

DRAFT



HSPD-12 PMO

PERSONAL IDENTITY VERIFICATION

**DOI STANDARD OPERATING
PROCEDURES (SOPs)**

**March 20, 2008
Version: 7.4.3**

DRAFT

DRAFT

1	INTRODUCTION	4
1.1	Overview of HSPD-12 Policy	4
1.1.1	The Directive:	4
1.1.2	The Guidance:	4
1.1.3	The Standard:	4
1.2	OMB Encourages Agency Participation in a Shared Services Model	4
1.3	DOI Background and Scope	5
2	DOI HSPD-12 IMPLEMENTATION STRATEGY	6
3	USAccess Role Management.....	7
3.1	Implementation Approach	7
3.2	Training and Certification of Role Holders	8
3.3	Pilot Enrollment Phase.....	Error! Bookmark not defined.
4	USAccess Business Process Implementation	9
4.1	Standard [Normal] PIV II Process	9
4.2	Batch Import Process for PIV II	10
5.	Pre-Enrollment Data Preparation.....	13
5.1	Employees.....	13
5.1.1	FPPS Data Cleanup.....	13
5.1.2	Data Cleanup.....	14
5.1.3	Emergency Response Official (ERO).....	15
5.2	Data Requirements for Contractors and Others	16
5.3	Active Directory.....	17
5.3.2	Script.....	17
6.	DOI PIV II Processing Groups	18
6.1	PIV II Group I.....	18
6.2	PIV II Group II.....	18
6.3	PIV II Group III	19
7.	CARD RECEIVING AND ACTIVATION.....	20
7.1	Introduction.....	Error! Bookmark not defined.
7.2	Purpose and Scope	Error! Bookmark not defined.
7.3	Card Shipment Receiving Process	20
7.4	Card Distribution Processes.....	20
7.5	The specific processes are described in the following sections.....	20
7.5.1	Shipped directly to DOI EAS	20
7.5.2	Shipped to DOI Card Issuing Office for Activation at MSO shared EAS.....	21
7.5.3	Shipped to DOI Card Issuing Office with Activation Station	21
7.5.4	Shipped to DOI Card Issuing Office and then Shipped to Applicant for Activation.....	22
7.5	Card Inventory and Activation Tracking Process	22
8.	PIV CARD LIFECYCLE MANAGEMENT.....	23
8.1	Re-Issuance	23
8.2	Termination.....	23
8.3	PIV Card Renewal	24
8.4	PIV Card Certificate Renewal	24
8.5	PIV Card Destruction.....	25
8.6	PIV Card Holder Daily Usage Operations.....	25

DRAFT

9. COMMUNICATIONS	27
9.1 Brochures: The DOI Access Credential will be distributed Agency-wide by the	27
9.2 Emails:	27
9.3 Enrollment Center Posters:	27
9.4 MSO Reference Sheets	27
9.5 DOI SOPs.....	27
9.6 HSPD-12 Portal on the DOI Home Page	27
APPENDIX A.....	28
PIV II SPONSOR ENROLLMENT TASKS.....	28
APPENDIX B	29
PIV II ADJUDICATOR ENROLLMENT TASKS.....	29

DRAFT

1 INTRODUCTION

1.1 Overview of HSPD-12 Policy

1.1.1 The Directive:

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.

1.1.2 The Guidance:

OMB Memorandum M-05-24 establishes the implementation requirements and schedule for compliance with the Directive.

1.1.3 The Standard:

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 201 established the standard business process for identity verification for employees and contractors (PIV I), as defines the PIV identity credentials physical and electronic technical specifications (PIV II). FIPS 201 was updated to version FIP 201-1 in March 2006.

1.2 OMB Encourages Agency Participation in a Shared Services Model

OMB recommends federal agencies share the development and implementation costs for HSPD-12 by cooperating under a Shared Services Model to implement PIV II. Using this model, participating agencies share system development and implementation costs, and share hosting the deployed solution across 225 locations in the United States.

The U.S. General Services Administration (GSA) implemented the USAccess Program, powered by the EDS Assured Identity™ solution, as a Shared Service to produce compliant PIV II credentials and to maintain associated identity accounts. The USAccess mission under 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.

DRAFT

1.3 DOI Background and Scope

HSPD-12 governance and management is provided by the HSPD-12 Executive Steering Committee (HSPD-12 ESC) and the HSPD-12 Program Management Office (HSPD-12 PMO), as documented in the HSPD-12 Charter dated October 12, 2006. Policies and procedures for HSPD-12 implementation, including the Standard Operating Procedures (SOPs) outlined in this document, have been developed by the HSPD-12 Implementation Team which includes representatives from all DOI Bureau and Offices.

The HSPD-12 ESC selected to utilize the GSA USAccess Shares Services on June 18, 2007. USAccess automates and centralizes the paper-based DOI PIV I process implemented in DOI on December 2005. It is anticipated that most bureaus will centralize the Sponsorship roles within their Human Resources offices, to collect enrollment information as employees process on board. DOI will transition from PIV I processes to the USAccess PIV II processes on a phased schedule, beginning with locations with access to USAccess Enrollment centers.

DRAFT

2 DOI HSPD-12 IMPLEMENTATION STRATEGY

Successful implementation and compliance to the HSPD-12 Directive and Standard requires a standard implementation across the DOI landscape. To achieve this goal, the HSPD-12 PMO will implement by the following PIV II Processing Enrollment Groups:

DOI PIV II Processing Groups

PIV II Pilot

Complete by April 30, 2008

The Pilot Phase includes selected groups in Washington, DC, Beltsville, MD, Arlington, VA, Ft. Collins, CO and Albuquerque, NM.

Using MSO Fixed Enrollment Centers

PIV II Group I

Complete by October 27, 2008

50 % DOI population

Using MSO and DOI Fixed Enrollment Centers

PIV II Group II

Complete by October 27, 2009

? % DOI population

Using MSO and DOI Fixed or Mobile Enrollment Centers

PIV II Group III

Complete by October 27, 2010

? % DOI population

Use lower cost remote solution

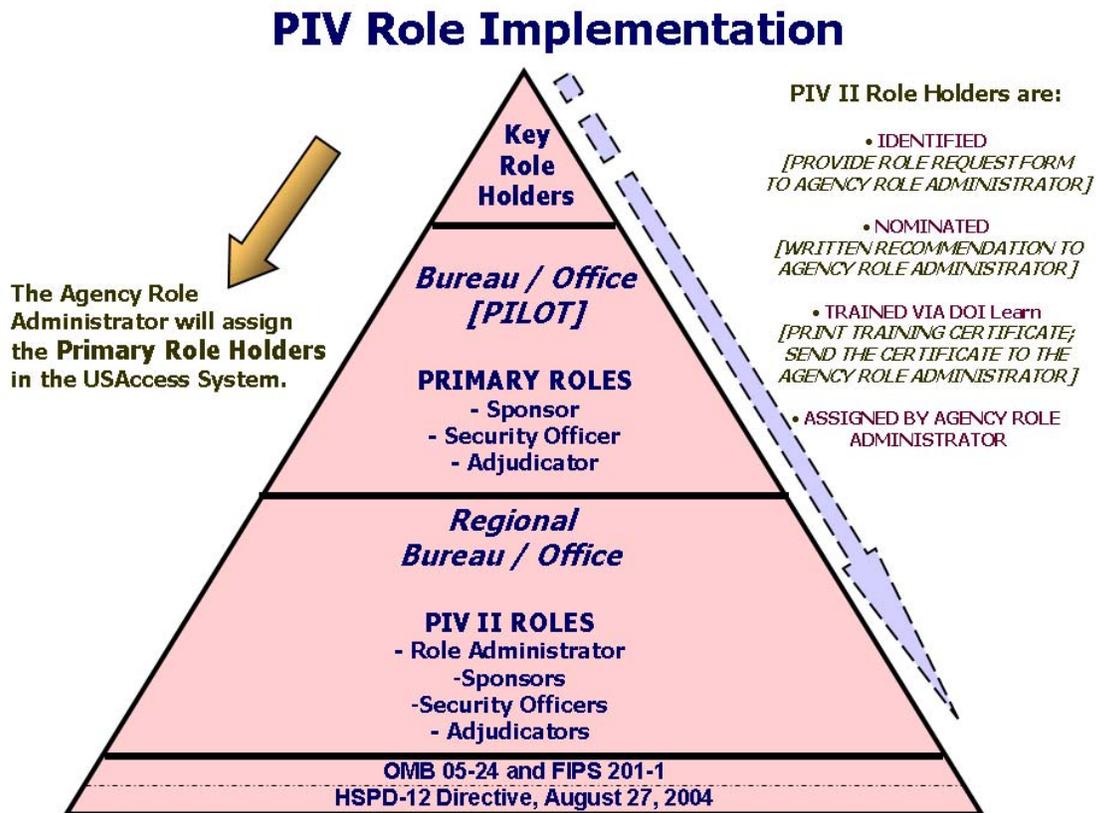
Processing of existing employees and contractors requires establishment of roles, business processes and verification of PIV data contained in the Federal Personnel and Payroll System (FPPS). The HSPD-12 PMO will evaluate bureau processing readiness based on the following categories:

- USAccess Role Management
- USAccess Business Process Implementation
- Pre-enrollment (sponsorship and adjudication) Data Preparation

3 USAccess Role Management

3.1 Implementation Approach

The USAccess operational environment officially starts with the assignment of USAccess system roles. DOI Role Management started with the assignment of five Key role holders, sponsored by GSA: Role Administrator, Sponsor, Adjudicator, Security Officer and Activator. The next step was to assign Primary role holders within each bureau and office to initiate enrollment of their existing employees and contractors into the USAccess System.



The PIV II system-based roles and responsibilities are as follows:

- **ROLE ADMINISTRATOR**-- required for DOI and Bureau levels to maintain separation of duties between roles. The Agency Role Administrator creates and manages role accounts for the Agency.
- **SPONSOR**--required at the DOI, Bureau, and Regional levels for collecting and entering enrollment data for new employees and contractors. The Sponsor

DRAFT

initiates the pre-enrollment process, manages the applicant's account, and approves/denies an applicant's application.

- **ADJUDICATOR**--required 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**--required and provided by GSA and/or DOI. Registrars are responsible for verifying the claimed identity of the applicant; validating the entire set of identity source documents presented at the time of registration; updating biographical information; collecting biographical documents; capturing the applicant's photo and biometric information; and explaining the privacy and security policies to the applicant.
- **SECURITY OFFICER**--required at the DOI, Bureau, and Regional levels to perform auditing and reporting, investigate/evaluate services to resolve impersonation conflicts, and perform PIV Card and certificate suspensions/reactivations/and revocations.
- **ACTIVATOR**—required at the Bureau and Regional levels to manage secure storage and deployment of printed PIV Cards; verify that the data on the screen and on the PIV Card match the applicant present; verify identity documents presented match the scanned documents; validate applicant's primary and secondary fingerprints; encode and activate the PIV Card; test the PIV Card; instruct the applicant on use, privacy, and security of PIV Card.

3.2 Training and Certification of Role Holders

All DOI role holders will be trained and certified as GSA USAccess system users. HSPD-12 role training is provided through DOI Learn, which will maintain a record of training certificates for audit purposes. Train the trainer classes are provided for each bureau and office, so their primary role holders learn how to coordinate their roles to complete the USAccess enrollment and activation functions for their employees and contractors. Primary role holders will continue to receive updated training information and be alerted to updates to the USAccess system. The assignment, Training & Certification and System Access process:

1. Supervisor signs Role Assignment form
2. Role Holder completes training via DOI Learn
3. Role Holder submits Role Assignment form and Training Certificate to Role Administrator
4. Role Administrator assigns role in USAccess
5. Role Holder receives email with USAccess login information

DOI or Bureau Role Administrator's monitor all roles and can revoke access at any time if the role holder violates the Privacy Act or FIPS 201-1 standard procedures.

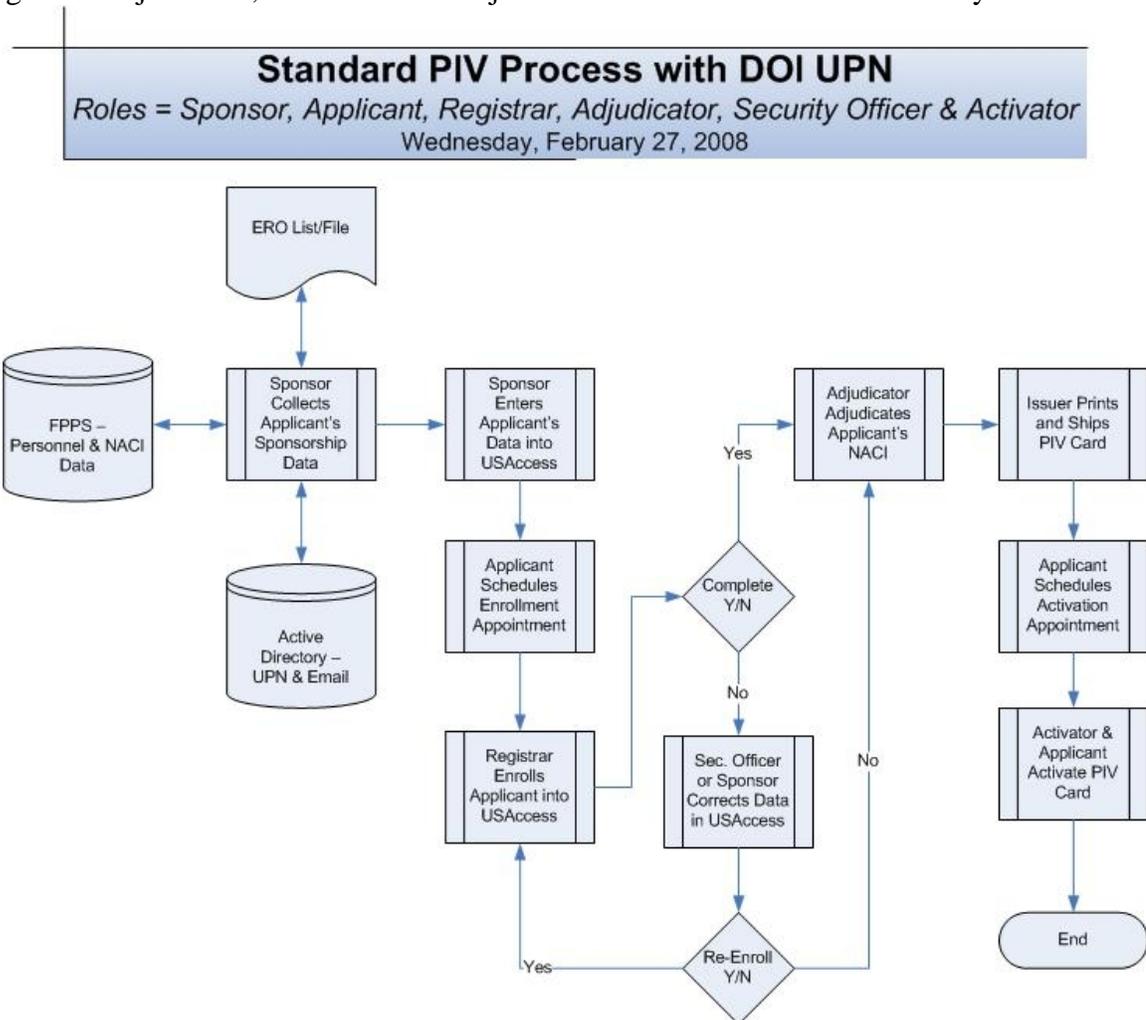
DRAFT

4 USAccess Business Process Implementation

4.1 Standard PIV II Process

The Department of Interior hires new employees on a regular basis. Employee information for newly hired DOI employees is recorded in FPPS, the DOI System of Record for Human Resource Information. Information for existing or current DOI employees resides in FPPS as well.

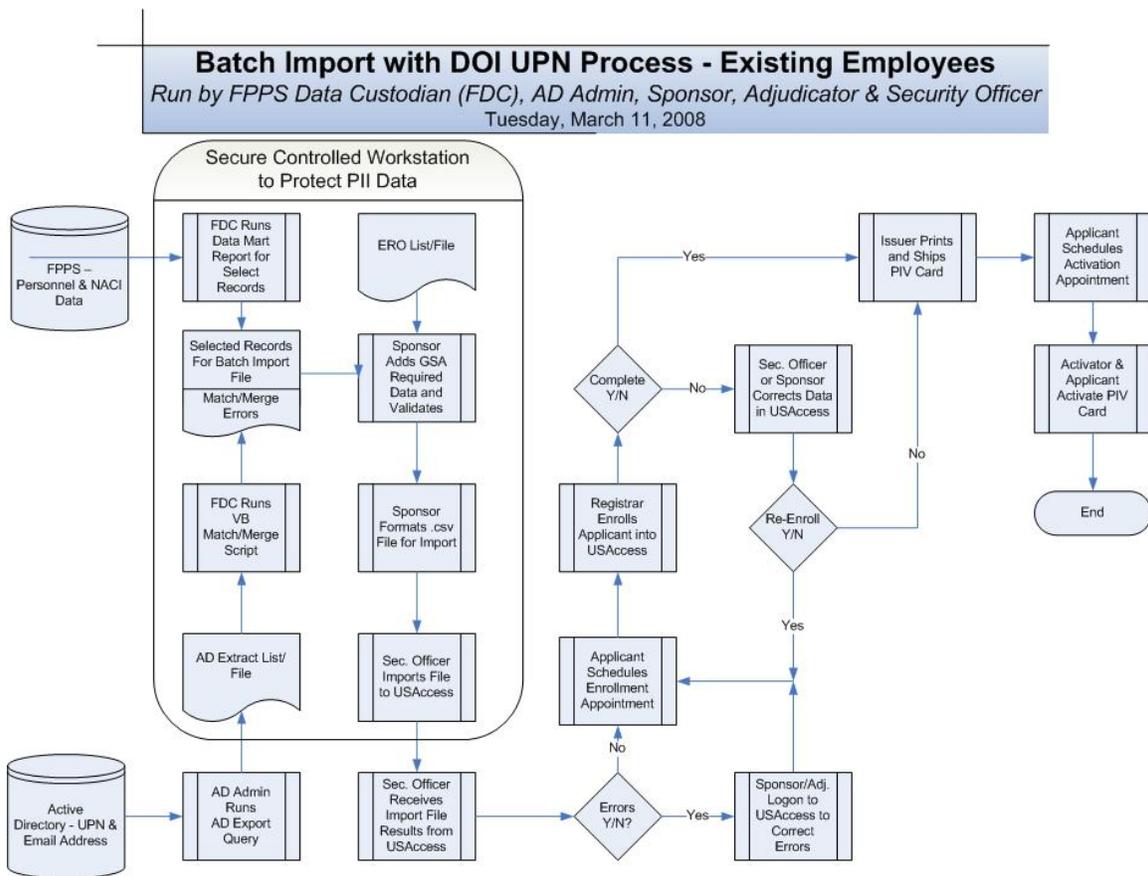
The standard PIV II processing responsibilities start by the Sponsor verifying the applicant's need for a PIV credential. Once the need for a credential is established, the Sponsor enters employee identification data into the USAccess system via the Sponsor portal. The applicant then enrolls through an identity verification process, and submits the necessary information for a background check. OPM provides the results to a designated Adjudicator, who enters the adjudication results into the USAccess system.



DRAFT

4.2 Batch Import Process for PIV II

Batch imports will be used to submit existing employee data to the USAccess system for PIV II Group I. This is the most efficient and timely method to import the large volume of existing DOI employee data into the USAccess System. Batch imports also support the DOI enrollment analysis strategy which is based on GSA's phased-deployment schedule to assist Government Agencies in rolling out the HSPD-12 Program and to facilitate card production. DOI's batch import process is different from other Agencies in that we're providing the USAccess system with "all" of the Sponsor and Adjudication data that's needed to populate a "complete" record. This will minimize the need for the Primary role holders (e.g., Sponsors and Adjudicators) to constantly correct imported applicant data.

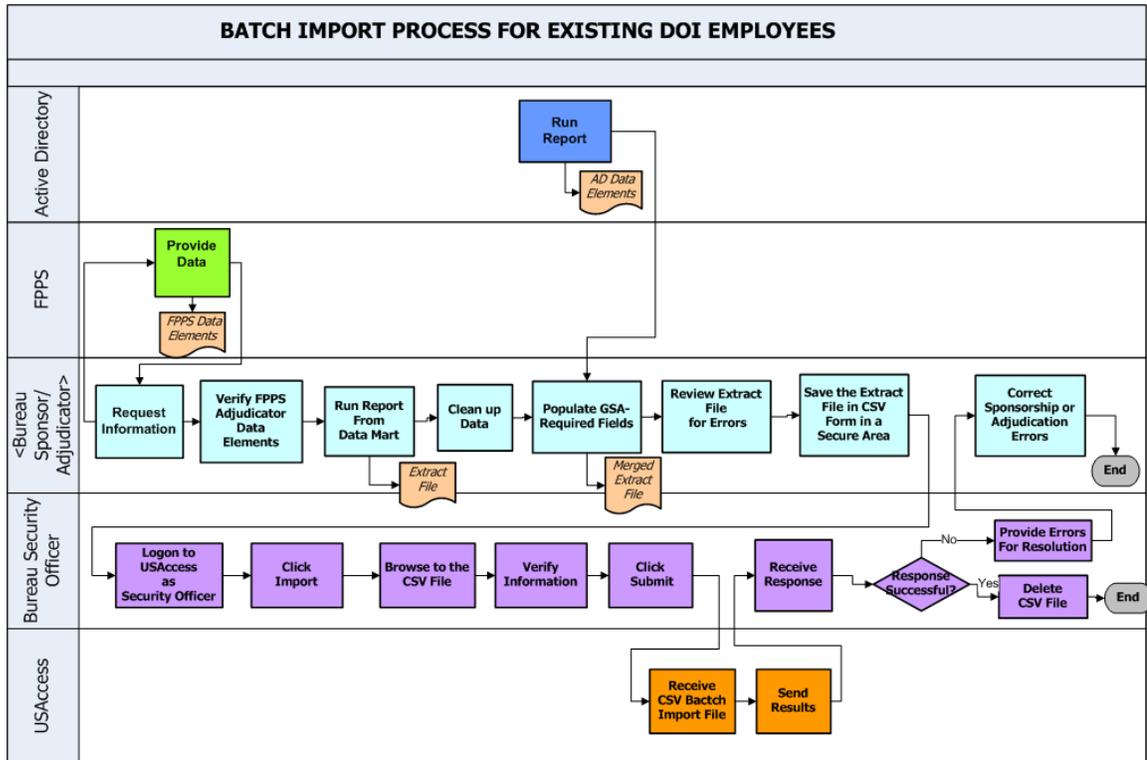


DRAFT

- The Sponsor/Adjudicator initiates the batch imports tasks in a secure computer by requesting a defined set of applicant data for specific employees, contractors, other personnel. If the applicant is a DOI employee, this request is sent to the FPPS Data Custodian. For Contractors and other personnel, this request may be sent to Acquisition Managers, Human Resource Managers or other DOI managers/supervisors who acquire contractor support.
- The FPPS Data Custodian provides a file (or spreadsheet) that contains bureau employee information [i.e., sponsorship and adjudication data] from the Federal Personnel and Pay System (FPPS). For contractors and other personnel, this information may be maintained in spreadsheet formats, Access Database, or other information tools.
- The Sponsor/Adjudicator performs data cleanup to ensure that the file is populated correctly; adds Active Directory (AD) data elements (i.e., business email; DOI User Principal Name (UPN), and saves the file in the CSV format in the secure computer area.
- The Security Officers are the only role holders that are authorized to send the batch import file to the USAccess system. The Security Officer logs into the USAccess system to retrieve the formatted CSV file, verify the information, and import the file to USAccess. The Security Officer then receives a notification (e.g., an email containing results) from the USAccess system. A “failed results” notification from the USAccess system indicates that the batch import file contained inaccurate information. The Bureau Security Officer will notify the Sponsor/Adjudicator that the batch import file contained inaccurate information.
- The Sponsor/Adjudicator corrects the enrollment errors and/or resolves the issues that are identified in the USAccess report, and returns an updated file to the Security Officer to import. This batch import process is illustrated as follows:

DRAFT

The Batch Import Process for Existing DOI Employees, Contractors and Other personnel is illustrated as follows:



DRAFT

5. Sponsorship Data Preparation

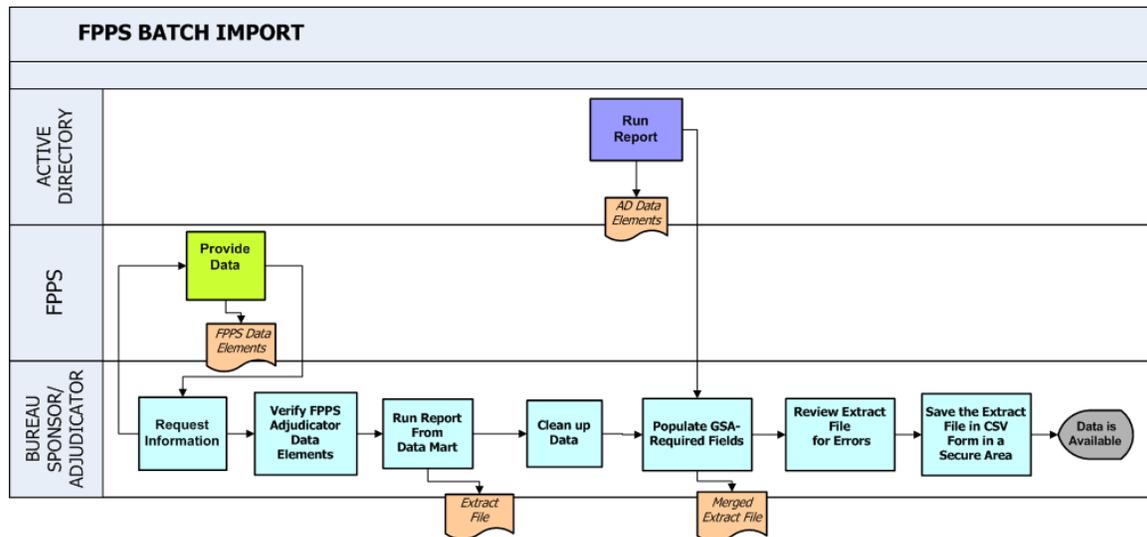
5.1 Employees

Sponsor and Adjudication data currently exists in FPPS for existing employees. This data needs to be verified prior to submission to GSA.

5.1.1 FPPS Data Cleanup

The Federal Personnel and Payroll System (FPPS) is the DOI System of Record for Human Resource Information. The FPPS Data Custodian is responsible for providing a report (or spreadsheet) that contains employee information [i.e., sponsorship and adjudication data] from FPPS. The FPPS batch import is an extraction of sponsorship information from FPPS, the System of Record for DOI employees. The responsibility for creating the batch import file is accomplished by Sponsor/Adjudicators, the FPPS Data Custodian, and Security Officers using data from the FPPS and DOI's Active Directory (AD) systems, and importing information into the USAccess system as follows:

BATCH IMPORT



DRAFT

5.1.2 Data Cleanup

No matter how data is entered into an information system, the quality of the output is only as good as the quality of the input. The best time to avoid problems is when the data is entered into the system. The main objective of the “Cleanup Data” process is to ensure the quality, accuracy, and timeliness of the data that is entered into the USAccess system. For example, in reviewing the “Adjudication Status” fields, the Adjudicator looks for “False” entries, because “false” entries will not successfully import into the USAccess system. The adjudication status field must be corrected. In data cleanup, the Sponsor and or Adjudicator can correct fields, if required. Data cleanup is essentially a validation check of all the data fields that are identified in the Data Mart HSPD-12 Template to reduce or eliminate input errors into USAccess System. The data fields in the HSPD-12 Template are listed in this table:

HSPD-12 DATA FIELDS TEMPLATE

<i>Name First</i>	<i>Postal Address City</i>	<i>Federal Emergency Response Official Flag</i>
<i>Name Middle</i>	<i>Postal Address State Code</i>	<i>Card Ship Address Code</i>
<i>Name Last</i>	<i>Postal Address Zip</i>	<i>SON</i>
<i>Name Suffix</i>	<i>Person ID</i>	<i>SOI</i>
<i>Social Security Number</i>	<i>Agency Person GUID2</i>	<i>OPAC</i>
<i>Tax ID</i>	<i>Sponsor Organizational Identifier</i>	<i>UPN</i>
<i>Foreign ID</i>	<i>Employment Status</i>	<i>Rank2</i>
<i>Citizenship</i>	<i>Sub-Agency Abbreviation</i>	<i>Agency Specific Text</i>
<i>Data of Birth</i>	<i>Person Organization Association Category</i>	<i>Agency Specific Data</i>
<i>Birth Country Code</i>	<i>Sponsor PID</i>	<i>Card Header</i>
<i>Birth State Code</i>	<i>Date of Sponsorship</i>	<i>Contract Number</i>
<i>Birth City</i>	<i>PIV Card Required Code</i>	<i>NAC Adjudication Note</i>
<i>Citizen Country Code</i>	<i>PIV Card Type</i>	<i>NAC Adjudication Value</i>
<i>Postal Address Street 1</i>	<i>Business Phone</i>	<i>NAC Adjudication Date</i>
<i>Postal Address Street 2</i>	<i>Business Email</i>	<i>NAC Adjudication Effective Person ID</i>
<i>Postal Address Street 3</i>	<i>Home Email</i>	End of Record

DRAFT

5.1.3 Emergency Response Official (ERO)

The OLESEM guidance signed on 12/21/07, established the criteria for ERO designations, and requests nomination of ERO approval managers. Emergency Response Officials must be identified in the USAccess system according to the Agency-Specific data fields that are shown as follows:

EMERGENCY RESPONSE OFFICIAL (ERO) FLAG AND TITLE

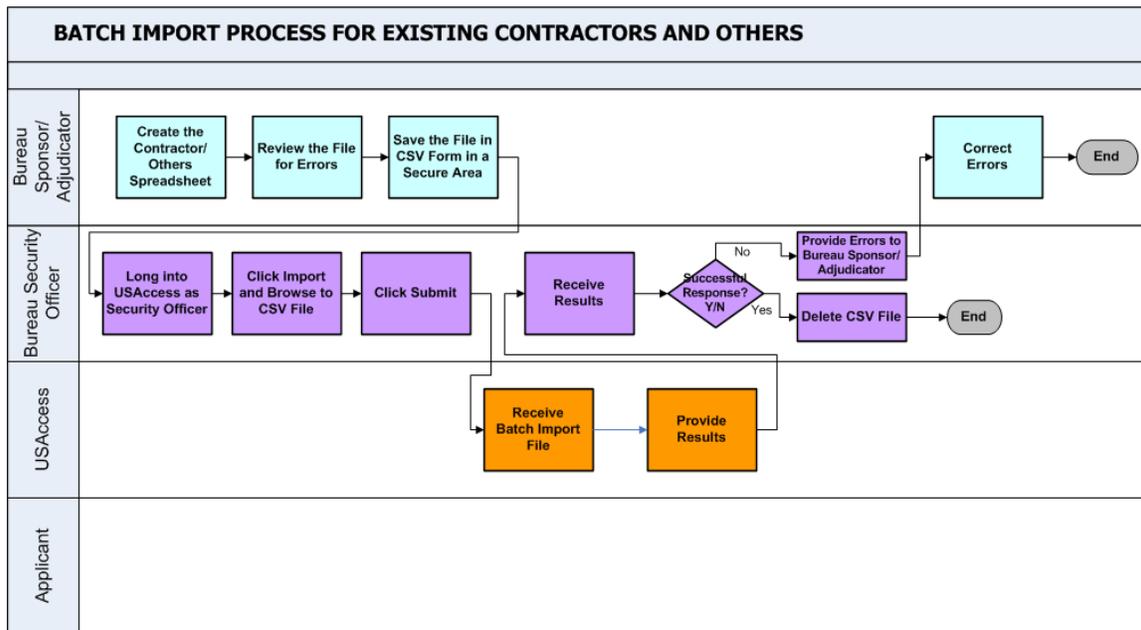
ERO Title	USAccess Title
Law Enforcement	Law Enforcement
Firefighter	Firefighter
Security Security/Courier Investigator	Security Officer
EMS/Rescue	EMS/Rescue
Emergency Management Continuity of Operations Plan (COOP), Continuity of Government (COG), National Response Plan (NRP), National Infrastructure Protection Plan (NIPP) Incident Response Other Individuals	Emergency Management

DRAFT

5.2 Data Requirements for Contractors and Others

Contractors and Others (or current/existing contractors and others) are those individuals who have completed background investigations and network access to DOI computer systems, and are located in proximity to additional operational Shared Enrollment, fixed, and mobile sites; and DOI leased, fixed, and mobile sites. Other personnel include Volunteers, Tribal Members, Visiting Scientists, Foreign Government visitors, Employees and Contractors Detailed from Other Federal Agencies, Presidential Transition Staff, Concessioners, and Cooperating Associations. Approximately 25% of the existing contractors and other personnel are projected to be enrolled in the USAccess system using the batch imports by October 27, 2007.

The Sponsor/Adjudicator will essentially create an existing **Contractor and Others** Spreadsheet using the same data elements that are identified for DOI Employees from FPPS. These data elements are listed above (*See Section 4.2 Batch Import*). The batch import process for existing **Contractors and Others** is illustrated as follows:



DRAFT

5.3 Active Directory

Active Directory is Microsoft's trademarked directory service, an integral part of the Windows architecture. Like other directory services, such as Novell Directory Services (**NDS**), Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.

The active directives provide the business emails and User Principal Name (UPN) data elements for each employee and contractor to the Sponsor. These data elements are mandatory data fields that must be populated for Sponsorship and enrollment into USAccess.

5.3.1 Report from FPPS Custodian

The reports from FPPS Custodians include the data elements for DOI employees, contractors and other personnel who need PIV II identification cards. FPPS reports contain security data elements, codes, values, and definitions in specified data formats and conventions. The FPPS Custodians are trained data specialists who can correctly interpret FPPS data and provide consistent information in various report formats. For example, the FPPS Custodian creates batch import reports in the FPPS Data Mart, which is an extraction of specific data elements from FPPS to meet HSPD-12 requirements.

5.3.2 Data Preparation Script

In the course of acquiring the mandatory data elements for HSPD-12 data, several "scripts" have been written or recommended to extrapolate data from active directives with reasonable success. Reasonable because scripts are highly dependent upon maintaining consistent applications, tools, and conventions wherever they may be used. To run scripts successfully, the same network configuration, tools, and applications must be present each time the script is executed. These conditions may be highly improbable and difficult to acquire. However, to increase accuracy and obtain high-quality success, Bureau IT specialists perform tests to ensure that the script can be executed on local networks. By testing the scripts locally, Bureau IT specialists can ensure data quality, accuracy and consistency. In an operational environment scripts can be tested, approved and provided globally to authorized users.

DRAFT

6. DOI PIV II Processing Groups

6.1 PIV II Group I

Processing of Existing DOI Employees

The first Group to be processed will be existing DOI employees who have completed background investigations, online computer systems, and are supported by a GSA Enrollment Center. All employees in the PIV II Group I phase are projected to be enrolled in the USAccess system by October 27, 2008.

- The batch import method will be used Group I enrollments. It is created by the Bureau Sponsor/Adjudicators. The Sponsor/Adjudicator receives a file that contains bureau employee information [i.e., sponsorship and adjudication data] from FPPS, the DOI System of Record for Human Resource Information. The Bureau Sponsor/Adjudicator initiates the batch imports tasks. Bureau Security Officers are the only roles that are authorized to send the batch import file to the GSAccess system.

6.2 PIV II Group II

Batch Import Existing Contractors and Newly Hired DOI Employees

The second Group to be enrolled into the USAccess system via the batch import process is existing contractors who have completed their background investigations, have online computer systems, and are supported by a GSA Enrollment Center. All existing contractors and newly hired DOI employees are projected to be enrolled in the USAccess system by October 27, 2009.

There are two methods for Group II processing: Batch Import and the Normal [Standard] PIV II Processes. We've illustrated one of the methods, the Batch Import Process, in Group I to sponsor and adjudicate existing DOI employees. The batch import and normal processes will be implemented as follows:

- The **BATCH IMPORT PIV II PROCESS** accommodates data input for large volumes of data. In Group II, the batch import process will be used to enroll existing contractors into the USAccess system. The Batch Import process for sponsoring existing contractors is illustrated in Section 5.2.
- The **NORMAL PIV II PROCESS** will be established to enter DOI newly hired employee information into the USAccess system by using online data entry or manual input activities. The Batch Import Process is an alternate process that supports the Normal [Standard] PIV II Process which is illustrated in Section 4.1.

DRAFT

6.3 PIV II Group III

Group III will focus on the processing of *remote Employees, Contractors, and Other personnel*. The *Remote Employees, Contractors, and Other personnel* will be processed in the USAccess system by October 27, 2010. Other personnel may include Volunteers, Tribal Members, Visiting Scientists, Foreign Government Visitors, Employees and Contractors Detailed from Other Federal Agencies, and the Presidential Transition Staff, Concessioners, and Cooperating Associations. Remote employees, contractors, visitors, volunteers, and others will be supported by Mobile GSA Shared Solution.

DRAFT

7. CARD RECEIVING AND HANDLING PROCESS

Even though the USAccess PIV Cards do not contain any electronically stored personal information at the time they are shipped from the manufacturer, they are still considered controlled media. As such, a “chain of trust” must be maintained from the time it is received on site until the time it is turned over to the Cardholder for activation.

DOI currently maintains many card issuing offices throughout the Department and bureaus, which are staffed with personnel experienced in the processing and handling of identification and building access cards. DOI has decided to leverage this experience by designating some of these existing offices and personnel to implement this process.

7.1 Card Shipment Receiving Process

Designated primary or secondary personnel will perform the following steps at their assigned card issuing office:

- Receive and sign for card shipment
- Open card shipment and add card information (e.g., full name, card number, etc.) to the card inventory log
- Secure cards in a locked container (e.g., drawer, file cabinet, etc.)

7.2 Card Distribution Processes

DOI supports four separate card distribution scenarios:

- Shipped directly to DOI Enrollment and Activation Station (EAS);
- Shipped to DOI card issuing office for activation at MSO shared EAS;
- Shipped to DOI card issuing office with activation station; and,
- Shipped to DOI card issuing office and then shipped to applicant for activation at an activation station.

7.3 The specific processes are described in the following sections.

7.5.1 Shipped directly to DOI EAS

The applicant will receive email notification to pick up and activate their card at a DOI EAS, where the designated primary or secondary personnel (in most cases a Registrar) will perform the following steps:

DRAFT

- Check applicant's government issued photo identity document (e.g., drivers license, DOI identification card, etc.)
- Retrieve applicant's card from secure container
- Sign and date the card inventory log
- Provide card to applicant along with electromagnetically opaque sleeve (cardholder)
- Observe applicant as they perform the activation of their card

7.5.2 Shipped to DOI Card Issuing Office for Activation at MSO shared EAS

The applicant will receive email notification to pick up their card from their DOI Card Issuing Office, where the designated primary or secondary personnel will perform the following steps:

- Check applicant's government issued photo identity document (e.g., driver's license, DOI identification card, etc.)
- Retrieve applicant's card from secure container
- Obtain applicant's signature and date on card inventory log
- Provide card to applicant along with electromagnetically opaque sleeve (cardholder) and card handling and activation instructions

Once the applicant receives their card, they will proceed to their selected MSO shared EAS location to activate their card.

7.5.3 Shipped to DOI Card Issuing Office with Activation Station

The applicant will receive email notification to pick up and activate their card at a DOI issuing office with an activation station, where the designated primary or secondary personnel will perform the following steps:

- Check applicant's government issued photo identity document (e.g., driver's license, DOI identification card, etc.)
- Retrieve applicant's card from secure container
- Sign and date the card inventory log
- Provide card to applicant along with electromagnetically opaque sleeve (cardholder)
- Observe applicant as they perform the activation of their card

DRAFT

7.5.4 Shipped to DOI Card Issuing Office and then Shipped to Applicant for Activation

The applicant will receive email notification that their card has been shipped to a DOI Card Issuing Office, however, the applicant works at a remote location and cannot pick up their card for activation in person. The designated primary or secondary personnel at the DOI Card Issuing Office will perform the following steps:

- Retrieve applicant's card from secure container
- Sign card inventory log to indicate shipping of card to applicant
- Package card along with electromagnetically opaque sleeve (cardholder) and card handling and activation instructions in a FedEx envelope
- Ship package to applicant with signature required
- File copy of FedEx shipping document

Once the applicant signs for FedEx package and receives their card, they will proceed to their selected activation station location to activate their card.

7.5.4.1 Shipped to DOI Card Issuing Office and then Shipped to Activation Site

The applicant will receive email notification that their card has been shipped to a DOI Card Issuing Office. However, when the applicant works at a remote location and cannot pick up their card for activation in person, they will send an email to notify this office when and where they intend to activate their card. The designated primary or secondary personnel at the DOI Card Issuing Office will perform the following steps:

- Retrieve applicant's card from secure container
- Sign card inventory log to indicate shipping of card to activation site
- Package card along with electromagnetically opaque sleeve (cardholder) a FedEx envelope
- Ship package to the activation site with signature required
- File copy of FedEx shipping document
- Send email to applicant with FedEx tracking number and card handling and activation instructions

Once the FedEx package arrives, the applicant will proceed to their selected activation station location to activate their card.

7.5 Card Inventory and Activation Tracking Process

To ensure that the card inventory log is properly maintained and that applicants have received and activated their cards, the designated DOI Card Issuing Office primary or secondary personnel will perform the following steps:

- Run the USAccess weekly card activation report
- Reconcile the inventory log by initialing each activated card record
- Send activation reminder to any applicant who has signed for but not activated their card

DRAFT

8. PIV CARD LIFECYCLE MANAGEMENT

8.1 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 occurs, the enrollment process required for re-issuance will also include fingerprint and facial image recapture. When the new facial image photo is taken during re-issuance, the existing photo in the database corresponding to the previously issued PIV card is made available to the Registrar for comparison during the enrollment. The old photo is displayed on the biographic screen when the previous record is retrieved, and also on the photo screen before taking the new photo. 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.

8.2 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

DRAFT

- 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 6.1.5.

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.

8.3 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.

8.4 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.

DRAFT

8.5 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. PIV Card destruction shall occur within 30 days of meeting the circumstances noted above.

Credential destruction shall be accomplished in the following manner:

- The Applicant's status should be set to "Terminated" through the Sponsorship portal.
- The credential shall be physically destroyed with concern for PII data as follows:
 - Place the credential card into an industrial shredder.
 - 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)
- 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.
- The Sponsor shall mark the card as "destroyed" on the sponsorship page for the credential owner in the Sponsorship portal and save the record.

8.6 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 loose, ink rubbing off, cuts/rips/tears occur in the card), they shall return to the Sponsor immediately.

DRAFT

- 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.

DRAFT

9. COMMUNICATIONS

The HSPD-12 Communications Strategy includes informing DOI managers, supervisors, employees, and organizations about the HSPD-12 goals, progress, and improvements. Information will be disseminated as follows:

9.1 Brochures: The DOI Access Credential will be distributed Agency-wide by the ...

9.2 Emails:

9.3 Enrollment Center Posters:

9.4 MSO Reference Sheets

9.5 DOI SOPs

9.6 HSPD-12 Portal on the DOI Home Page

DRAFT

APPENDIX A PIV II SPONSOR ENROLLMENT TASKS

NORMAL [STANDARD] PIV II:

1. Logon as SPONSOR in the USAccess system
2. Input the Social Security Number (SSN) or Last Name AND Date of Birth (MM/DD/YYYY) of the individual you wish to Sponsor
3. Click on Search
4. Click on NEW APPLICANT
5. Enter information (e.g., First Name, Middle Name, Last Name, Date of Birth, SSN, Ethnicity, Citizenship, Citizenship Status, Personal/Home email, etc.)
- 6.

BATCH IMPORT PIV II:

1. Identify Applicant(s) for enrollment (e.g., By title, location, individual name(s))
2. Request Report from FPPS
3. Verify FPPS Data Elements
4. Run Report from Data Mart
5. Cleanup Data
6. Populate GSA-Required Fields
7. Review the Merged File for Errors
8. Save File in CSV Form in a secure area
9. Correct Sponsorship Errors
- 10.

DRAFT

APPENDIX B PIV II ADJUDICATOR ENROLLMENT TASKS

NORMAL [STANDARD] ENROLLMENT:

BATCH IMPORT ENROLLMENT:

DRAFT

APPENDIX C

PIV II SECURITY OFFICER ENROLLMENT TASKS

NORMAL [STANDARD] ENROLLMENT:

BATCH IMPORT ENROLLMENT:

DRAFT

APPENDIX D

PIV II REGISTRAR ENROLLMENT TASKS

NORMAL [STANDARD] ENROLLMENT:

BATCH IMPORT ENROLLMENT:

DRAFT

APPENDIX E PIV II ACTIVATOR TASKS

NORMAL [STANDARD] ENROLLMENT:

BATCH IMPORT ENROLLMENT:

DRAFT

APPENDIX F – REFERENCES

- HSPD-12 Directive, August 27, 2004
- OMB 05-24,
- FIPS 201-1, Federal Information Processing Standard (FIPS)
- NIST-79,
- PIV Card Issuer Operations Plan, v1.1, August 15, 2007