROLE EVENT	ROLE HIERARCHY ENFORCEMENT ACTIVITY	SYSTEM OR AGENCY SPECIFIC ENFORCEMENT
<b>Change in Role Membership</b>		
MSO System or Agency Sponsor Termination	Negates Applicant sponsorship at the time of Sponsor submittal	Applies to both System and Agency roles

ROLE EVENT	ROLE HIERARCHY ENFORCEMENT ACTIVITY	SYSTEM OR AGENCY SPECIFIC ENFORCEMENT
	Applicants previously sponsored are unaffected	
MSO System or Agency Adjudicator Termination	Negates Applicant adjudication at the time of adjudication submittal Applicants previously adjudicated are unaffected	Applies to both System and Agency roles
MSO System or Agency Activator Termination	Negates Applicant activation at the time activation submittal Applicants previously adjudicated are unaffected	Applies to both System and Agency roles
Registrar Performing Another Role	Registrar can also perform role as Activator	Applies to Agency roles
<b>Records Access</b>		
MSO System Security Officers records access rights	MSO System Security Officers can access ALL records	System and Agency independent
Agency Security Officers records access rights	Agency Security Officers can only access records for their designated Agency	Agency specific
Agency Sponsor creating or modifying records	Sponsors can only create or modify sponsorship records for their designated Agency	Agency specific
Agency Adjudicators creating or modifying records	Adjudicators can only create or modify adjudication records for their designated Agency	Agency specific
Agency Activators performing card activation	Activators are not Agency-bound, and thus, can activate any Agency or system PIV Card	System and Agency independent
<b>Role Account Administration</b>		
Agency Role Account Management	Agency Role Account Administrator Officer can only create and manage roles for their designated Agency, and sub-agencies, as applicable	Agency specific
MSO System Role Account Administration	MSO System Role Account Administrator can create and manage roles across Agencies	Agency independent
<b>System Management and Audit Logs</b>		
MSO System Security Officer Audit Log Access	Note: In general, only Security Officers (System and Agency) will have access to system and audit logs MSO System Security Officers have access to ALL system and audit logs	System and Agency independent
Agency Security Officer Audit Log Access	Agency Security Officers have access to system and audit logs relevant to their Agency Agency Security Officers may only see events in	Agency relevant dependency for system access

ROLE EVENT	ROLE HIERARCHY ENFORCEMENT ACTIVITY	SYSTEM OR AGENCY SPECIFIC ENFORCEMENT
	system logs tied to either activities of their Agency, or Applicants sponsored by their Agency.	

## 2.4 MSO and Agency Program Initialization Operations

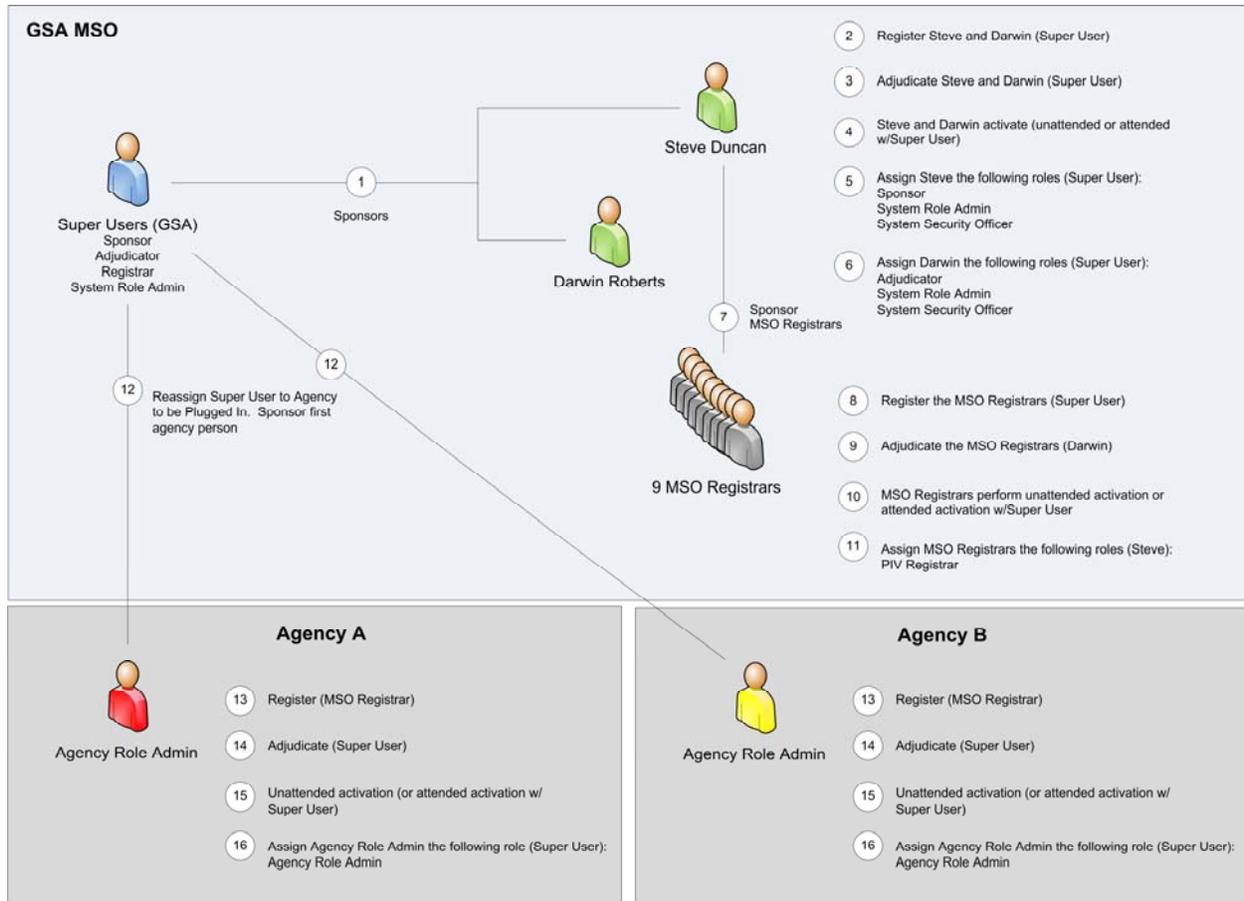
The following subsections will document the step-by-step process for initializing the MSO Program for both the MSO and all participating agencies.

### 2.4.1 MSO System-Specific Initialization

This section provides a description of the various steps necessary to launch the MSO Program PIV role assignments within the MSO environment. Using this approach, the MSO structure becomes established, and enables the GSA MSO to stand up each individual Agency and help them build out their Agency specific implementations.

Overall, this system represents the classic “Chicken or the Egg” concept. The MSO system is a credentialing system being operated by credential holders. In order to create users in the system, there must first be a user already created who performs the operations. As such, it is important to establish an MSO Super User at the system level. This Super User is seeded into the system and has special privileges across the application space to enable the initial establishment of the key role holders. The individual performing the actions of the Super User will be a trusted member of the MSO team.

The following steps describe the process represented in Figure 2-16: MSO System Initialization for establishing the MSO credentialing support structure.



**Figure 2-16: MSO System Initialization**

1. The first step is for the Super User to sponsor the two initial key role holders in the MSO organization. These role holders will be pivotal in establishing the other players in the system.
2. The Super User will then perform the enrollment of the two MSO representatives.
3. The representatives will already have an existing background check, so the Super User need only fill in the adjudication particulars for each individual.
4. The MSO representatives may then perform unattended activation to receive their official PIV Cards.
5. Next, the Super User assigns the MSO representative 1 to the Sponsor, System Role Administrator, and Security Officer role.
6. The Super User then assigns the MSO representative 2 to the Registrar, System Role Administrator, and Security Officer role.
7. The next phase creates a bench of Registrars available for the MSO to provide for initial Agency enrollments. The first step in the creation of the MSO Registrars is for MSO

representative 1 (depicted as Steve Duncan above) to Sponsor the batch of MSO Registrars.

8. The Super User will then perform the enrollment of the MSO Registrars.
9. Adjudication is performed by MSO Representative 2 (depicted as Darwin Roberts above).
10. The MSO Registrars perform unattended activation to activate their official PIV Cards for use in the enrollment system.
11. The MSO Registrars are then added to the PIV Registrar group so they may perform the function of Registrar for the GSA and other agencies. This group's assignment is performed by either one of the MSO representatives since they both hold System Role Administrator privileges.

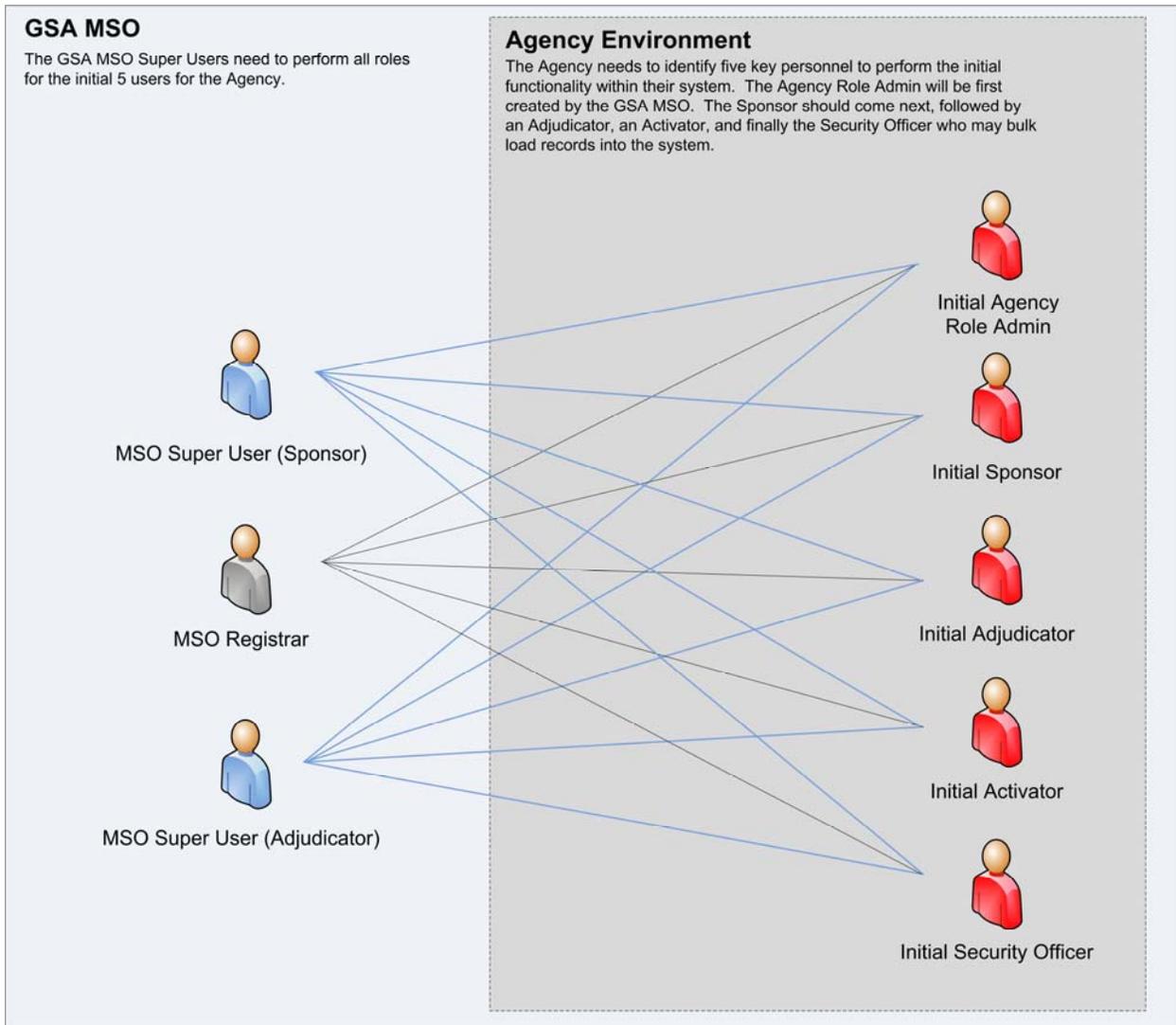
At this point, the MSO has established a team of users with enough control to help an Agency create their own credentialing support infrastructure. There is a MSO Sponsor, MSO System Role Administrators, and a bench of Registrars available for a particular Agency to leverage.

1. The next step is for the MSO to work with particular agencies in a one-on-one interaction to determine the plan for identification and implementation of their key role holders. Once the Agency has signed up for the creation of the first key role holder, the MSO will reassign the Super User to that particular Agency in order to maintain the scope of influence for only that Agency. The Super User then sponsors the initial Agency Sponsor and initiates the process within the particular Agency.
2. After which, the MSO Registrars are leveraged to enroll the initial Agency role holders (Sponsor, Adjudicator, Activator, and Security Officer).
3. The Super User records the adjudication results.
4. The Agency Role Administrator is now created, and, after the MSO representatives establish the additional Agency roles (Sponsor, Adjudicator, Activator, Security Officer), as described in the next section, the Agency Role Administrator is positioned to start identifying other Agency personnel to be assigned to follow-on Agency PIV roles.

### **2.4.2 Agency System-Specific Initialization**

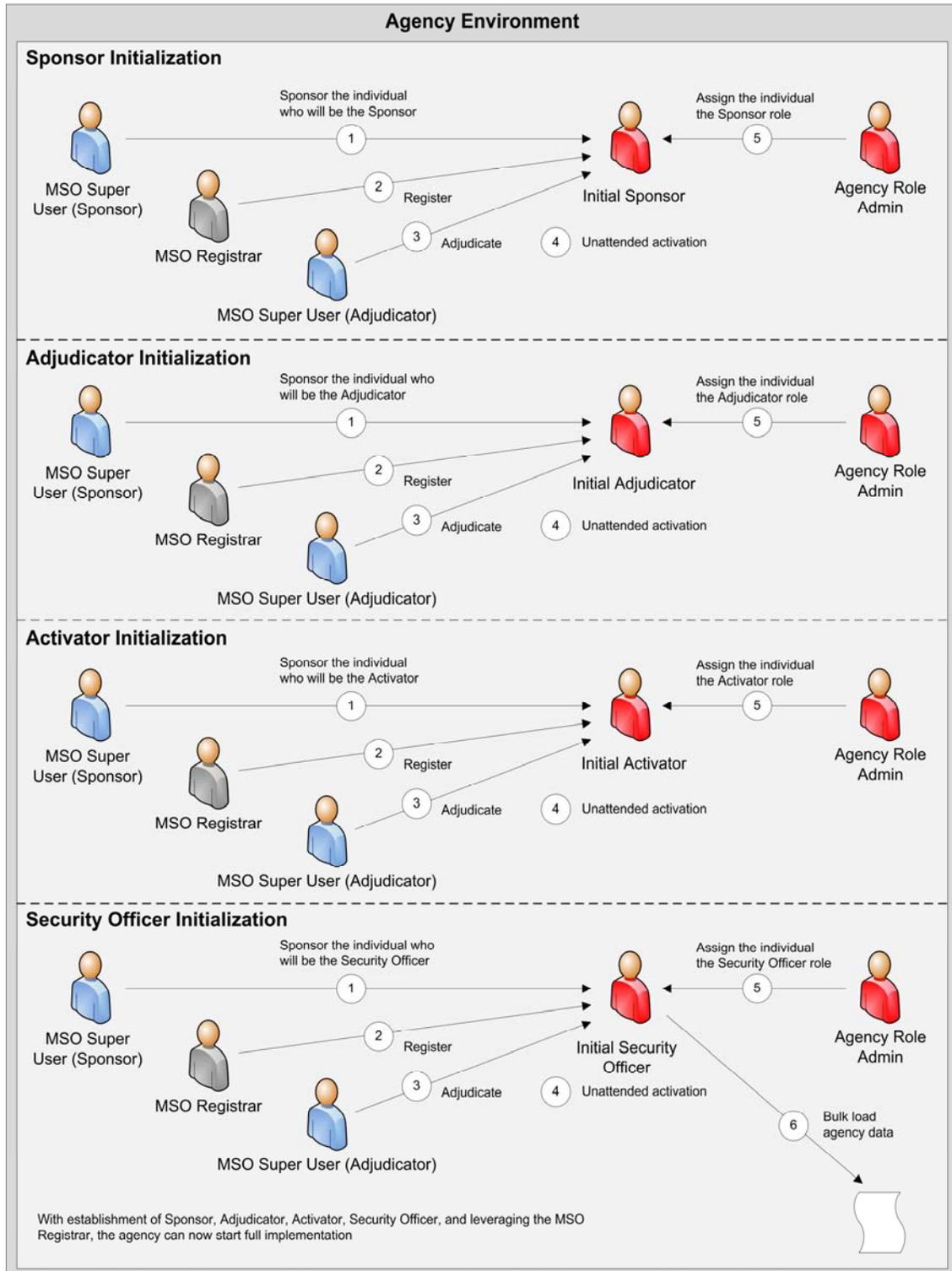
The previous section provided details on the establishment of the key MSO role holders and the initial Agency Sponsor. This section discusses creating the entire Initial Agency Role environment, and provides the methodology for an Agency to stand up their implementation of the MSO credentialing program after their Initial Agency Role assignments have been created.

The relationships in Figure 2-17: Identifying Key Agency Personnel depicts the interaction between the MSO program office and each Agency at a high level. Prior to kick off, the MSO will work with the Agency to determine the most suitable time to initiate the additional Agency users into the system. The Agency should identify their key personnel who will perform the "initial" PIV role functionality within their Agency.



**Figure 2-17: Identifying Key Agency Personnel**

The Agency Role Administrator identifies the specific Agency personnel for the roles of Initial Agency Sponsor, Initial Agency Adjudicator, and Initial Agency Security Officer. The MSO Super Users, acting as MSO Sponsor, MSO Registrar, and MSO Adjudicator create the four Initial Agency Roles for those identified individuals, as shown in Figure 2-18: Creating the Initial Agency Role Environment.



**Figure 2-18: Creating the Initial Agency Role Environment**

### 2.4.3 Enrolling Additional Agency Personnel

Following the establishment of Initial Agency Roles created by the MSO, the Agency now can implement those roles to stand up and expand their implementation of the MSO credentialing program. At this point, the Agency has a firm footing and should be able to start processing a higher number of Applicants through the system. It is the Agency's discretion, beyond the initial users, how they want to staff their program. The Agency may want to add another individual and assign them the Registrar role so they may perform enrollments without leveraging the MSO Registrars. The Agency may also want to add multiple Sponsors and Adjudicators to handle the increasing work load. All of these options are available to the Agency to help expedite the creation of new PIV Cardholders.

## 2.5 PIV Card Lifecycle Operations

### 2.5.1 Re-Issuance

Once an Applicant is issued a PIV card, that individual becomes a Cardholder. PIV Card Re-Issuance occurs when

- A Cardholder's PIV card is lost, damaged, stolen
- A Cardholder's PIV card is invalid due to a status change that modifies the printed text on the PIV Card
- A Cardholder's PIV card biometrics printed or embedded electronically on the card are no longer valid.

Re-Issuance also coincides with termination and revocation operations for the existing card and certificates, explained in the next section. If any one of the three bullets listed above occur, the enrollment process required for re-issuance will also include fingerprint and facial image recapture.

The Agency Sponsor and Security Officer will have the ability to initiate a card re-issuance event. The Cardholder will have to go through the Sponsorship, Enrollment, and Activation processes again to receive a new PIV Card. The Cardholder will not be required to go through the Adjudication process. The Cardholder will then be notified of the re-issuing and the scheduling of the enrollment time by the Agency Sponsor and Security officer. A new card will be activated for 5 years.

### 2.5.2 Termination

As part of PIV card Re-Issuance, the existing PIV card must also be terminated. Termination includes the revocation of all certificates, and physical destruction of the PIV card (if it is available). During PIV Card re-issuance and termination the following occur:

- The PIV Card itself is revoked

- The PKI CA is informed and the certificates on the PIV Card are revoked
- Online Certificate Status Protocol (OCSP) responders and Certificate Revocation Lists (CRLs) are updated so that queries with respect to certificates on the PIV Card are answered appropriately.
- GSA MSO and agency databases containing Federal Agency Smart Credential Number (FASC-N) values must be updated to reflect the change in status
- Through data replication, GSA MSO agency accounts and the Identity Management (IDMS) system are updated with the card termination and certificate revocation status.
- The Card Holder's privacy data collected during PIV Card Registration (PII) is handled in accordance with the data storage and retention policies that are enforced by the associated GSA PIV System of Record.
- The PIV card is collected and destroyed (if available). Terminated PIV cards shall be disposed of in accordance with established requirements for the physical destruction of PIV cards. PIV Card destruction is explained in Section 2.5.3.

When the PIV card is to be terminated, the Agency Sponsor or Agency Security Officer shall initiate the PIV card and certificate revocation process in the System, and the revocation process shall be completed within 18 hours of notification. The card revocation can also be handled in an automated process as the CMS Notification Service routinely scans Applicant records. When the CMS Notification Service finds an Applicant's status of "terminated, rejected, or revoked" it automatically sends a revoke notification to the CMS Web Service which interacts with the CMS where the Applicant's PIV Card status is changed to "invalid." The Applicant's PIV Card and certificates are then revoked

If emergency revocation is required, the Agency Security officer contacts the MSO Security Officer, requesting emergency action. In turn, the MSO Security Officer executes the emergency revocation.

### **2.5.3 PIV Card Renewal**

PIV Card Renewal is the process by which a PIV Card is replaced after 5 years of use. The card renewal process will be no different from the re-issue event, except the Cardholder must be notified automatically at 90 days prior to the expiration of the card. The Cardholder receives notification that the Cardholder's PIV Card is about to expire, with one of the scheduled renewal times of 90, 60, and 30 days. The system emails the renewal notification to the Cardholder. Accordingly, the Cardholder can initiate the process for card renewal. The Cardholder will have to go through the Sponsorship, Enrollment, Adjudication, and Activation processes again to receive a new PIV Card.

### **2.5.4 PIV Card Certificate Renewal**

For a PIV Card Certificate Renewal event, the Cardholder is notified that the PIV Cardholder's certificates are about to expire. The system routinely scans Cardholder records. When a PIV

Cardholder's certificate expiration date coincides with one of the scheduled renewal notification times (90, 60, or 30 days), the system emails the PIV Cardholder a renewal notification. The certificate renewal process can be activated in two methods, Attended Certificate Renewal and Unattended Certificate Renewal.

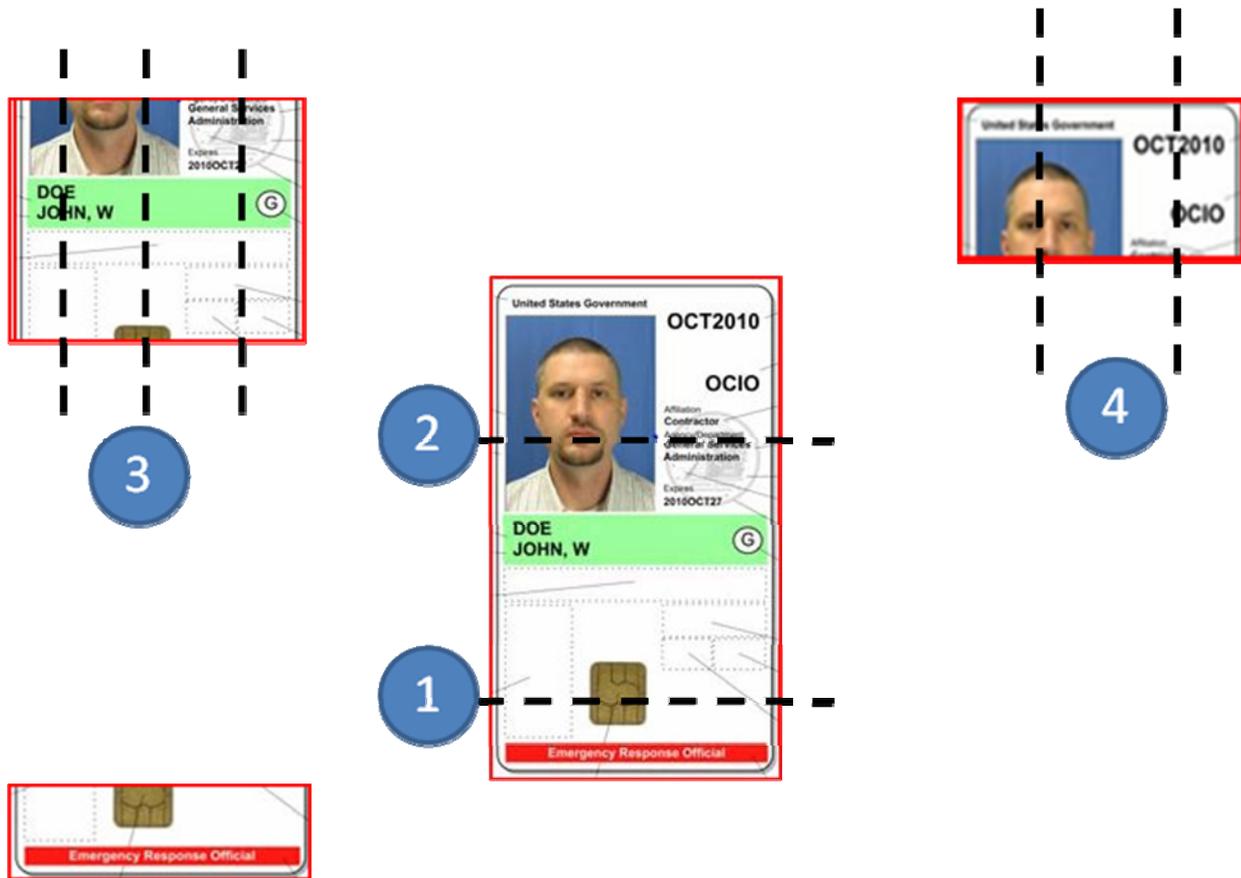
### 2.5.5 PIV Card Destruction

A PIV card must be destroyed under the following circumstances:

- When it has expired
- When the owner has lost affiliation (separation, end of contract, etc)
- When returned after being out of direct control of the owner, in accordance with Federal PKI Policy
- When the credential is replaced with a new credential due to name change, re-issuance, re-enrollment.

Credentials returned to sponsor for destruction should be revoked and then physically destroyed to ensure that the privacy data of the credential owner is protected in accordance with the privacy act. Credential destruction shall be accomplished in the following manner:

1. The Applicant's status should be set to "Terminated" through the Sponsorship portal.
2. The credential shall be physically destroyed with concern for PII data as follows:
  - a. Place the credential card into an industrial shredder.
  - b. Alternatively, cut the credential as shown in the diagram shown
    - Cut through the Integrated Circuit Chip (ICC) as shown by (1)
    - Cut the remainder through the photo as shown by (2)
    - Cut the center section into 3 pieces with emphasis on destruction of the name(3)
    - Cut the top section into 3 pieces (4)
3. This process will ensure that the ICC is destroyed, all contactless antennae are destroyed, and PII information is removed from the face of the card. Additionally, the magnetic stripe on the rear shall be severed and the bar code (if printed) shall be removed.
4. The Sponsor shall mark the card as "destroyed" on the sponsorship page for the credential owner in the Sponsorship portal and save the record.



### 2.5.6 PIV Card Holder Daily Usage Operations

The Card Holder has important card usage responsibilities that require careful consideration. The PIV card is not only a visual form of employee identification, it is also the platform that confirms assigned privileges to federal personnel, allowing them to conduct their daily business operations such as accessing network system resources or to enter approved federal facilities. The Cardholder Usages are identified below:

Cardholders are expected to protect the PIV card’s physical integrity, operability, and data content accuracy, as a normal part of their duties as an employee, contractor, or affiliate, and alert the PIV Sponsor if any of the following occurs:

- If the PIV card begins to wear (i.e., laminate coming lose, ink rubbing off, cuts/rips/tears occur in the card), they shall return to the Sponsor immediately.
- If the PIV card is lost or stolen, the Card Holder shall notify the Sponsor immediately.
- If the PIV card does not operate properly when inserted into a logical or physical access reader, the Cardholder shall notify the Sponsor immediately.
- If any personal information changes, the Cardholder shall notify the Sponsor immediately (i.e., changes in affiliation, name change, or other personal information changes).

- When the PIV card is scheduled to expire within 6 weeks, in order to maintain its operability without lapse.

HSPD-12 and FIPS-201-1 require agencies to increase the protection of Government facility and systems access. The PIV card is issued to securely and reliably provide that capability. The PIV Cardholder plays a central role in this capability and must not leave the PIV Card unattended, especially in a smart card reader, as doing so risks tampering and exploitation.

The rule of thumb for PIV card protection is to keep the card where it belongs, in its plastic holder attached to the lanyard on the Cardholder's person if it is not currently being used for logical access to computer systems. Only the Agency issued lanyard/holder will be used to wear and display the PIV card. No pins, badges, decals or similar items may be added to the badge or holder. In addition, no holes are to be punched in cards for any reason. A hole punched in the card will impact the embedded antennae and will void the warranty.

## 2.6 Privacy Policy

HSPD-12 explicitly states that “protecting personal privacy” is a requirement of the PIV system. As such, GSA Offices shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in FIPS 201-1, as well as those specified in Federal privacy laws and policies, including but not limited to Section 207 of the E-Government Act of 2002, the Privacy Act of 1974, as amended (5 U.S.C. §552a), and OMB Memorandum M-03-22, as applicable.

PIV records are subject to the Privacy Act and E-Government Act of 2002 requirements. GSA Offices and staff that collect, maintain, safeguard and use this information must comply with the Government statutory requirements and Policy. The GSA Privacy Act Program (CPO 1878.1) regulation requirements on safeguarding Privacy Act information must be used to ensure that appropriate safeguards are in place for handling PIV information.

The GSA Privacy Act Program (CPO 1878.1) ensures that those authorized to access personnel records subject to the Privacy Act of 1974 understand how to apply the Act's restrictions on disclosing information from a system of records, and specific Privacy Act system of records instructions.

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

One new privacy measure is that certain information on PIV information are to be provided to card Applicants, see Appendix E – PIV Card Usage Privacy Act Notice. Another new measure is that GSA will post, in multiple locations GSA's PIV Privacy Act statement/notice, complaint procedures, and appeals procedures for those denied identification or whose identification credentials are revoked and sanctions for employees violating Agency privacy policies and post the notice.

Protecting the personal privacy information required to issue a PIV card is a primary concern of HSPD-12 and the GSA PCI Manager. The GSA has written, published, and maintained a clear and comprehensive Privacy Impact Assessment (PIA) document which lists the types of information collected about PIV Applicants, the purpose of collection, what information may be disclosed to whom during the life of the PIV card, how the information will be protected, and the complete set of uses of the card and related information. The GSA PIV SORN identifies the approved usage and government entities that are officially authorized to access Applicant identity records, which includes releasing records for legal purposes.

If an individual wishes to access his or her PIV record, the individual must work through the local Agency Security Officer or other privacy authority to request that the GSA MSO provides a report of the individual's collected data. The GSA MSO has a separate CLIN available to the Agency for ordering the data report.

The GSA MSO has already complied with the below requirements in developing the MSO PIV system:

- The GSA PCI Manager assures systems containing personal information adhere to fair information act practices
- The GSA PCI Manager maintains compliance of PIV systems with stated privacy policies and practices governing the collection, use, and distribution of information; and
- The GSA PCI Manager enforces limited access to information in PIV systems to those persons with a legitimate need for the information.

## 2.7 Background Investigation Requirements

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

Appendix F describes the types of forms required for various background investigations and OPM scheduling and contact information.

Locating and referencing a completed and successfully adjudicated NACI or unexpired higher-level background investigation may also satisfy the requirements. To locate and reference a previously completed and successfully adjudicated NACI, contact the Bureau/Office Personnel Security Office or Human Resources Office within the local Agency, as appropriate. If the Applicant indicates that he/she has already been the subject of a Federal background investigation without a subsequent break in Federal employment, or Federal contracting employment not exceeding two years, the Applicant will be asked to furnish specific information, which will be used to verify the background investigation. The Agency Office of Human Resources (OHR) may meet the above requirements by completing the Form SF-75,

Request for Preliminary Employment Data, Section G, Security Data, for federal employees transferring to GSA.

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

In accordance with the NACI these are the basic and minimum investigations required from all new federal employees and contractors. These consist of the following searches:

- OPM Security/Suitability Investigations Index (SII)
- Defense Clearance and Investigations Index (DCII)
- FBI Name Check

A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes: employment (five years); education (five years and highest degree verified); residence (three years); references; law enforcement (five years); and NACs.

A provisional PIV Card will be issued after successfully completing the FBI/NAC investigation, verifying applicant's PIV information and collecting two forms of identification (see Appendix C). Once these steps are completed, a PIV Card will be successfully activated. However, the PIV Card will be revoked if the background investigation results are negative for the employee/contractor. A credential may also be revoked at any time for just cause during the investigative process or thereafter and if a security event that has occurred that forces revocation of the PIV Card.

For employees and contractors hired prior to October 27, 2005, if the agency has maintained records indicating the NCHC investigative requirements (including fingerprint check) were completed for these individuals, and they were successfully adjudicated, then these employees and contractors will not need to complete a new NCHC. However, for any employees or contractors hired on or after October 27, 2005, agencies should maintain a copy of the prints (either the full set or just the two prints required by FIPS 201) so a biometric match may be conducted in the future as necessary. Additionally, as agencies implement their enrollment stations during FY2007 and FY2008, they must ensure these employees and contractors are in full compliance with FIPS 201-1 Section 4.4.1, particularly the requirement that fingerprints taken during the PIV enrollment action "shall be used for one-to-many matching with the database of fingerprints maintained by the FBI." This ensures that fingerprints taken during the same enrollment action are used for the PIV Card templates and the FBI NCHC of the Applicant.

If a person has had a "break in service" (i.e., left a job for which they had to be investigated to meet FIPS 201-1 requirements), of two years or more, a new investigation must be conducted before a PIV credential can be issued. In accordance with Executive Order 12968, if the break in

service is less than two years, an updated security questionnaire should be completed and any admitted issues resolved as appropriate.

See Appendix G, Appeal Rights for Denial of a Credential.

## 3.0 PCI Operations Certification and Accreditation

---

### 3.1 Introduction

The purpose of this section is to provide the GSA Certification Agent with sufficient information for a PIV certification and accreditation decision, which should include:

- The specific requirements for issuing PIV Cards
- The processes in place or planned for meeting the PIV Card requirements
- The supporting materials and identify management related documents, such as:
  - The PIV Card Issuer’s privacy policy for Applicants
  - Descriptions of management procedures for assuring continued reliable operations
  - All agreements with agencies regarding using the services of the PIV Card Issuer
- The Certification Agent Findings and Recommendations Summary

The MSO C&A team uses this PCI Operations Plan as input for establishing the reliability of the component organization with regard to the PIV requirements in FIPS 201-1. As defined in the SP 800-79, the reliability of a PIV Card Issuer is established by assessing that the organization meets the following required attributes, which are defined in greater detail in the SP 800-79:

- Knowledgeable
- Capable
- Accountable
- Available
- Legal
- Compliant
- Well Managed
- Trustworthy
- Adequately Supported
- Secure

Other attributes that are desired and should also be assessed are that the PIV Card Issuer is:

- Prepared/responsive/efficient
- Cost effective
- Adaptable

- Cooperative

### 3.1.1 Assessment / Methodologies

The certification agent will use, where applicable, the following assessment methodologies:

- **Review and Analysis**— broad methods of assessment that may be applied to most attributes but are best applied to reviewing documents (plans, policies, rules) and analyzing them in accordance with applicable standards.
- **Interview**— direct conversation with an assessment subject in which both pre-established and follow-on questions are asked, responses documented, discussion encouraged, and conclusions reached.
- **Demonstration/Observation**— a product producer or service provider showing an assessor how a product works or a service is performed.
- **Sampling/Statistics**— actively selecting relevant process information in accordance with a statistical sampling plan or equivalent in order to verify that the functions or services produced on an on-going basis also satisfy the initial requirements.
- **Evaluation/Measurement**— analyzing an attribute of a product, service, or organization using a metric or equivalent that is selected to produce a result useful for assessing quality and reliability.
- **Compliance/Conformance with Standards**— analyzing a product, service, or organization to determine if the specified standards are being followed appropriately.
- **Precedence/Accepted Practice**— assessing an attribute and deeming it acceptable because it has been successfully used previously by others or has been used so frequently that it has become a de facto standard.
- **Comparison with Peers**— assessing an attribute of a person or organization by comparing the result of an assessment with that of a similar person or organization; comparing the certification and accreditation documentation and results of one PCI against those of others to seek equivalence in operational capability and reliability and trust.
- **Experience**— assessing one or more attributes of an organization based on evaluating previously provided products or services similar or identical to those required by FIPS 201-1.
- **Testing/Validation**— actively testing a product or service against a set of specifications using applicable test methods and metrics; validation is testing against a standard.

### 3.1.2 Status

The MSO PCI operation is currently in the following status:

- N/A – Initial C&A Not Yet Performed

### 3.1.3 References

- FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors, National Institute of Science and Technology (NIST), March 2006
- SP 800-73-1 Interfaces for Personal Identity Verification, National Institute of Science and Technology (NIST) March 2006
- SP 800-76-1 Biometric Data Specification for Personal Identity Verification, National Institute of Science and Technology (NIST) January 2007
- SP 800-78 Cryptographic Algorithms and Key Sizes for Personal Identity Verification, National Institute of Science and Technology (NIST) April 2005
- SP 800-79 Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, National Institute of Science and Technology (NIST) July 2005
- Federal Identity Management Handbook, General Services Administration (GSA)
- OMB HSPD-12 Implementation Guidance, Office of Management and Budget (OMB)

## 3.2 SP 800–79 Assessment Report

### 3.2.1 Organization Description

The following section provides a detailed description of the MSO Card Issuer organization in relation to how it addresses the HSPD-12 requirements. Table 3-1: PIV Role Name and Personnel relates SP 800-79 Roles (PIV Role Name) with associated MSO roles and responsibilities. The following definitions are provided:

**Table 3-1: PIV Role Name and Personnel**

PIV Role Name	Role Description	Personnel/Responsible Organization(s)
PIV Applicant	The individual to whom a PIV credential needs to be issued.	Federal Employee, Contractor
PIV Sponsor	The individual who substantiates the need for a PIV credential to be issued to the Applicant and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant.	Sponsors will be Agency specific. The MSO will name an Agency specific role manager who will assign the sponsors and transmit that assignment to the MSO and the Shared Services to assign their roles.
PIV Registrar	The entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant.	Registrars will be divided into two groups. One group will be assigned by agencies depending on how the enrollment station shall be manned and will be Agency specific. The MSO manages that assignment to the system and has them properly provisioned as a registrar and able to assume that role after training and

PIV Role Name	Role Description	Personnel/Responsible Organization(s)
		<p>certification.</p> <p>Other registrars will be provided by the MSO contract and will be the responsibility of the MSO. The contractor shall insure these personnel are properly checked for background status, properly trained and certified, and capable to performing the registrar role.</p>
PIV Issuer	<p>The entities that performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The PIV Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.</p>	<p>The MSO is responsible for this task via oversight of the Shared Services contractor.</p>
PIV Digital Signatory	<p>The entity that digitally signs the PIV biometrics and Cardholder Unique Identifier (CHUID).</p>	<p>Entrust is the certified PKI SSP under the contract requirements.</p>
Privacy Representative	<p>The entity that ensures all privacy requirements have been complied with during the PIV implementation process.</p>	<p>The MSO is responsible for privacy roles within the system and for data integrity. Privacy issues within the Applicant population shall be brought to the specific Agency privacy personnel for resolution and to the MSO PM for MSO specific or coordination functions.</p>
PIV Card Applicant Representative	<p>The entity responsible for being an advocate for the Applicant. The PIV Card Applicant Representative will safeguard the privacy of Applicant and assist Applicants who have been denied a GSA PIV Card due to identity document issues.</p>	<p>The PIV Card Applicant Representative is supplied by the MSO Office within the Shared Services concept and jointly with the 42 commissions and Agency leads who have signed for the MSO.</p>
Facility Director and Facility PCI Manager	<p>These department roles are administrative in nature and provide a management and responsibility hierarchy for the GSA PCI certified organizations.</p>	<p>James Schoening is the Deployment Team Manager who will be interfacing with facility choices and requirements. He works for Michael Butler as the MSO PM.</p>
PIV Authentication Certification Authority	<p>The CA that signs and issues the PIV Authentication Certificate.</p>	<p>Entrust</p>
PIV Card Issuer Manager	<p>The individual responsible for ensuring that all the services specified in FIPS 201-1* are provided reliably and that PIV Cards are produced and issued in accordance with its requirements.</p>	<p>MSO Project Manager</p> <p>Michael Butler is the responsible entity for providing credentialing services IAW the FIPS to all member agencies.</p>

PIV Role Name	Role Description	Personnel/Responsible Organization(s)
	<p>* For the PIV-I C&amp;A, the focus of this role will be on the identity proofing and registration processes.</p>	
<p>Certification Agent</p>	<p>The individual, group or organization that has the appropriate skills, resources and competencies to perform certifications of a PIV Card Issuer.</p> <p>The Certification Agent will be assigned by GSA for validation of PCI.</p>	<p>GSA FAS CIO</p> <p>Casey Coleman as the FAS CIO and her agents, Anthony Konkwo and David Trczynski, are required to perform the MSO specific C&amp;A that is initially qualified by the GSA APL process.</p>
<p>PIV Adjudicator</p>	<p>The individual who verifies the status and applicability of the background check. Either for record purposes or to initiate the background investigation</p>	<p>Adjudicator</p>
<p>PIV Activator</p>	<p>The individual who verifies the PIV Cardholder and aids in provisioning of the credential</p>	<p>Activator</p>
<p>PIV Role Administrator</p>	<p>The individual who is the responsible official to assign roles within the PIV system and administrates the chain of trust within the Agency POV process.</p>	<p>Role Administrator</p>
<p>PIV Security Officer</p>	<p>The individual who oversees all PIV credentials within an organization and has the ability to revoke or suspend credentials based upon Agency or system policies. Acts as a liaison to inquiries on identity information.</p>	<p>Security Officer</p>
<p>PIV Card Applicant Representative</p>	<p>The individual who represents the interests of current or prospective Federal employee and contractors who are the Applicants for PIV Cards.</p>	<p>MSO provides this role for the Shared Services at a system level.</p> <p>All MSO Agencies have an HSPD-12 lead that are responsible for their individual credential processes and who convey their requirement within the MSO shareholder process. The agencies will assign their sponsors and the MSO will insure they are properly trained and certified.</p> <p>In the event that an applicant is refused a credential due to incomplete sponsorship or suitability, their recourse is the use the existing business processes within their organization to seek redress.</p> <p>If an applicant is not issued a credential due to a systems or configuration issue, it is the responsibility of the MSO to</p>

PIV Role Name	Role Description	Personnel/Responsible Organization(s)
		<p>address that issue and to expeditiously provide a credential within the mandates of HSPD-12.</p> <p>All MSO customers have a designated HSPD-12 lead coordinator who may aid any applicant in issues that arise from credential issuance.</p>
PIV Agency Official for Privacy	The individual who oversees privacy-related matters in the PIV system and should work with the PIV Card Applicant Representative to ensure that the rights of Applicants and PIV subscribers are protected.	<p>MSO provides a conduit for privacy concerns and coordinates with Agency specific privacy officers on any Privacy related inquiries.</p> <p>The MSO has filed a Systems of Record Notice (SORN) in the Federal Register to meet the needs of the service as well as performed a Privacy Impact Assessment (PIA) that covers all MSO customers.</p> <p>In the role of 'service' the MSO must meet all applicable laws and regulations and expeditiously respond to privacy requests by customer agencies and individual credential holders.</p> <p>The MSO will provide access to questions and inquiries via a portal at <a href="http://www.FedIDCard.gov">www.FedIDCard.gov</a>.</p>

The MSO credentialing organization consists of the MSO employees who manage the system and have roles that provide service across the entire Shared Services federation. As an Agency is brought into the Shared Services, the MSO manages the Agency configuration (unique topology and data concerns); validates the initial Agency roles and provides the vehicle for these personnel to receive their training, role assignments, and initial cards. In addition, MSO manages any unique Agency data requirements that may interface to the Shared Services with associated contractor interfaces. Specific MSO assignments are shown in Table 3-2: MSO PIV Roles Contact Information.

**Table 3-2: MSO PIV Roles Contact Information**

IV Role	Responsible Office	Employee Name			
		Name(s)	Office	Phone #	Email Address
Facility PCI Manager	GSA MSO	James Schoening	MSO	(202) 501-7367	<a href="mailto:Jim.schoening@gsa.gov">Jim.schoening@gsa.gov</a>
PIV Sponsor, Employee	GSA MSO	Lead SSP Sponsor Steven Duncan	MSO	(202) 219-0815	<a href="mailto:Stephen.duncan@gsa.gov">Stephen.duncan@gsa.gov</a>

IV Role	Responsible Office	Employee Name			
		Name(s)	Office	Phone #	Email Address
PIV Sponsor, Contractor	GSA MSO	Lead SSP Sponsor			
		Steven Duncan	MSO	(202) 219-0815	<a href="mailto:Stephen.duncan@gsa.gov">Stephen.duncan@gsa.gov</a>
PIV Sponsor, Volunteer/Affiliate	GSA MSO	Lead SSP Sponsor			
		Steven Duncan	MSO	(202) 219-0815	<a href="mailto:Stephen.duncan@gsa.gov">Stephen.duncan@gsa.gov</a>
PIV Registrar	GSA MSO	Lead SSP Registrar			
		Jim Schoening	MSO	(202) 501-7367	<a href="mailto:Jim.Schoening@gsa.gov">Jim.Schoening@gsa.gov</a>
PIV Issuer	GSA MSO	Lead SSP Sponsor			
		Steven Duncan	MSO	(202) 219-0815	<a href="mailto:Stephen.duncan@gsa.gov">Stephen.duncan@gsa.gov</a>
PIV-I Card Applicant Representative	GSA MSO	Mike Butler			
		MSO PM or Agency HSPD-12 Lead	MSO	(703) 772-0631	<a href="mailto:Michael.butler@gsa.gov">Michael.butler@gsa.gov</a>
Facility Privacy Official/Applicant Representative	GSA MSO	Mike Butler			
		MSO PM or Agency HSPD-12 Lead	MSO	(703) 772-0631	<a href="mailto:Michael.butler@gsa.gov">Michael.butler@gsa.gov</a>

### 3.2.2 Review, Analyze and Record Supporting Documents

#### 3.2.2.1 Defined Process and Policy Inventory

Table 3-3: Process and Policy Inventory, lists the applicable laws, directives, policies, regulations, and standards affecting the PIV Card Issuer operations.

**Table 3-3: Process and Policy Inventory**

Title	Brief Description/Purpose	Status	Author/Date
FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors	Being Applied	National Institute of Science and Technology (NIST), March 2006
SP 800-73-1	Interfaces for Personal Identity Verification	Being Applied	National Institute of Science and Technology (NIST) March 2006

Title	Brief Description/Purpose	Status	Author/Date
SP 800-76-1	Biometric Data Specification for Personal Identity Verification	Being Applied	National Institute of Science and Technology (NIST) January 2007
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	Being Applied	National Institute of Science and Technology (NIST) April 2005
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations	Being Applied	National Institute of Science and Technology (NIST) July 2005
Federal Identity Management Handbook	Implementation guide for government Agency credentialing managers	Being Applied	General Services Administration (GSA)
OMB HSPD-12 Implementation Guidance	Implementation guide for Federal Departments and Agencies	Being Applied	Office of Management and Budget (OMB)

The Certification Agent will be required to review the PCI documentation to assess standards compliance, planning, change management, equipment inventory, operations and life cycle management. Table 3-4: Document Inventory lists all documents reviewed by the Certification Agent. The documents listed in this table are viewed to provide an assessment.

**Table 3-4: Document Inventory**

Source Doc/ Version	Title	Date	Document Name
	Application for ID Card		
	C&A Vendor PIV System Overview		
	Concept of Operations		
	Configuration Management Plan		
	Contingency Plan		
	Standard Operating Procedures		
	System Design Documentation		
	Disaster Recovery Plan		
	Implementation Plan (Site Specific)		
	Information System Security Plan		
	Integrated Project Plan		
	Overview of PIV system		
	PIV System Software and Hardware		
	User Specification Guide		

### 3.2.3 PIV Sub-System Inventory

The PIV System is made up of four sub-systems that provide the functionality required to support PIV Card issuance and the business process and procedures necessary to perform the data capture, data management, identity proofing, identity management, access management, logical access control, physical access control, authorization, and authentication surrounding the PIV credential. Table 3-5: PIV Project System Inventory lists the PIV Project systems used by the PIV Card Issuer in performing the required services.

**Table 3-5: PIV Project System Inventory**

PIV Project System	Subsystem	Vendor/Provider
Card Management System (CMS)	Card Management System Smart Cards	Oberthur Card Systems
Public Key Infrastructure (PKI)	PKI Shared Service Provider Certificate Authority (SSP CA)	Entrust
Identity and Access Management (IAM)	Enrollment Identity Management Access Management Directory Services	EDS
Hosting Data Center	Hosting Information	Northrop Grumman

#### 3.2.3.1 PIV System Automated System Inventory

Table 3-6: Automated System Inventory lists systems used by the PIV Card Issuer in performing required services.

**Table 3-6: Automated System Inventory**

System Name	Purpose	System Owner Organization
MSO Shared Credentialing Service	Provides IDMS and Credential Services	MSO under contract to EDS
MSO PKI SSP	Provision PKI Credentials to MSO Shared Services Customers	MSO under contract to EDS

### 3.2.4 Observed PCI Demonstration and Performed Interview

A Certification Agent attended a demonstration of the PCI process and interviewed the Sponsor, Registrar and Activator. Table 3-7: PIV Card Enrollment Process presents the processes observed and represents a sample PCI process.

**Table 3-7: PIV Card Enrollment Process**

Step	Process Flow	New Federal Government Employee, Contractor, or Affiliate	Current Employee, Contractor, or Affiliate, but New to Facility	Current Federal Government Employee, Contractor, or Affiliate	Comments
1.	An Applicant is sponsored by an Agency Sponsor	X	X	X	Package includes ID proofing instructions, and investigation forms (i.e. e-QIP)
2.	Applicant is directed to bring identity documents to Registrar on enrollment day	X	X	X	
3.	If background check required, Sponsor has Applicant fill out investigation form	X	X	X	e-QIP will be used, if available
4.	Complete Applicant information and forward to Sponsor	X	X	X	
5.	Sponsor verifies authenticity of the information	X	X	X	
6.	Sponsor verifies Applicant's need for PIV Card	X	X	X	
7.	Sponsor forwards investigation form to OPM / SIC requesting a background check	X	X	X	
8.	OPM conducts background check	X	X	X	
9.	OPM sends back background check results (Adjudicator)	X	X	X	Adjudicator advises appropriate individuals (i.e. Sponsor, Registrar) of adjudication results

Step	Process Flow	New Federal Government Employee, Contractor, or Affiliate	Current Employee, Contractor, or Affiliate, but New to Facility	Current Federal Government Employee, Contractor, or Affiliate	Comments
10.	Sponsor completes sponsorship and forwards to Registrar	X	X	X	Documents delivered in a sealed enveloped to Registrar
11.	On enrollment day, Applicant presents I-9 documents to Registrar. Authenticity of documents verified by Registrar. Applicant is ID proofed by Registrar	X	X	X	Registrar proofs IDs for authenticity
12.	Registrar takes Applicant's photo	X	X	X	
13.	Registrar enters Applicant's identity information in the PIV system	X	X	X	
14.	Applicant is fingerprinted by Registrar (flat, ten prints)	X			Roll method is used at this time
15.	Employee reports to the PIV Card Enrollment Station	X	X	X	
16.	Activator verifies IDs of Applicant, confirms validity of received information from PIV Sponsor and validity of Registrar approval	X	X	X	
17.	Activator issues PIV Card to Applicant	X	X	X	

### 3.2.5 Process Flow Diagram

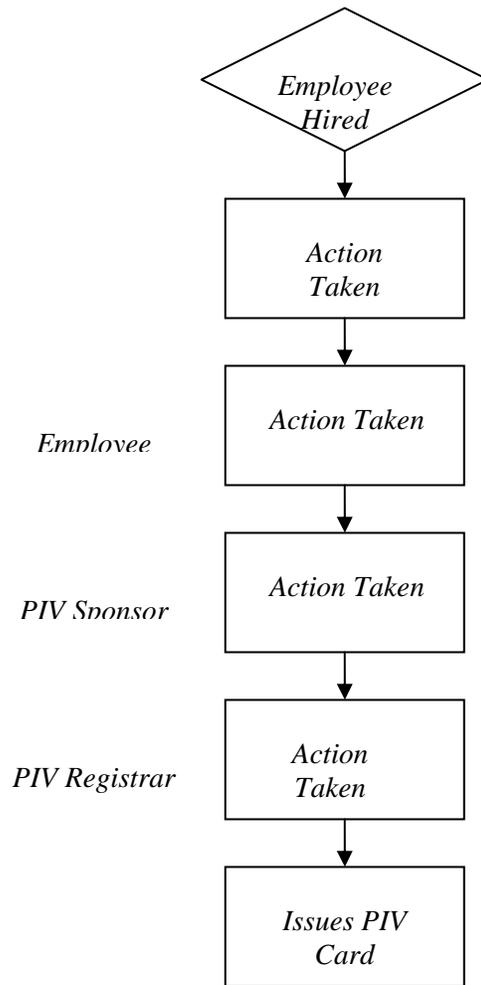


Figure 3-1: MSO PCI Process Flow Diagram

### 3.2.6 Perform SP 800-79 Attributes Assessment

The MSO C&A team (Certification Agent) uses the PIV 800-79 Certification Report as a written testimony for establishing the reliability of the MSO PIV Card Issuer (PCI) organization(s) with regard to the PIV issuing requirements described in FIPS 201-1 section 2.2. As defined in the NIST Special Publication (SP) 800-79, the reliability of a PIV Card Issuer is established by assessing that the PCI organization meets the following required attributes, which are defined in greater detail within SP 800-79. Table 3-8: PCI 800-79 Required Attributes provides a written account and assessment by the Certification Agent on how the PCI meets the requirements of SP 800-79.

**Table 3-8: PCI 800-79 Required Attributes**

Required Attribute	Description	Assessment
Knowledgeable	The characteristic of a person or organization of having both the ability and capacity of understanding all the management, documentation, document control, work flow, privacy, security, technical foundation, data, devices, communications, and electronic processing requirements in FIPS 201-1.	The Certification Agent performed numerous interviews of the knowledgeable PIV staff and EDS provided a demonstration of the PIV process from Registration through Issuance. The staff was certified to operate in their PIV role and performed duties as per MSO PIV policy, process and guidelines. Workflow, demonstration, and training align with FIPS 201-1.
Capable	The characteristic of a person or organization of possessing the management, personnel, facilities, equipment, funding, and technical abilities of performing the required services of FIPS 201-1 including development of a plan, initiation of required acquisitions and initiation of corrective actions as appropriate.	MSO has formed a PIV Program Management Office (organization) and PIV Card badging facility. Organizational roles and duties are clearly defined to support the FIPS 201-1 processes, roles and services. The current MSO roadmap defines the first stage of PIV compliance as production.
Accountable	The requirement of a person or organization for accepting responsibility for assigned tasks and then being held personally or organizationally responsible for performing the tasks successfully or for accepting the results of failing to accomplish them.	PIV Roles are clearly defined. Separation of duties and responsibilities are inherent. Each of the PIV roles requires training, certification and signatures to attest to their roles and responsibilities in implementing the PCI process.
Available	The characteristic that required functions and services will be performed, by the PCI, whenever desired by the consumer or customer.	The PCI office has set hours for PIV Card issuance. This is defined by each Agency. Shared stations are initially required to operate 8 hours daily. Leased stations operate based on Agency needs. The MSO will manage the hours across agencies to insure that personnel are properly serviced.

Required Attribute	Description	Assessment
Legal	The system is operating within all the applicable laws.	<p>The Integrated Project Team (IPT) meets on a consist basis. The team consists of representatives from Human Resources, Information Technology, Security and Law Enforcement, General Counsel, Privacy, Contracting, and MSO and GSA. The IPT supports the PMO by providing the internal subject matter experts required to support deployment of the PIV Solution. The responsibilities of the IPT include:</p> <ul style="list-style-type: none"> <li>Develop PIV policies, processes, and procedures</li> <li>Support design and deployment of technical solution</li> <li>Support integration of technical solution into MSO architecture</li> <li>Support deployment of PIV solution processes, procedures, and technology</li> </ul>
Compliant	The system is operating consistent with, and utilizing as required, all applicable policies, standards, rules, and regulations.	<p>The PCI Process adheres to the following:</p> <ul style="list-style-type: none"> <li>• 800-37 systems certification in progress</li> <li>• 800-53 (security controls)</li> <li>• 800-79 process</li> <li>• GSA System standards and guidelines</li> <li>• FIPS 201-1 standard &amp; associated NIST publications</li> </ul>
Well Managed	The system is processing the abilities needed to plan, initiate, coordinate, and provide services required by FIPS 201-1 with the cooperation and support of all its operations personnel and staff.	The PCI has developed documents to establish a well managed program to include the following: Project Management Plan, Concept of Operations, Deployment Plan, and Org Chart.
Trustworthy	The characteristic of a person or organization in which their statements may be accepted as being true without question and that their functions will be performed and services provided as advertised or expected.	All PIV Sponsors, Registrars, and Issuers are trained and certified to perform their respective roles, which require background checks and adjudication prior to certification.
Adequately supported	Having the personnel, facilities, equipment, finances, and support infrastructures needed to perform assigned duties and fulfill responsibilities.	PIV Project Management Plan is in place. PIV Project Oversight, Integrated Product Team, Deployment team and PIV Support in place.

Required Attribute	Description	Assessment
Secure	The characteristic of a person, organization, facility, or information system that safety, valuable asset protection, and sensitive and critical information assurance will be provided to the level desired and expected.	Currently, NIST SP 800-37 Certification & Accreditation is being performed on the PIV system. A PIV System Security Plan exists. The C&A includes a Risk Assessment, Vulnerability scan, System Controls Assessment (testing), System Security Plan updates, a Plan of Action and Milestones (POAM)

The NIST SP 800-79 includes other PIV Card Issuer attributes that are desirable and should be examined. The Certification Agent will perform an assessment of the additional attributes, as shown in Table 3-9: PCI-79 Desirable Attributes.

**Table 3-9: PCI-79 Desirable Attributes**

Desirable Attributes	Description	Status
Prepared/responsive/efficient	Characteristics of a person or organization exhibiting proper planning to be able to perform a service, capable of responding to it in a normal or expedited requests, and able to perform it without undue expenditure of time or resources.	
Cost effective	Characteristic of a product, service, person, or organization that the cost for obtaining a product or service or using a person or organization to perform a service is proportional to the value of the product or service.	
Adaptable	Able to change to exhibit new characteristics, perform new services, use new technology, and operate in new environments as requirements change.	
Cooperative	Characteristic of a person or organization to work with other people or organizations in performing a service without causing delay, anxiety, or frustration.	

### 3.3 Certification and Accreditation

This section describes the C&A phases and associated responsibilities and maps the phases to the 800-79 process.

#### 3.3.1 Initiation Phase

Task #	Title	Description	Responsibility	800-79 Process
1	Preparation	The objectives of this task are to prepare for certification and accreditation by reviewing the PCI Operations Plan and confirming that the plan is consistent with FIPS 201-1 and the provided services and operations comply with it.		
1.1		Confirm that the PCI system has been fully described and documented in the PCI Operations Plan.	PCI Manager	Review the PCI Operations Plan
1.2		Confirm that the applicability of the PCI's services and supporting automated system has been documented in the PCI Operations Plan and that it is not categorized as National Security.	PCI Manager	Review the PCI Operations Plan
1.3		Confirm that the PCI has adopted and will use approved identity proofing and registration processes as required in FIPS 201-1 and that all required roles, responsibilities, activities, and actions specified in the approved model (Role Based and System Based Models are pre-approved) are adequately documented in the PCI Operations Plan and are used for performing the required services.	PCI Manager	Review the PCI Operations Plan
1.4		Confirm that the PCI has adopted and will use approved PIV Card Issuance and Life Cycle maintenance procedures.	PCI Manager	Verified Concept of Operations (CONOPS)

2	Resource Identification			
2.1		Identify the DAA, AOP, Certification Agent(s), PIV Card Applicant Representative(s), and other interested Agency officials that are involved with Agency personal identity verification, identity badge management, physical and information system access control, and information security that will be providing certification and accreditation support.	PCI Manager	Representatives described in CONOPS and System Security Plan
2.2		Determine the resources required for the certification and accreditation of the PCI services and supporting automated system and prepare a plan of execution.	PCI Manager; DAA	
3	Operations Plan Analysis and Acceptance			
3.1		Reviews the list of desired attributes of a PCI described in these guidelines and selects those that should be exhibited by the PCI in addition to the required attributes in order to satisfy Agency requirements.	DAA; Certification Agent	Reviewed desired list of attributes and decided that all 4 attributes applied and are desirable and PCI process is compliant.
3.2		Select appropriate methods to assess the required and desired attributes of the PCI.	Certification Agent	The Certification Agent will use the following assessment methods:  <ol style="list-style-type: none"> <li>1. Review and Analysis</li> <li>2. Interview</li> <li>3. Demonstration</li> <li>4. Compliance with standards</li> </ol>

3.3		Analyze the PCI Operations Plan to determine if there are vulnerabilities that would result in not satisfying all the policies, procedures, and other requirements in FIPS 201-1 and of the Agency being serviced by the PCI if the plan was implemented properly and the specified operations performed as planned.	DAA, Certification Agent	PCI Operations Plan is incorporated into implementation and deployment guides. Certification Agent recommends the MSO PCI develop an independent Operations Plan.
3.4		Accept the PCI Operations Plan as acceptable.	DAA	DAA shall review final SP 800-79 report and cover letter.

### 3.3.2 Certification Phase

Task #	Title	Description	Responsibility	800-79 Process
4	PCI Services and Attribute Assessment			
4.1		Assemble all documentation and supporting materials necessary for the assessment of the PCI; if these documents include previous assessments, then review the findings, results, and evidence.	PCI Manager; Certification Agent	Gathered documents as inventoried in Tables 5 and 6.
4.2		Assess the required and desired attributes of the PCI using methods and procedures selected or developed.	Certification Agent	See Table 9 and Table 10.
4.3		Prepare the assessment report.	Certification Agent	Assessment Report prepared dated (TBD-DATE).
5	Certification Documentation			
5.1		Provide the PCI Manager with the certification report.	Certification Agent	Certification report prepared (TBD-DATE).
5.2		Revise the PCI Operations Plan.	PCI Manager	PCI Operations Plan to be developed per recommendations.

Task #	Title	Description	Responsibility	800-79 Process
5.3		Prepare the Corrective Action Plan (CAP).	PCI Manager	Corrective Actions are included in Summary and Findings section of the SP 800-79 Report.
5.4		Assemble the accreditation package and submit to DAA.	PCI Manager, Certification Agent	PCI Manager shall assemble the accreditation package and submit to the DAA.

### 3.3.3 Accreditation Phase

Task #	Title	Description	Responsibility	800-79 Process
6	Accreditation Decision			
6.1		Determine the risk to Agency operations, Agency assets, or individuals based on the PCI's vulnerabilities and the CAP and perform a final certification review.	DAA	DAA shall use this SP 800-79 Report to determine the risk to Agency operations.
6.2		Determine if the risk to Agency operations, Agency assets, or individuals is acceptable, that the required and desired attributes are exhibited as needed, that the reliability of the PCI has been adequately assessed, and prepare the final accreditation decision letter.	DAA	DAA shall determine risk to Agency operations and prepare final accreditation decision letter.
7	Accreditation Documentation			
7.1		Provide copies of the final accreditation package including the accreditation decision letter, in either paper or electronic form, to the PCI Manager and any other Agency officials having interests, roles, or responsibilities in the PIV System. A copy of the submittal letter and the selected authorization letter should be forwarded electronically to PIVaccreditation@nist.gov when they are delivered to the intended recipient.	DAA	DAA shall provide copies of the final accreditation package to the PCI Manager.

Task #	Title	Description	Responsibility	800-79 Process
7.2		Update the PCI Operations Plan.	PCI Manager	PCI Manager shall update the PCI Operations Plan.
8	PCI Management and Control			
8.1		Using established management and control procedures, document any changes that may be significant with respect to service offerings, PIV Card operations, or the PIV support automated system (including hardware, software, firmware, and surrounding environment).	PCI Manager	PCI Manager shall document significant changes.
8.2		Analyze the proposed or actual changes to the PCI (including hardware, software, firmware, and surrounding environment) services and operations and analyze them to determine the impact of such changes.	PCI Manager	PCI Manager shall analyze the proposed and/or actual changes.
9	PCI Status Monitoring			
9.1		Select the attributes of the PCI to be monitored.	PCI Manager	PCI Manager shall decide the attributes to be monitored.
9.2		Assess the required and selected desired attributes to determine the extent to which they are exhibited by the PCI in all aspects of providing services to the Agency and producing the desired outcome with respect to meeting the requirements specified in FIPS 201-1.	DAA, PCI Manager	DAA and PCI Manager shall assess the attributes to determine the desired outcome meets the requirements in FIPS 201-1.
10	Status Reporting and Documentation			
10.1		Update the PCI Operations Plan based on documented changes to the PCI operational requirements, personnel, facilities, equipment, and technology available to implement PIV systems and components and the results of the monitoring process.	PCI Manager	PCI Manager shall update the operations plan.

Task #	Title	Description	Responsibility	800-79 Process
10.2		Update the CAP based on the documented changes to the operations plan and the results of the monitoring process.	PCI Manager	PCI Manager shall update the CAP.
10.3		Report the status of the PCI to the DAA.	PCI Manager	PCI Manager shall report the status of the PCI to the DAA.

### 3.4 C&A Summary

The Certification Agent is focused on performing an assessment of the PCI FIPS 201-1, PIV-II services. The assessment methodologies performed by the Certification Agent included:

- Recorded the PCI Organization and Roles & Responsibilities
- Reviewed, Analyzed and Recorded the PCI supporting documents
- Observed the PCI demonstration and performed interviews
- Generated the PCI Process Flow Diagram
- Performed SP 800-79 PCI Attributes Assessment
- The MSO PCI has elected to implement the roles and responsibilities as set forth in FIPS 201-1 and NIST Special Publication 800-79. The PCI process includes supplemental roles that help facilitate and further ensure the integrity of the PCI process. In addition, the PCI exhibited the attributes defined in SP 800-79 and have been reviewed, assessed and listed by the Certification Agent in Section 2.7 of this PCI Operations Plan. In summary, the PCI satisfies the requirements of HSPD-12 and FIPS 201-1 PIV-1 for instituting a consistent, reliable and secure process for enrolling and issuing identity cards to approved applicants (federal employees and contractors).
- GSA senior management participation is an integral part of the success and implementation of the PIV solution. The PCI Manager and staff are knowledgeable (trained and certified), showed exemplary confidence during the PCI demonstration and understand the requirements as set forth in HSPD-12 and FIPS 201-1. The PCI processes are implemented as designed and is adequately documented in the PCI Program Management Plan, Implementation Plan and Concept of Operations.
- The PCI implementation ensures more complete, reliable, and trusted identification of individuals for controlling access to Federal physical facilities and information systems.

## 4.0 Supporting Documentation

---

### 4.1 PIV Implementation Guidance

#### 4.1.1 Introduction

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

HSPD-12 requires that all government agencies develop specific and consistent standards for both physical and logical identification systems. The National Institute of Standards and Technology (NIST) published FIPS 201-1 to establish detailed standards on implementing processes and systems to fulfill the requirements of HSPD-12. This Operations Plan addresses the Personal Identity Verification (PIV) requirements of FIPS 201-1. The 2002 Federal Information Security Management Act (FISMA) does not permit waivers to the FIPS 201-1 standards. Additional supporting information related to FIPS 201-1 compliant MSO operations are presented in the following sections.

#### 4.1.2 Card Production

##### 4.1.2.1 Process Overview

Enrollment records are sent to the Card Production Facility after each enrollment record has successfully passed through the various security checks. The Card Production Facility is Oberthur. An Oberthur employee will initiate the PIV Card personalization, printing, and chip encoding processes. Before the PIV Cards are shipped back to the enrollment workstation location (per shipping model), the Oberthur employee inspects the quality of each card. If the quality of the PIV Card meets acceptable standards, the Oberthur employee securely packages and ships the PIV Cards in batches to the designated agency official via a courier service.

##### 4.1.2.2 Actors

The following participants are involved in the Card Production process:

- **Card Production Facility Employee:** An employee of the card production facility that is responsible for managing the card production process.
- **Courier:** A service that securely transports the PIV Cards to the enrollment center's designated agency official.

#### **4.1.2.3 Process Description**

Once an applicant has successfully passed the required security checks, the MSO HSPD-12 Shared Service Solution system automatically and securely transmits a card production file to the Card Production Facility. The card production facility uses this file to produce and personalize the card. Once PIV Cards have been produced, the CPF employees are responsible for securely packaging the cards and shipping them back to the appropriate enrollment sites. The CPF employee also sends a message to the Card Management System (CMS) notifying it of the PIV Cards that have been produced.

#### **4.1.3 Expiration Date Requirements**

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

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

New employees and new contractors must be issued PIV-II credentials beginning October 2008.

For individuals who have been Federal department or agency employees over 15 years, a new investigation and PIV credential issuance may be delayed, commensurate with risk, but must be completed no later than October 27, 2008.

#### **4.1.4 Audits and Records Management**

The Office of the Inspector General (OIG) has responsibility for auditing identity proofing and registration records. As such, all agencies should be prepared for such reviews. Agencies must comply with MSO "Records Disposition Management", the creation, maintenance, use, and disposition of all records associated with the PIV-II process.

#### **4.1.5 Reporting Requirements**

Beginning March 1, 2007 and each quarter thereafter, MSO will post to their federal agency public website a report on the number of PIV credentials issued. The GSA Managed Services Office will ensure all reporting requirements are met and provided to senior MSO managers and the DAA along with the HSPD-12 Executive Steering Committee. These are the required documents:

1. Audit Reports allow real time access to monitor, reconcile, and audit system processing.
2. Program Management Reports provide information that can be used to manage the organization's PIV services, supplied in the form of regular management reports to the program office. A sub-category of the management reports are administrator reports. Administrator reports are internally accessed web queries that allow role based users to access information needed to perform their duties within the system.

3. System Performance Reports are comprised of metrics collection and monitoring data that are useful for understanding consumer trends, inventory flow, and credential use information.
4. Security Reports provide status updates and results of monitoring activity and collect information that will assist in the detection of fraud and ensure system security.

## 4.2 Training

### 4.2.1 Training Sources

The USAccess Training Team can choose from a variety of training options to fulfill contract requirements. These options may include:

- Instructor-led classroom training (ILT)
- Virtual Instructor-led training via WebEx
- Self-paced, Web-based training (WBT)
- Provision of Training Scripts and Job aids

The USAccess Training Team will use self-paced, Web-based Training (WBT) to deliver training for the seven PIV roles. The WBT will be housed on a GSA government approved Learning Management System (LMS).

### 4.2.2 Instructor-Led Training

Instructor-led training classes employ a variety of materials and techniques to create an engaging experience for learners. Learning strategies include presentation, lecture, hands-on exercises, small group discussion, guided tours, WBT use, and software demonstrations using realistic training environments.

EDS Instructional Systems Designers (ISDs) rely on Learning and Development industry best practices to develop and deliver effective and engaging training solutions. The ADDIE model, which stands for Analyze, Design, Develop, Implement, and Evaluate, guides our instructional design approach. Original content will be developed in collaboration with subject matter experts (SMEs) to ensure consistency with all NIST documentation standards.

The EDS project team including EDS employees, its in-house consultants, Northrop Grumman Technical Consultants, and Help Desk Agents will be initially trained using ILT. Since the WBTs will not be available until after the first group of L1 Registrars are deployed, this group may also receive classroom instruction.

Since many of EDS' accounts include Help Desk services, a thorough soft skills curriculum is in place for EDS help desk agents. This course work includes telephone courtesy, empathy, active listening, troubleshooting as well as trouble documentation and resolution content.

### 4.2.3 Virtual Classroom/Web Seminar Training

Instructor-led training, as described above, can also be delivered to the learner in a virtual classroom via WebEx, Live Meeting or a similar product. With careful planning, this delivery option can rival the effectiveness of classroom training. Some considerations for using web seminar training follow:

- **Class length** is an important consideration since participants are usually less willing to sit in front of a computer all day than in a classroom. Breaking the instruction up into a maximum of two hour increments is recommended. Class lengths vary according to the number of questions and the class size. Hands-on practice sessions run longer than refreshers or demonstrations.
- **Course Content** should be confined to a single procedure or a related series of procedures. Learners should be able to identify the procedure to be discussed and elect to take the desired class.
- **Media Use** should be varied for web seminar training. The platform offers an environment where the software application can be demonstrated, movies and animation can be played, PowerPoint presentations can be viewed, and text can be read. Interaction is accomplished using the polling, questions, chat, application sharing, and whiteboard features within the virtual classroom. Additionally, audio conferencing can be simulcast so that an instructor's voice can narrate activities. Using a variety of media increases the participants' emersion in the content and helps to keep them engaged for longer time periods. Use of varied media can also allow longer presentations to be successfully conducted.

The USAccess Training team may use web seminar training to refresh skills or retrain audiences to stay up to date with technical advances. This delivery option will be used where geographic distance or a limited number of participants makes conducting live classroom training impractical. Web seminar training can be an effective delivery option for retraining and/or personnel changes through attrition.

### 4.2.4 Web-based Training

The Web-based training (WBT) will fulfill standards described in Section 508 of the US Rehabilitation Act.

The program's WBT can be described with the following additional characteristics:

- Self-spaced, user controlled
- Level 2 Interactivity as defined by The U.S. Department of Defense DOD in "Department of Defense Handbook: Development of Interactive Multimedia Instruction (IMI)."
- Includes embedded video clips
- Includes audio track

Leveraging existing material EDS employees educated and experienced in ISD will direct the training development effort. These employees will be supplemented by onsite consultants specializing in related disciplines needed intermittently to execute production tasks.

Original content development, storyboarding, and training will be carried out by EDS employees and their consultants supported by media and programming services externally performed by our vendors. HP Productions, Inc. is a certified small/minority/woman-owned business specializing in media production whose clients include FDIC, Department of Defense, FBI, U.S. Coast Guard and the Department of Justice Integrated Performance Systems (IPS) offers leading-edge eLearning technology and courseware, and is currently engaged in creating e-learning supporting EDS Assured Identity™.

In lessons where skill acquisition is planned, participants will be presented with an explanation and a demonstration of the skill. Hands-on time will be allocated to allow the participants to practice the newly acquired skill. (Note: Quantity of practice time is contingent upon the number of systems set up in the classroom. At this point, the classroom set up is assumed to have at least one complete system.) Full feedback and coaching will be provided at the end of the practice exercises. Table 4-1: WBT Working Titles provides working titles for the WBT for the MSO HSPD-12 program.

**Table 4-1: WBT Working Titles**

WBT Working Title	Estimated Duration	Description
GSA PIV Sponsor Training	40 minutes	Includes audio, screen shots, and swf movies of the application.
GSA PIV Registrar Training	60 minutes	Includes audio, screen shots, swf movies, and video
GSA PIV Adjudicator	30 minutes	Audio, screen shots, swf movie
GSA PIV Activator Training	30 minutes	Includes audio, screenshots, swf movies, maybe some video
GSA PIV Security Office Training	40 minutes	Includes audio, screen shots, swf movies
GSA PIV Role Administrator Training	20 to 30 minutes	Includes, audio, screen shots, swf movies
GSA PIV Credential Holder Training	15 minutes	Includes audio, screen shots, and video

#### 4.2.5 Learners Roles and Responsibilities

All training modules shall monitor, track, and certify role mastery and cap the training experience with a certification exam. The certificate must be reported across the system to the

MSO and it must be electronically reported in print to the individual agency lead. The training requirements, by role, are assigned in Table 4-2: WBT Roles and Responsibilities.

**Table 4-2: WBT Roles and Responsibilities**

Role	Responsibility
Sponsor	Initiates the Pre-enrollment process Manages the applicant's account Approves/Denys an applicant's application
Registrar	Verifies the claimed identity of the applicant Validates the entire set of identity source documents presented at the time of registration Updates biographical information Collects biographical documents Captures photo Captures biometric information Explains privacy and security policies to the applicant
Adjudicator	Reviews the decision in the completed background check Records whether an applicant has been approved or denied for a Personal Identity Verification (PIV) card
Activator	Manages secure storage and deployment of printed PIV Cards Verifies the data on the screen and on the PIV Card matches the applicant present Verifies the identity documents presented match the scanned documents Validates applicant's primary and secondary fingerprints Encodes and activate the PIV Card Tests the PIV Card Instructs the applicant on use, privacy, and security of PIV Card
Security Officer	Performs auditing and reporting Vets services to resolve impersonation conflicts Performs PIV Card and certificate suspensions/reactivations/and revocations
Role Administrator	Creates and manages role accounts for the designated Agency
PIV Card User	Uses the PIV Card for physical and logical access Maintains the integrity of the PIV Card with regard to Agency and HSPD-12 privacy and security standards
Help Desk Agent	Handle and process calls from system role holders Handle email inquiries from end users
Installers (onsite technicians)	Certifies that all equipment is setup and functioning properly Credentialing center layout meets all room and privacy requirements

Role	Responsibility
	<p>Certifies that the Registrar is fully trained and has full access to the credentialing center</p> <p>Certifies that there is properly placed building signage designating the center location</p>

### 4.3 GSA Technical Requirements for Managing Roles

Beginning with the review of Role Administrator, technical requirements in Table 4-3 identifies the interactions and policies enforced for the GSA defined role structure. In addition, the technical requirements for the various role categories are presented in Table 4-3 along with their respective Workflow Use Cases, and descriptive Web Applications, where applicable. *The Technical Requirements listed in the table below follows the HSPD-12 Technical Requirements documented in the RFQ GSA HSPD-12 Shared Services Provider II, section 6.2.*

**Table 4-3: Implementing Technical Requirements for Managing Roles**

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
<b>Role Administration</b>			
7	Hierarchical system role administration structure shall be implemented to provide an MSO System Role Admin role with oversight and account administration responsibilities over both System Sponsor and Adjudicator roles as well as Agency Role Administrators. Agency Role Administrator manages Agency Sponsor, Adjudicator, Activator, and Security roles.	Standard System Implementation with Hierarchical Structure and Separation of Duties	Role administration is implemented for all Web Interfaces
9	System compartmentalizes role account administration by Agency Affiliation. a. The Agency Role Account Administrators Officer can only create and manage accounts for his/her agency. b. The System Role Account Administrator can create and manage accounts across agencies.	Standard System Implementation with Hierarchical Structure and Separation of Duties	Role administration is implemented for all Web Interfaces
27	New federal employees and non-federal employees shall be entered into the System by individuals in a Government designated sponsor role.	Standard System Implementation with Hierarchical Structure and Separation of Duties	Role administration is implemented for all Web Interfaces

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
	<p>a. Role administration hierarchy enforces the condition that Sponsors for a given agency can only be created and managed by the Agency Role Administrator. The Agency Role Administrator shall only be created by the System Role Administrator.</p>		
<b>Sponsorship Roles and Responsibilities</b>			
<p><b>General Conditions: All persons performing the functions of sponsorship, enrollment, or adjudication, will authenticate to the EDS GSA HSPD-12 system with a PIV II credential.</b></p>			
8	<p>System shall compartmentalize access to records by agency and/or role.</p> <p>b. Sponsors can only create and modify sponsorship records in their designated Agency.</p>	Hierarchical Structure and Separation of Duties	Sponsor web interface allows Agency Sponsors to manually create and/or update sponsored records in the IDMS component of the SIP
27	New federal employees and non-federal employees shall be entered into the System by individuals in a Government designated sponsor role.	12.1.3.1 Sponsor Applicant	Sponsor web interface allows Agency Sponsors to manually create and/or update sponsored records in the IDMS component of the SIP
28	<p>System shall provide update functionality for existing applicants' records.</p> <p>a. Sponsors for a given agency shall have visibility to all applicant/user records for their agency through Sponsor web interface.</p> <p>b. Sponsors can modify data attributes to existing records through Sponsor web interface or Agency/HR-LOB web service interface or other agency approved methods / organization.</p>	12.1.3.2 Update Applicant Sponsorship Information	Sponsor web interface allows Agency Sponsors to manually create and/or update sponsored records in the IDMS component of the SIP
32	<p>Sponsor search capability shall initiate the sponsorship process in the system. Search function shall be performed for all applicants:</p> <p>System shall provide Sponsor with</p>	12.1.3.2 Update Applicant Sponsorship Information	Sponsor web interface allows Agency Sponsors to manually create and/or update sponsored records in the IDMS component of the SIP

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
	<p>applicant search capability.</p> <p>i. If Applicant does not exist (new applicant) the system shall display blank sponsorship fields.</p> <p>1. System shall provide new applicant data entry and save functionality.</p> <p>ii. If Applicant already exists in the system:</p> <p>1. If Applicant is affiliated with Agency within the requesting Sponsor's scope, the system shall provide update functionality for existing applicant attributes.</p> <p>2. If Applicant is not affiliated with Agency within the requesting Sponsor's scope, the system shall not display existing agency relationship information but shall allow additional sponsorships.</p>		
38	System shall prevent a previously enrolled applicant from additional enrollment unless the Agency Sponsor or Security Officer specifically allows reenrollment.	12.6.3.4 Card Re-issuance or Card Reprint flows	Sponsor web interface allows Agency Sponsors to manually create and/or update sponsored records in the IDMS component of the SIP
<b>Registrar Enrollment Roles and Responsibilities</b>			
<b>General Conditions: All persons performing the functions of sponsorship, enrollment or adjudication, will authenticate to the EDS GSA HSPD-12 system with a PIV II credential</b>			
36	Mutual role exclusivity shall be enforced, except that Registrar can perform a secondary role as Activator in the System.	12.2.3 Enrollment Flow	Registrar web interface allows Agency Registrars to manually update enrollment information in sponsored records in the IDMS component of the SIP
37	Registrar shall verify that the enrolling applicant is sponsored and System shall prevent enrollment unless a sponsored record for the applicant exists.	12.2.3 Enrollment Flow	Registrar web interface allows Agency Registrars to manually update enrollment information in sponsored records in the IDMS component of the SIP
45	System shall provide the capability for Registrar to search applicant	12.2.3 Enrollment Flow	Registrar web interface allows Agency Registrars to

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
	records.		manually update enrollment information in sponsored records in the IDMS component of the SIP
51	The primary and secondary fingerprints shall be automatically segmented from the 10 finger slap.  c. Enrollment Station shall require Registrar to certify missing or damaged fingers and shall require confirmation by the Activator.	12.2.3 Enrollment Flow	Registrar web interface allows Agency Registrars to manually update enrollment information in sponsored records in the IDMS component of the SIP
58	Registration packages shall be digitally signed by the Registrar using the PIV Card, and the digital signature shall be validated prior to acceptance by the System.	12.2.3 Enrollment Flow	Registrar web interface allows Agency Registrars to manually update enrollment information in sponsored records in the IDMS component of the SIP
<b>Adjudication Roles and Responsibilities</b>			
<b>General Conditions: All persons performing the functions of sponsorship, enrollment or adjudication, will authenticate to the HSPD-12 system with a PIV II credential</b>			
8	System shall compartmentalize access to records by agency and/or role.  c. Adjudicators can only create or modify adjudication records for their designated Agency.	Hierarchical Structure and Separation of Duties	Adjudicator web interface allows Agency Adjudicators to manually update adjudication information in sponsored records in the IDMS component of the IDMS
59	System shall allow authorized Adjudicators to create and modify applicant adjudication records. Adjudication is related to an identity record, not an Agency relationship. Therefore, only one Agency may adjudicate a given background investigation level.  a. Upon receipt of any adjudication results, an Agency Adjudicator can manually input an applicant's adjudication status (positive or unsuccessful adjudication) directly into the HSPD12 system through the provide web interface.  b. Upon receipt of any adjudication results, an Agency Adjudicator can	12.3.3 Adjudication Flow  12.6.3.2 Revoke and Destroy PIV Card Flow	Adjudicator web interface allows Agency Adjudicators to manually update adjudication information in sponsored records in the IDMS component of the IDMS

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
	input an applicant's adjudication status (positive or unsuccessful adjudication) into an HR system that programmatically feeds the Shared Service IDMS through the HR Web Service interface		
<b>Security Officer Roles and Responsibilities</b>			
8	<p>System shall compartmentalize access to records by agency and/or role.</p> <p>a. Agency Security Officers can access records only for his/her designated agency</p> <p>e. Only the System Security Officers can access all records</p>	Hierarchical Structure and Separation of Duties	<p>Security Officer web application provides three discrete functions:</p> <p>Auditing and reporting capabilities for monitoring Shared Service activities. Visibility is scoped to the Security Officer's Agency.</p> <p>Vetting services to resolve impersonation conflicts during the one-to-many impersonation check.</p> <p>PPIV Card and Certificate suspension/ reactivation/and revocation capabilities.</p>
10	<p>Audit logs shall support forensic and system management capabilities, with the minimum capability to reconstruct role-holder events.</p> <p>a. Only Security Officers shall have access to System logs.</p> <p>b. Only the System Security Officers shall have visibility to all logs.</p> <p>c. Agency Security Officers shall have access to System logs relevant to activities specific to their agency. Agency Security Officers may only see events tied to applicants sponsored by that agency.</p>	Hierarchical Structure and Separation of Duties	<p>Security Officer web application provides three discrete functions:</p> <p>Auditing and reporting capabilities for monitoring Shared Service activities. Visibility is scoped to the Security Officer's Agency.</p> <p>Vetting services to resolve impersonation conflicts during the one-to-many impersonation check.</p> <p>IV Card and Certificate suspension/reactivation/and revocation capabilities.</p>
11	All transactions and events shall be logged for auditing purposes and made available to designated government representatives on-	Hierarchical Structure and Separation of	Security Officer web application provides three discrete functions:

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
	<p>demand.</p> <p>a. Only Security Officers shall have access to audit logs.</p> <p>b. Only the System Security Officers shall have visibility to all logs.</p> <p>c. Agency Security Officers shall only have access to audit logs relevant to activities specific to their agency.</p>	Duties.	<p>Auditing and reporting capabilities for monitoring Shared Service activities. Visibility is scoped to the Security Officer's Agency.</p> <p>Vetting services to resolve impersonation conflicts during the one-to-many impersonation check.</p> <p>PIV Card and Certificate suspension/reactivation/and revocation capabilities.</p>
18	System shall provide an authenticated Agency Security web interface for designated Agency security officials to provide card lock/unlock, PIN set/reset, card suspension, card revocation, card renewal, agency role management, and enrollment security event services.	<p>12.4.3 Issuance Flow</p> <p>12.6.3 Credential Usage Flows</p>	
33	The system shall provide the ability to process a flag set during Enrollment to alert the MSO Security Officer if fraudulent source documents or variables are suspected. The System shall prevent a card from being printed until the MSO Security Officer resolves the issue or invalidates the enrollment.	12.6.3.1 Suspend PIV Card Flow	<p>Security Officer web application provides three discrete functions:</p> <p>Auditing and reporting capabilities for monitoring Shared Service activities. Visibility is scoped to the Security Officer's Agency.</p> <p>Vetting services to resolve impersonation conflicts during the one-to-many impersonation check.</p>
38	System shall prevent a previously enrolled applicant from additional enrollment unless the Agency Sponsor or Security Officer specifically allows reenrollment.	12.6.3.4 Card Re-Issuance	<p>PIV Card and Certificate suspension/reactivation/and revocation capabilities.</p>
67	The contents of the pre-issuance package shall be hashed and compared against the post-issuance package data elements. All variances shall be logged and alerts shall be transmitted to designated government representatives. Card activation shall be blocked until the System Security Officer resolves the issue	12.4.3 Issuance Flow	<p>Security Officer web application provides three discrete functions:</p> <p>Auditing and reporting capabilities for monitoring Shared Service activities. Visibility is scoped to the Security Officer's Agency.</p>

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
127	<p>and approves activation continuance.</p> <p>All System components shall be protected with centrally managed endpoint security agents that persistently detect modification of critical files and fire real-time security alerts if the security profile is illegitimately modified.</p> <p>a. Solution shall allow rollback capability to last known good state if approved by MSO Security Officer.</p> <p>b. Solution shall provide detailed data to allow MSO Security Officer to determine specifics of file modification event.</p>	12.6.3.3 Reactivate PIV Card Flow	<p>Vetting services to resolve impersonation conflicts during the one-to-many impersonation check.</p> <p>PIV Card and Certificate suspension/reactivation/and revocation capabilities.</p>
<b>Card Activation Roles and Responsibilities</b>			
8	<p>System shall compartmentalize access to records by agency and/or role.</p> <p>d. Activators are not agency-bound; any Activator can activate any System PIV Card.</p>	Hierarchical Structure	Activator web interface allows Agency-designated Activator role-holders to activate and unlock PIV Cards
51	<p>The primary and secondary fingerprints shall be automatically segmented from the 10 finger slap.</p> <p>c. Enrollment Station shall require Registrar to certify missing or damaged fingers and shall require confirmation by the Activator.</p>	12.2.3 Enrollment Flow	
92	<p>A secure activation service web page shall be provided</p> <p>c. The applicant to whom the credential is to be issued (and on whom the background investigation was completed) shall be confirmed to be the intended applicant/recipient as approved by the appropriate authority as follows:</p> <p>i. Attended Activation</p> <p>1. The Activator authenticates to</p>	12.5.3 Activation Flow	Activator web interface allows Agency-designated Activator role-holders to activate and unlock PIV Cards

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
	the Activation system		
92	<p>A secure activation service web page shall be provided</p> <p>c. The applicant to whom the credential is to be issued (and on whom the background investigation was completed) shall be confirmed to be the intended applicant/recipient as approved by the appropriate authority as follows:</p> <p>i. Attended Activation</p> <p>3. The applicant provides the primary fingerprint using the biometric reader for a 1:1 match in the IDMS database. Upon successful match:</p> <p>a. Biometric authentication override function is available to Activator to support activation for applicants declared by the Registrar to have no suitable fingerprints during enrollment.</p>	12.5.3 Activation Flow	Activator web interface allows Agency-designated Activator role-holders to activate and unlock PIV Cards
92	<p>A secure activation service web page shall be provided</p> <p>c. The applicant to whom the credential is to be issued (and on whom the background investigation was completed) shall be confirmed to be the intended applicant/recipient as approved by the appropriate authority as follows:</p> <p>i. Attended Activation</p> <p>6. Applicant performs a 1:1 biometric match of the primary fingerprint against the biometric loaded on the Applicant's PIV Card.</p> <p>a. Biometric authentication override function is available to Activator to support activation for applicants declared by the Registrar to have no suitable fingerprints during</p>	12.5.3 Activation Flow	Activator web interface allows Agency-designated Activator role-holders to activate and unlock PIV Cards

Technical Requirement Number (Para. 6.2)	Technical Requirement	Workflow Use Cases	Web Applications
	enrollment.		
<b>Card Holder Roles and Responsibilities</b>			
53	The Enrollment Station shall require the Applicant to test and validate the segmented primary and secondary fingerprints by live sample comparison against the created minutiae to ensure that the templates will work when put on the card.	12.2.3 Enrollment Flow	Cardholder Support Services – provides a single point-of-entry to PIV Cardholders for support services including PIN unblocking, PIN set/reset, and FAQ.
92	<p>(Unattended Activation)</p> <p>A secure activation service web page shall be provided</p> <p>c. The applicant to whom the credential is to be issued (and on whom the background investigation was completed) shall be confirmed to be the intended applicant/recipient as approved by the appropriate authority as follows:</p> <p>i. Attended Activation</p> <p>2. The Applicant docks his/her PIV Card into the biometric card reader.</p> <p>3. The applicant provides the primary fingerprint using the biometric reader for a 1:1 match in the IDMS database.</p> <p>4. The applicant sets his or her PIN (6 to 8 digits in length).</p> <p>6. Applicant performs a 1:1 biometric match of the primary fingerprint against the biometric loaded on the Applicant's PIV Card.</p> <p>7. The PIV authentication key, digital signature key, and card management key shall be generated and these certificates and the key management key certificate shall be created and loaded on the PIV Card.</p>	12.5.4 Unattended Activation	Cardholder Support Services – provides a single point-of-entry to PIV Cardholders for support services including PIN unblocking, PIN set/reset, and FAQ.

<b>Technical Requirement Number</b> <b>(Para. 6.2)</b>	<b>Technical Requirement</b>	<b>Workflow Use Cases</b>	<b>Web Applications</b>
	<p>a. System shall require applicant's digital signature of card receipt/subscriber agreement.</p>		
<p>92</p>	<p>(Unattended Activation)                      A secure activation service web page shall be provided</p> <p>c. The applicant to whom the credential is to be issued (and on whom the background investigation was completed) shall be confirmed to be the intended applicant/recipient as approved by the appropriate authority as follows:</p> <p>ii. Unattended Activation</p> <ol style="list-style-type: none"> <li>1. The Applicant docks his/her PIV Card into the biometric card reader.</li> <li>2. The Applicant enters their one-time Activation PIN to authenticate to the Activation system.</li> <li>3. The applicant provides the primary fingerprint using the biometric reader for a 1:1 match in the IDMS database. Upon successful match:                             <ol style="list-style-type: none"> <li>a. The applicant sets his or her PIN (6 to 8 digits in length).</li> </ol> </li> <li>4. Applicant performs a 1:1 biometric match of the primary fingerprint against the biometric loaded on the Applicant's PIV Card.</li> <li>6. System shall require applicant's digital signature of card receipt.</li> </ol>	<p>12.5.4                      Unattended Activation Flow</p>	<p>Cardholder Support Services – provides a single point-of-entry to PIV Cardholders for support services including PIN unblocking, PIN set/reset, and FAQ.</p>

<b>Technical Requirement Number</b> <b>(Para. 6.2)</b>	<b>Technical Requirement</b>	<b>Workflow Use Cases</b>	<b>Web Applications</b>
108	<p>System shall provide cardholders with the ability to lock and unlock their PIV Card and certificates as a mitigation strategy in the event a user loses control of their PIV Card.</p> <p>a. User-initiated card locking/unlocking capability requires strong authentication to mitigate a Denial of Service attack vector.</p>	12.6.1.5 PIN Unlock	Cardholder Support Services – provides a single point-of-entry to PIV Cardholders for support services including PIN unblocking, PIN set/reset, and FAQ.

## Appendix A – Terms And Acronyms

Acronym	Definition
ALC	Account Lookup Code
BI	Background Investigation
C&A	Certification and Accreditation
CA	Certificate Authority
CAP	Corrective Action Plan
CHUID	Cardholder Unique Identifier
CM	Configuration Management
CMS	Card Management System
CONOPS	Concept of Operations
CPF	Card Production Facility
DAA	Designated Approval Authority
DCII	Defense Clearance and Investigations Index
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Department of State
EDS	Electronic Data Systems
EO	Executive Order
e-QIP	Electronic Questionnaire for Investigations Processing
FAQ	Frequently Asked Questions
FBI	Federal Bureau Investigation
FBI FP	FBI National Criminal History Fingerprint
FICC	Federal Identity Credential Committee
FIPS	Federal Information Processing Standards
GOCO	Government Owned/Contractor Operated
GSA	General Services Administration
HR	Human Resources
HR-LOB	Human Resource Lines-of-Business
HSPD - 12	Homeland Security Presidential Directive #12
IAM	Identity and Access Management
IDMS	Identity Management System
INS	Immigration & Naturalization Service

Acronym	Definition
IPT	Integrated Project Team
LACS	Logical Access Control System
MSO	Managed Services Office
NCHC	[FBI] National Criminal History Check (i.e., National Agency Check [NAC])
NACI	National Agency Check with Written Inquiries
NIST	National Institute of Standards and Technology
OHR	Office of Human Resources
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPAC	Office of Payment and Collections
OPM	Office of Personnel Management
OVI	Optical Variable Ink
PACS	Physical Access Control System
PCI	PIV Card Issuer
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Phase 1
PIV-II	Personal Identity Verification – Phase 2
PKI	Public Key Infrastructure
POAM	Plan of Action and Milestone
SII	Security/Suitability Investigations Index
SOI	Submitting Office Identifier
SON	Submitting Office Number
SORN	System of Record Notice
SSO	System Security Officer
SP	Special Publication
SSP	Shared Service Provider
TBD	To Be Determined
QA	Quality Assurance

## Appendix B – Definitions

---

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

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

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

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

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

**Contractor** – see “Employee”.

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

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

**FBI FP Check** – National Criminal History Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI.

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

**Identity-proofing** – the process of providing identity source documents (e.g., driver’s license, passport, birth certificate, etc.) to a registration authority, or the process of verifying an individual’s information that he or she is that individual and no other. FIPS 201-1 requires that

one of these documents be an original State or Federal Government-issued photo ID, and the other be from the approved set of identity documents listed on Form I-9.

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

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

**National Agency Check with Inquiries (NACI)** – the basic and minimum investigation required of all Federal employees and contractors consisting of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

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

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

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

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

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

## Appendix C – MSO Approved Identity Documents Guide

### \*HSPD-12 “Day One” Credentialing Process Guide\*

**Welcome to the GSA Credentialing Service! This document will help you learn what actions to take, where to go and what documents you will need to enroll for your Agency’s new HSPD-12 identification credential.**

#### (1) Getting Started

You will begin the process by giving your personal information to your Agency Sponsor – this is the person who will enter your information into the system. You will need to provide demographic information, identification information, and either (1) proof of favorably adjudicated background investigation or (2) fingerprints and background information to begin a new background investigation.

#### (2) Visiting the Credentialing Center

Once your paperwork is completed by your Agency Sponsor and delivered, you will be contacted via email and notified of the enrollment center location and appointment time.



#### (3) What to Bring

To validate your identity at the HSPD-12 Credentialing Center, you will need **2 of the following documents, including 1 Government-issued Photo Identification:**

1. U.S. Passport (unexpired or expired)
2. Certificate of U.S. Citizenship (Form N-560 or N-561)
3. Certificate of Naturalization (Form N-550- or N-570)
4. Unexpired foreign passport, with I-551 stamp or attached Form 1-94 indicating unexpired employment authorization
5. Permanent Resident Card or Alien Registration Receipt Card with photograph (Form I-151 or I-1551)
6. Unexpired Temporary Resident Card (Form I-668)
7. Unexpired Employment Authorization Card (Form I-668A)
8. Unexpired Reentry Permit (Form I-327)
9. Unexpired Refugee Travel Document (Form I-571)
10. Unexpired Employment Authorization Document issued by DHS that contains a photograph (Form I-668B)
11. Driver’s license or ID card issued by a state or outlying possession of the United States
15. U.S. Military card or draft record
16. Military dependent’s ID card
17. U.S. Coast Guard Merchant Mariner Card
18. Native American tribal document
19. Driver’s license issued by a Canadian government authority
20. U.S. Social Security Card issued by the Social Security Administration
21. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
22. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal
23. Native American tribal document
24. US Citizen ID Card (Form I-197)
25. ID Card for use of Resident Citizen in the United States (Form I-179)
26. Unexpired employment authorization document issued by DHS)

- provided it contains a photograph
- 12. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph
- 13. School ID with photograph
- 14. Voter's registration card

(4) What's Next?

Once your identity is validated, the Registrar at the Credentialing Center will take your photograph, capture your fingerprints, and send your information to the central printing facility to have your new identification card created. Your card will be shipped to the Credentialing Center and you will be notified via email to pick up your card. You will need to verify your fingerprints before your card is activated and turned over to you.

For further information, please contact Hspd\_12 MSO Coordinator Steve Duncan at [stephen.duncan@gsa.gov](mailto:stephen.duncan@gsa.gov).

## Appendix D – OMB Memo M-05-24

---

The following is an excerpt from OMB Memorandum M-05-24, Implementing Guidance for HSPD-12.

### **To whom does the Directive apply?**

As defined below, Department and Agency heads must conduct a BI, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access to Federally controlled facilities and/or information systems.

### **Departments and Agencies**

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

Does not apply to:

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

### **Employee**

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

Does not apply to:

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

### **Contractor**

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

Does not apply to:

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

### **Federally Controlled Facilities**

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

### **Federally Controlled Information Systems**

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

Does not apply to:

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

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

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

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

## Appendix E – PIV Card Usage Privacy Act Notice

---

**What is the Personal Identity Verification (PIV) Card?** You are being issued a PIV Card that is one part of a system for protecting federal buildings, computers, applications, and data. This is a secure and reliable card based on your verified identity. If you have a Government badge, the PIV Card may replace your badge.

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

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

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

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

**How Will My Information Be Used?** Your associated Agency and other agencies will use the information on the PIV Card and may use some of the stored information about you when you access to federal facilities, computers, applications, or data to prove your identity and your right of access. This information will be kept as long as you have a valid PIV Card. Use of the card is limited to that identified by the Government guidelines and to that identified in the Privacy Act system of records notices that cover each system for the PIV Card process.

**Who Will See My Information?** Information about you that we store to issue you a PIV Card and run the program may be given without your consent as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a(b)) and to the appropriate Government organization if your records show a violation or potential violation of law; to the Department of Justice, a court, or other decision-maker when the records are relevant and necessary to a law suit; to a federal, state, local, tribal,

or foreign Agency that has records we need to decide whether to retain an employee, continue a security clearance, or agree to a contract; to a Member of Congress or to Congressional staff at your written request; to the Office of Management and Budget to evaluate private relief legislation; to Agency contractors, grantees, or volunteers, who need access to the records to do Agency work and who have agreed to comply with the Privacy Act; to the National Archives and Records Administration for records management inspections; and to other federal agencies to notify them when your card is no longer valid.

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

**Where Can I Get More Information about How My Information is Used?** If you have questions or concerns about the use of your information, you may contact your organization's HSPD-12 Coordinator or Privacy Act official.

## Appendix F – Background Investigation Scheduling

### HSPD-12 IMPLEMENTATION OFFICE OF PERSONNEL MANAGEMENT INVESTIGATIONS

#### REQUIRED FORMS

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

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

#### REQUESTING ADVANCE NAC AND FINGERPRINT CHECK

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

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

OPM USE ONLY		Codes <b>R</b>	Case Number
Type of Investigation	Extra Coverage <b>3</b>		

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

## Appendix G – Appeal Rights For Denial Of A Credential

---

The following procedure is to be followed:

### 5. Appeal Rights for Federal Service Applicants

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

### 6. Appeal Rights for Contract Applicants and Agency Affiliates

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

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

**Decision** - After consideration of the determination and any documentation submitted by the PIV-II Applicant for reconsideration of the initial determination, the Agency Head/Staff Office Director or his/her designee will issue a written decision, which informs the PIV-II Applicant/Respondent of the reasons for the decision. The reconsideration decision will be final.