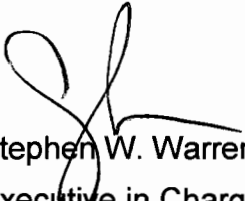


**HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) PROGRAM**

- 1. REASON FOR ISSUE:** This handbook defines Department-wide roles, responsibilities, and procedures to implement VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program* for the management, issuance, and use of identity credentials within the VA.
- 2. SUMMARY OF CONTENT/MAJOR CHANGES:** This handbook sets forth revised roles, responsibilities, and procedures for an HSPD-12 Program that integrates Personal Identity Verification (PIV), Physical Access Control System (PACS), and Logical Access Control System (LACS) capabilities within VA.
- 3. RESPONSIBLE OFFICE:** Office of Operations, Security, and Preparedness (007), Office of Personnel Security and Identity Management, HSPD-12 Program Office.
- 4. REFERENCES:** VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*; VA Directive 0710, *Personnel Security and Suitability Program*; VA Directive 6500, *Managing Information Security: VA Information Security Program*; VA Directive 6502, *VA Enterprise Privacy Program*. VA Handbook 6502.1, *Privacy Event Tracking*; VA Directive 5021, *Employee/Management Relations*; 5 U.S.C. § 2105, *Employee*; Title 38 U.S.C., 7401 *Veterans' Benefits*;
- 5. RESCISSIONS:** None.

**CERTIFIED BY: BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS**

Distribution: Electronic Only

  
Stephen W. Warren  
Executive in Charge and  
Chief Information Officer for  
the Office of Information and  
Technology

  
Kevin Hanretta  
Assistant Secretary for Operations,  
Security, & Preparedness

This page left intentionally blank.

**CONTENTS**

PARAGRAPH	PAGE
INTRODUCTION	5
ROLES AND RESPONSIBILITIES	6
CREDENTIAL TYPES, ELIGIBILITY, AND AFFILIATIONS	13
IDENTITY VERIFICATION AND CREDENTIAL ISSUANCE	16
CREDENTIAL MANAGEMENT LIFECYCLE	18
APPEALS PROCESS	23
PIV PRIVACY GUIDELINES	25
APPENDIX A: DEFINITIONS	A-1
APPENDIX B: ACRONYMS	B-1
APPENDIX C: APPLICANT ELIGIBILITY AND ACCESS TYPE	C-1
APPENDIX D: EMPLOYMENT ELIGIBILITY VERIFICATION	D-1
APPENDIX E: CREDENTIAL TOPOLOGIES	E-1
APPENDIX F: BIOMETRIC DATA CAPTURE	F-1

This page left intentionally blank.

## 1. INTRODUCTION

### a. Background

(1) *Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors* mandates issuance of a standard and reliable form of identification to federal employees and contractors in compliance with technical and procedural requirements defined in *Federal Information Processing Standards (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors*.

(2) HSPD-12 directs all federal agencies and departments to issue identity credentials to provide government workers, contractors, and affiliates with a credential that provides the attributes of security, authentication, trust, and privacy and can be used to verify identities in order to enter federal buildings or gain access to federal computer networks.

### b. Purpose

(1) The purpose of this Department of Veterans Affairs (VA) Handbook 0735, in conjunction with the policies and responsibilities defined in VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, is to provide guidance regarding use, administration, and governance of VA identity credentials.

### c. Scope

(1) This Handbook defines the roles supporting the PIV process at VA facilities.

(2) This Handbook provides guidance for identity proofing of all VA employees, contractors, and affiliates requiring access to VA facilities or information systems.

(3) This Handbook provides guidance for the issuance of Personal Identity Verification (PIV) Cards, Non-PIV Cards, and Flash Badges for access by VA employees, contractors, and affiliates.

(4) This Handbook provides guidance on the use of identity credentials for physical and logical access, including usage by Physical Access Control Systems (PACS) and Logical Access Control Systems (LACS).

### d. Applicability

(1) This VA Handbook 0735 applies to VA facilities that issue PIV Credentials, henceforth referred to as a VA PIV Card Issuing (PCI) Facility;

(2) This VA Handbook 0735 applies to VA owned, leased, and contracted facilities, other government agencies that support VA mission requirements, or any other third party utilizing VA information to perform a VA authorized activity;

(3) This VA Handbook 0735 applies to VA employees, contractors, and affiliates requiring long-term or short-term access to VA facilities or information systems in order to perform a VA authorized activity; and

## VA HANDBOOK 0735

- (4) This VA Handbook 0735 applies to roles that support PIV processes and functionality.

(5) The Office of Operations, Security, and Preparedness (OSP) is responsible for the development and dissemination of additional directives, handbooks, memoranda, notices, and best practices to implement these procedures or to institute additional requirements to maintain the VA HSPD-12 Program, as needed

## 2. ROLES AND RESPONSIBILITIES

### a. Department Roles

- (1) Senior Agency Official

(a) In accordance with VA Directive 0735, *Homeland Security Presidential Directive-12 (HSPD-12) Program*, the Assistant Secretary for Operations, Security, and Preparedness is the Senior Agency Official for the VA HSPD-12 Program.

- (b) Manages and provides oversight for VA's HSPD-12 program.

- (c) Documents all VA identity management responsibilities, roles, and procedures.

(d) Identifies and designates qualified individuals to the roles of Designated Accreditation Authority (DAA), Assessor, VA Official for Privacy (AOP), and other VA officials involved with identity management.

- (2) Designated Accrediting Authority (DAA)

(a) The Director of Personnel Security and Identity Management within the Office of Operations, Security and Preparedness (OSP) is the DAA for the VA HSPD-12 Program.

(b) Reviews certification documentation and the recommendation prepared by the Assessor/Certification Agent (CA) and issues appropriate Authorities to Operate (ATO) for VA PCI Facilities.

- (3) Assessor

(a) The Director of the HSPD-12 Program Management Office is the designated Assessor of the VA HSPD-12 Program.

(b) Is organizationally separate from the persons and the office(s) directly responsible for the day-to-day operation of identity management for the Department and correction of deficiencies and discrepancies identified during the certification.

(c) Conducts reviews, in accordance with this Handbook and National Institute for Standards and Technology (NIST) Special Publication Guidelines for

the Accreditation of Personal Identity Verification Card Issuers (SP) 800-79-1, of the programs and procedures established in this document for the issuance of PIV credentials.

(d) This process assures that VA has adopted and is using an approved identity proofing, registration, issuance, and life cycle maintenance processes as required in FIPS 201 and that all required roles, responsibilities, activities, and actions specified in the approved model are adequately documented.

(4) Organization Identity Management Official (OIMO) for HSPD-12

(a) The Director of VA's HSPD-12 Program Management Office is the OIMO for the VA HSPD-12 Program.

(b) Implements the policies of the organization, assuring that all procedures are performed reliably, and provides guidance and assistance to PCI Facilities.

(c) Ensures that all PIV roles are staffed by capable, trustworthy, knowledgeable, and trained personnel.

(d) Ensures that all credential issuance services, equipment, and processes meet FIPS 201 requirements and NIST 800-79-1 standards.

(e) Monitors and coordinates activities with PCI Managers.

(f) Supports and maintains the NIST 800-79-1 assessment and accreditation process.

(5) Senior Agency Official for Privacy (SAOP)

(a) Deputy Assistant Secretary for the Office of Information Technology, Chief Information Security Officer (CISO)

(b) Oversees privacy-related matters in the identity management process to ensure that the rights of Applicants are protected in accordance with applicable laws and regulations.

(c) Audits the entire VA PIV process and PIV system implementation to confirm compliance with the Privacy Act of 1974, and other applicable privacy laws and regulations, as defined in the Privacy Impact Assessment (PIA).

(d) Consults with PIV Credentials Applicant Representatives on matters concerning Applicant rights under the Privacy Act of 1974.

(e) Monitors PIV system operations to ensure compliance with applicable System of Records Notices (SORNs) and notifies key VA officials (PIV system owner, Information Security Officers, management, etc.) of compliance issues.

(6) HSPD-12 Program Management Office

## VA HANDBOOK 0735

(a) Addresses policy and program questions and issues that arise during all phases of the PIV Credentials management lifecycle.

(b) Provides communications to VA organizations regarding policy, program operations, system announcements, and education.

(c) Works with the PIV Technical Team to monitor system issues.

(7) PIV Technical Team

(a) Addresses technical Credentials management issues that arise during all phases of the PIV Credentials management lifecycle identified in this document.

(b) Works with local Information Resource Managers, Information Security Officers, and the National Service Desk (NSD) to address PIV Credential issuance hardware and software support issues.

(c) Serves as the primary point of contact for vendors involved in the maintenance and operation of the PIV Credential issuance system.

(8) Local Office of Information and Technology (OIT) Staff

(a) Addresses all initial service requests related to PIV Credential issuance hardware and software and escalates service requests to the IT PIV Technical Team, as necessary.

(b) Works with the PIV Technical Team and the National Service Desk-Specialty to address PIV Credential issuance hardware and software support issues.

(9) National Service Desk- Specialty (NSD)

(a) Provides help desk support for the PIV system users related to PIV Credential issuance, including trouble ticket management and procedures for escalating issues to the PIV Technical Team.

(b) Interfaces with appropriate services, security, support groups, and organizations, as required.

(c) Works with the PIV Technical Team and local OIT staff to address PIV Credential issuance hardware and software support issues.

### **b. Facility PIV Official Roles**

(1) General

(a) The official titles for all PIV Official Roles in the PIV process contain "PIV" followed by the function title, such as "PIV Sponsor."



(b) VA requires a separation of duties in PIV Credential issuance whereby no single individual has the power to issue a credential without the involvement of, at a minimum, a second authorized person. The roles of Sponsor, Registrar, and Issuer are mutually exclusive for the issuance of a single credential. The VA PIV system role-based access control structure precludes role sharing during the PIV Credential issuance process.

(c) PIV responsibilities may be assigned as a full time position or as a collateral duty to designated VA agency personnel and VA contractors who have other primary duties.

(d) All individuals fulfilling a PIV Official Role are required to undergo training for that role. PIV Official Role certification training is valid for a period of one (1) year, at which time recertification must occur.

(e) All individuals fulfilling a facility PIV Official Role shall be formally appointed in writing by the PCI Manager. The PCI Manager is appointed by the facility director or equivalent position at that facility. All other roles are appointed by the PCI Manager.

(f) A backup shall be appointed by the PCI Manager for each role to ensure continuous operations of the PCI Facility.

(g) All individuals holding a PIV Official Role must be issued and possess a VA issued PIV credential.

(h) All individuals holding a PIV Official Role will be granted and possess the appropriate rights in the PIV system once the appropriate level of background investigation has been verified.

(2) Personal Identity Verification (PIV) Card Issuer (PCI) Manager:

(a) Is a Federal government employee.

(b) Shall be appointed within each VA organization as designated below:

1. VBA: the Chief of Support Services (CSS), the Officer in Charge in the event that there is no CSS, or a position as designated in writing by the Facility Director;

2. VHA: the Facility Director/ Regional Office Director or a position as designated in writing by the Facility Director/ Regional Office Director; and

3. All other facilities: the position equivalent to a Facility Director/ Regional Office Director or a position as designated in writing by the role equivalent to a Facility Director/ Regional Office Director.

(c) Will in place of or in conjunction with, the Registrar, have a completed favorable background investigation (MBI or higher), training for access to the Office of Personnel Management (OPM) Personnel Investigations Processing System (PIPS), and is granted access to the OPM PIPS to validate the initiation and status of Applicant background investigations.

(d) Manages PCI Facility staff performing credential issuance duties at that PCI Facility.

(e) Ensures the PCI Facility has a sufficient supply of all materials necessary to issue credentials; including card stock, electromagnetically opaque sleeves, lanyards, printer ribbons,

## VA HANDBOOK 0735

laminated, and other appropriate office supplies.

(f) Delegates and authorizes individuals to perform a PIV Official Role at that PCI Facility.

(g) Maintains a record of all PIV Role appointment letters, certification letters, and TMS certificates of completion (scanned electronic versions are sufficient).

(h) Manages the entire PIV system at the PCI Facility.

(i) Ensures that the badging life cycle at the PCI Facility complies with FIPS 201, NIST SP 800-79-1, and this Handbook.

(j) Corrects any irregularities to existing policies and processes which may occur during the credential life cycle and Applicant processing.

(k) Serves as the authoritative official that assumes responsibility and accountability for the complete PCI Facility credentials issuance process and lifecycle.

(l) Ensures the separation of duties between the Sponsor, Registrar, and Issuer roles.

(3) Sponsor

(a) Is a Federal government employee.

(b) Has a completed favorable background investigation (NACI or higher).

(c) Holds the following position for the identified applicant affiliation:

1. For VA employees, a Human Resources (HR) representative or designated supervisor;

2. For contractors, the Contracting Officer Representative (COR); and

3. For affiliates, the program coordinator, authorized administrator, or authorized supervisor of a specific program.

(d) Notifies the Applicant of all requirements for obtaining a credential, including proper Form I-9, *OMB No. 1115-0136, Employment Eligibility Verification*, compliant identity documents and completion of appropriate background investigation requirements, and assists them in completing registration requirements.

(e) Validates that an Applicant performing work for their organization has a need for access to VA facilities or network assets.

(f) Assures that the background investigation level selected for the Applicant is appropriate for the position.

(4) Registrar

(a) Is a Federal government employee or contractor.

(b) Has a completed favorable background investigation (MBI or higher).

(c) Holds no other role in the PIV Credential issuance process for a given Applicant.

(d) In place of, or in conjunction with the PCI Manager, undergoes the proper investigation, has a completed favorable background investigation (MBI or higher), and training for access to the OPM PIPS, and is granted access to the OPM PIPS to validate the initiation and status of Applicant background investigations.

(e) Reviews and validates the Applicant's identity proofing documents in accordance with Form I-9 and OMB guidelines.

(f) Reports to VA police, Federal Protective Service or other local Federal law enforcement officials when there is a reasonable suspicion that fraudulent identity documentation is presented by an Applicant as proof of identity.

(g) Validates that Applicants have the appropriate level background investigation scheduled or completed at OPM for the position, as defined by Sponsor.

(h) Collects the Applicant's biometrics and photograph.

(i) Evaluates the application in the VA PIV portal to determine whether a PIV application is satisfactory and applies VA-specific actions identified in the Operating Plan to reject an unsatisfactory PIV application.

(5) Issuer

(a) Is a Federal government employee or contractor.

(b) Has a completed favorable background investigation (NACI or higher).

(c) Holds no other role in the PIV Credential issuance process for a given Applicant.

(d) Prints and encodes all approved credential types and verifies that no errors were made during the encoding or printing process.

(e) Performs a visual verification of the Applicant's face against the photograph printed on the credential and the photograph stored on the credential and verifies the Applicant's identity by ensuring a (1:1) fingerprint biometric match occurs.

(f) Informs the Applicant of their responsibilities as a Cardholder prior to issuing the credential.

(g) Observes the Applicant sign for taking possession of the PIV Credential and officially releases the credential to the Applicant and provides the Applicant with the approved electromagnetically opaque sleeve and lanyard.

(6) Applicant

(a) Is a prospective or new VA employee, contractor, or affiliate requiring access to VA facilities or information technology (IT) resources

(b) Holds no official PIV role, other than as a requester for a PIV Credential.

## VA HANDBOOK 0735

(c) Provides all required demographic data, photograph, biometrics, and identity documents during the enrollment process.

(d) Completes, signs, and releases forms required for employment and/or background investigation (OF306, Standard Form 85, Standard Form 85P, Standard Form 86).

(e) Signs for acceptance of the credential and acknowledges Cardholder responsibilities for handling, protection, and use of the credential.

(f) Is referred to as the "Cardholder" upon acceptance of the credential.

(7) Cardholder

(a) Is a VA employee, contractor or affiliate in possession of a PIV Card, Non-PIV Card, or Flash Badge while on duty.

(b) Protects the credential's physical integrity and operability of the contactless and contact devices on the credential.

(c) Maintains possession of the credential on or about their person at all times while on official duty. The credential must not be left unattended as doing so risks unauthorized access, tampering or exploitation or loss and must be properly secured during off duty hours.

(d) Ensures the credential is stored in a GSA approved electromagnetically opaque sleeve provided by the PCI Facility when not in a card reader for logical access or when being presented to a card reader for physical access.

(e) Displays the credential at all times while at a VA facility inside the provided electromagnetically opaque sleeve and shall be worn and visible, above the waist on the outermost garment with the photo side visible. The only exception is where displaying the credential may cause a safety risk to a Cardholder, patient, or other individual. The Cardholder shall follow appropriate occupational safety requirements when conducting certain medical procedures or patient interactions, or when working around machinery with moving parts.

(f) Ensures that pins, buttons, badges, decals, or similar items are not added to the PIV Credential.

(g) Schedules a credential renewal with the badging office within 6 weeks prior to card expiration.

(h) Notifies the PCI Facility when:

1. The PIV Credential is lost or stolen;

2. The PIV Credential does not operate properly; or

3. Personal information that appears on the PIV Credential changes (e.g., changes in affiliation or a name change).

(i) Notifies local PCI Facility personnel, VA Police, and the Information Security Officer (ISO) within 4 hours when their PIV Card, Non-PIV Card is lost or stolen.

(j) Handles PIV Credentials found unattended as sensitive Personal Identifiable Information (PII) and return them to a local PCI Facility personnel.

(k) Returns the PIV Credential when access to VA facilities or information systems is no longer required or when a change in affiliation occurs.

### **3. CREDENTIAL TYPES, ELIGIBILITY, AND AFFILIATIONS**

#### **(a) General Guidance**

(1) PIV Cards, Non-PIV Cards, and Flash Badges issued in accordance with HSPD-12 and Federal Information Processing Standards (FIPS) 201, are the sole forms of federal credentials used by VA for identity verification of employees, contractors, and affiliates.

(2) The official names of the identity credentials issued by VA are PIV Cards, Non-PIV Cards, and Flash Badges. "PIV Credential" or "credential" may be used when formally referring to all three credential types.

(3) PIV Credentials are issued to vetted Applicants and are required for physical and/or logical access to VA facilities and information systems in accordance with HSPD-12.

(4) Non-expired PIV Credentials issued by other federal agencies shall be accepted as proof of identity and, upon electronic verification of the credential's validity and when proper authority is granted, may allow access to VA facilities and information systems.

(5) Credentials issued by VA organizations, such as those issued to VA Police, Office of the Inspector General (OIG) Inspectors, and Healthcare Professionals establish the authority and rights of the position of the individual carrying the credential but not the identity of the individual. These credentials must be used in combination with the PIV Credential to verify the Cardholder's identity.

(6) APPENDIX C: APPLICANT ELIGIBILITY AND ACCESS TYPE describes the criteria for Applicants who will receive a PIV Card, a Non-PIV Card, or a Flash Badge, based on the Applicant's length of service and access requirements, as determined by the position duties and/or employment duration. In addition, specific background investigation processing requirements are also dependent on the Applicant's access requirements.

(7) APPENDIX D: EMPLOYMENT ELIGIBILITY VERIFICATION describes the criteria for identity proofing Applicants who will receive a PIV Card, Non-PIV Card, or Flash Badge.

(8) APPENDIX E: CREDENTIAL TOPOLOGIES provides a list of fields included on PIV Cards, Non-PIV Cards, and Flash Badges, as well as visual examples of each credential.

#### **(b) Credential Types**

(1) Personal Identity Verification (PIV) Card

(a) PIV Cards allow access to VA facilities and information systems.

(b) PIV Cards may be issued to employees, contractors, and affiliates, including foreign nationals, who have a verified need to access VA facilities and information systems for a period of more than 180 consecutive or aggregate days in a 365 day period.

## VA HANDBOOK 0735

(c) PIV Cards are issued following, at a minimum, the completion and successful adjudication of a Special Agreement Check (SAC) (name and fingerprint check) and a scheduled National Agency Check with Written Inquiries (NACI) or higher level background investigation at OPM

(d) PIV Cards are issued following review of two Form I-9 approved identity documents, (APPENDIX D: EMPLOYMENT ELIGIBILITY VERIFICATION). One identity document must be a federal or state government- issued photo identification (ID).

(e) Continued possession and use of a PIV Card requires favorable adjudication of a NACI or higher background investigation.

(f) PIV Cards are valid for a period, from the credential issuance date, not to exceed three (3) years for employees and the lesser of three (3) years or contractor contract period of performance/work agreement expiration date plus option years for contractors or affiliates.

### (2) Non-PIV Card

(a) Non-PIV Cards are visually different from PIV Cards (APPENDIX E: CREDENTIAL TOPOLOGIES).

(b) Non-PIV Cards allow access to VA facilities and information systems.

(c) Non-PIV Cards may be issued to contractors and affiliates, including foreign nationals, who have a verified need to access VA facilities and information systems for a period of 180 consecutive or aggregate days or less in a 365 day period, over a 3 year period.

(d) Non-PIV Cards are issued following, at a minimum, the completion and successful recording of a Special Agreement Check (SAC) with no issues reported by OPM.

(e) Non-PIV Cards are valid for a period, from the credential issuance date, not to exceed three (3) years.

### (3) Flash Badge

(a) Flash Badges are visually different from PIV Cards and Non-PIV Cards. (APPENDIX E: CREDENTIAL TOPOLOGIES).

(b) Flash Badges allow access to common VA physical facilities. Flash Badges do not allow access to VA information systems or restricted areas.

(c) Flash Badges may be issued to contractors and affiliates, including foreign nationals, who have a verified need to access common VA physical facilities only for a period of 180 consecutive or aggregate days or less in a 365 day period.

(d) Flash Badges are issued following, at a minimum, the completion of an identity verification using one Form I-9 approved identity document with a photo.

(e) Flash Badges are valid for a period not to exceed one (1) year from the issuance date.

(4) Visitor Passes

- (a) Issuance of visitor passes is the responsibility and at the discretion of each Facility Director.
- (b) Visitor passes may be issued to individuals requiring short-term access to a VA facility for a period not to exceed 15 days in a 365 day period.
- (c) Visitor passes are issued on a daily basis and expire at the end of the day of issuance.
- (d) Visitor passes are issued following, at a minimum, review of one valid and current State or Federal government issued photo ID
- (e) Visitors must be escorted in areas restricted to the general public.

(5) Other Badges

- (a) Other badges not mentioned in this document may not be used for the purpose of FIPS 201 identity verification.
- (b) Facilities and organizations may issue other types of badges (i.e. hang tags) for use at their facility or within their organization. These badges are not required to be accepted at other VA facilities, except where granted by other VA policies, and do not provide proof of identity or access to the facility. Such badges may include position titles, names, and photos in any size or color variation deemed appropriate by the facility or organization. These badges may not be issued in place of and may only be used in concert with (to supplement) a PIV, Non-PIV, or Flash badge or visitor badge.

- (c) Other badges must be printed in a manner that does not resemble a PIV Credential.

**(c) Applicant Affiliations**

- (1) VA Employee. All appointive positions in VA as defined in 5 U.S.C. 2105, U.S.C. title 38.
- (2) Contractor. Individuals performing tasks or task orders under VA sponsored contracts the with the responsibility to perform services or tasks on legal contract with VA.
- (3) Affiliate. All individuals who serve VA through academic affiliation, volunteer services or Veterans Service Organization's (VSO's). See appendix A for additional description.
- (4) Foreign National. All Applicants (VA Employee, Contractor, or Affiliate) from designated and Non-designated countries, including lawful permanent residents. This does not include foreign born or naturalized United States citizens or individuals with a dual citizenship that includes the United States. Designated countries are those countries with which the United States has no diplomatic relations, countries determined by Department of State to support terrorism, countries under Sanction or Embargo by the United States, and countries of Missile Technology Concern. For additional information on designated countries please visit the Department of State website: [www.state.gov](http://www.state.gov)

## VA HANDBOOK 0735

(5) Federal Emergency Response Official (FERO). A FERO is a Federal employee or contractor who is responsible for the execution of, or performs duties in accordance with the responsibilities of, the National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), National Incident Management System (NIMS), and/or the National Continuity Policy Implementation Plan (NCPIP). The NCPIP includes Continuity of Operations (COOP) and Continuity of Government (COG) members. Public Law 110-53 applies to incident management personnel, emergency response providers, other personnel, and resources supporting the response to a natural disaster, act of terrorism, or other emergencies. All members of the VA Emergency Relocation Group (ERG) to include Crisis Response Team (CRT); Integrated Operations Center (IOC) Team; those with Devolution and Reconstitution roles (Devolution Emergency Response Group (DERG) and Reconstitution Emergency Relocation Group (RERG) will be authorized to be designated as a FERO.

### **(d) Exemptions**

(1) Individuals exempt from undergoing a background investigation (NACI or higher) in accordance with VA Directive 0710, *Personnel Security and Suitability Program*, shall be issued a Non-PIV Card.

(2) Individuals exempt from undergoing a SAC check in accordance with VA Directive 0710 shall be issued a Flash Badge.

(3) Individuals receiving an exemption from background investigations or SACs may be allowed access to VA facilities and information systems.

## **4. IDENTITY VERIFICATION AND CREDENTIAL ISSUANCE**

### **(a) Manage Credential Request**

(1) The Applicant Sponsor initiates a credential request in the PIV portal's Manager Section for a current or prospective Applicant. The credential request contains the following data:

- (a) Applicant Information;
- (b) Employment Information;
- (c) Type of Request and Employment Status;
- (d) Physical Security Access;
- (e) Contractors, Affiliates, and Temporary Employment Information; and
- (f) Manager Information.

(2) The credential request is electronically signed and submitted to the Sponsor.

### **(b) Sponsorship**

(1) The Sponsor receives and reviews the Manager approval and the credential request.

(2) The Sponsor approves or denies the credential request, establishing the bona fide



need for a relationship between the Applicant and VA. Approved credential requests are electronically signed by the Sponsor and submitted to the Registrar.

**(c) Registration**

(1) Prior to their new PIV Credential badging appointment, PIV Credential Applicants must have a new Special Agreement Check (SAC) completed, including adjudication. This applies even if the Applicant has a NACI on record. Exception: If a SAC has been completed, with no issues reported by OPM in the previous 120 days, the Registrar will accept the results of that recent SAC.

(2) The Registrar receives and reviews Manager and Sponsor signatures and reviews the credential request.

(3) The Registrar verifies the identity of the Applicant through review and validation of identity source documents (APPENDIX D: EMPLOYMENT ELEGIBILITY CRITERIA). All identity source documents must be current and unexpired. See Appendix.

(4) Identity documents that are unacceptable, invalid, or reasonably suspected of being fraudulent (e.g., absence of security hologram, or other known security feature; smeared ink; missing information; etc.) shall not be accepted. Registrars shall notify the Applicant, Sponsor, and PCI Manager that proper identity documentation was not provided and issuance of a PIV Credential was denied. In cases where the identity documentation is known or suspected of being fraudulent, Registrars should record information about the suspected identity documents and report documents to the PCI Manager for referral to VA police, Federal Protective Service or other local Federal law enforcement officials as appropriate. Suspect identity documentation should not be confiscated by PCI Facility personnel.

(a) Form I-9 approved identity documents must contain names that match the Applicant name in the credential request and the name on each I-9 approved identity document. Variations in names are not allowed unless a legal document addressing a name change (such as in the case of a marriage) is provided to validate the legal change of name.

(b) Form I-9 approved identity documents that do not pass Registrar review are rejected and another Form I-9 approved identity document must be provided and subjected to review.

(5) The Registrar verifies the Applicant's background investigation status using OPM PIPS.

(a) The Applicant has an investigation on file or scheduled at the Office of Personnel Management (OPM) that meets VA's Directive 0710 background investigation and reciprocity requirements.

(b) If no investigation is on file or scheduled at OPM, the appropriate personnel (i.e., Human Resource or Personnel Security and Suitability representative) initiates an invitation to the OPM Electronic Questionnaire for Investigations Processing (e-QIP) for the Applicant to complete the appropriate background investigation forms prior to PIV Credential issuance.

## VA HANDBOOK 0735

(6) The Registrar captures the Applicant's fingerprints (APPENDIX F: BIOMETRIC DATA CAPTURE).

(7) The Registrar captures the Applicant's facial image in a photograph (APPENDIX F: BIOMETRIC DATA CAPTURE).

(8) The Registrar electronically signs the credential request and submits the credential request to the Issuer.

### **(d) Issuance**

(1) The Issuer receives and reviews Manager, Sponsor, and Registrar signatures, and processes the credential request.

(2) The Issuer encodes the credential.

(3) The PIV system encodes the Applicant's photograph, the fingerprint templates, 4 required digital certificates (i.e., Digital Signature, Encryption, PIV Authentication and Card Authentication certificates), and any historical Encryption certificates from previously issued credentials.

(4) The Issuer prints the credential and verifies that no errors were made in printing. If errors were made, the credential is reprinted by the Issuer. Rejected credentials are documented as rejected and destroyed.

(5) The Issuer performs a visual verification of the Applicant's face against the photograph printed on the credential and the photograph stored on the credential.

(6) The Issuer verifies the Applicant identity by performing a one-to-one biometric match comparing the biometrics stored on the credential against those of the Applicant.

(7) The Applicant sets their six-digit Personal Identification Number (PIN) to securely lock the credential.

(8) The Applicant reviews and electronically signs the Card Acceptance Statement.

(9) The Issuer officially releases the credential to the Applicant and provides them with a lanyard and GSA approved electromagnetically opaque sleeve. Lanyards that meet local requirements (e.g., breakaway, organizationally unique) may be substituted at the discretion of the local PCI Manager.

## **5. CREDENTIAL MANAGEMENT LIFECYCLE**

**(a) PIV Credential Issuance.** Refer to Section 4, Identity Verification and Credential Issuance for issuance requirements.

### **(b) PIV Credential Use**

(1) PIV Cards, Non-PIV Cards, and Flash Badges are property of the U.S. Government. All personnel are responsible for appropriately safeguarding issued credentials; immediately reporting the loss or fraudulent use of a credential; challenging un-

carded personnel in restricted areas (when appropriate); notifying the proper authorities of a name change; properly displaying a credential when on a facility; and surrendering a credential upon resignation, retirement, expiration of contract or work agreement; or upon the direction of the issuing authority.

(2) Forging, falsifying, or allowing misuse of a credential or other forms of VA identification in order to gain unauthorized access to VA physical or logical resources is prohibited and may result in criminal sanctions and/or administrative penalties, including disciplinary or adverse personnel action and/or restricted or denied access to VA resources.

(3) PIV Credentials are to be returned to VA once an individual's association with VA has ended. Credentials should be returned to the HR Representative; Designated/ Authorized Supervisor; Program Coordinator; Authorized Administrator; or PCI Facility personnel no later than the last day of association with VA. PIV Credentials may not be kept as souvenirs.

(4) The credential and PIN shall not be shared with any other individual.

(5) Credentials should be kept inside the provided electromagnetically opaque sleeve.

(6) Credentials shall be displayed at all times while at a VA facility inside the provided electromagnetically opaque sleeve and shall be worn and visible, above the waist on the outermost garment with the photo side visible. The only exception is where displaying the credential may cause a safety disk to a Cardholder, patient, or other individual. The Cardholder shall follow appropriate occupational safety requirements when conducting certain medical procedures or patient interactions, or when working around machinery with moving parts.

(7) The Cardholder cannot alter the credential by applying elements such as stickers, permanent or temporary symbols, or the affixing of any device (e.g., tenure pin, service pin, lapel pin, etc.).

### **(c) Card Inventory**

(1) The PCI Manager or other appropriate authority shall designate, in writing, a point of contact (POC) who is responsible for receipt of, signing for, and inventory and storage of card stock.

(2) Card stock shall be accessible only by authorized personnel and maintained in a secure manner. Cards are stored using the following minimum requirements:

(a) Properly identified and treated as "controlled material" for inventory;

(b) Segregated from classified materials, firearms, ammunition, or currency;

(c) Stored in a secure area protected by guard(s), key lock(s), card reader(s) at all times; and

(d) Stored in a secure, GSA container.

(3) Card stock shall be monitored through the use of a log which includes the name of

## VA HANDBOOK 0735

the individual monitoring the inventory and the date and time of each of the following activities:

- (a) Card delivery;
- (b) Card printing;
- (c) Acceptance by the Applicant;
- (d) Date of return;
- (e) Date of termination; and
- (f) Date of destruction.

(4) Credentials that are lost, stolen, or unaccounted while in storage shall be reported immediately to the PCI Manager. The PCI Manager shall report this discovery to the HSPD-12 Program Office within 4 hours of notice. The PCI Manager shall immediately report incidents of lost or stolen credentials to the Information Security Officer (ISO) in accordance with VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*. The PCI Manager will forward a detailed report outlining all pertinent facts to the facility ISO within 2 days of receiving reports of the lost, stolen, or unaccounted credentials.

### **(d) Facility, organization, and office transfers.**

(1) VA PIV Credentials shall not be confiscated when a VA Cardholder transfers between VA facilities, organization, or offices.

(2) VA credentials will transfer with the Cardholder to the new VA Facility, organization, or office.

### **(e) Credential Acceptance at VA Facilities**

(1) VA PIV Credentials will be accepted at all VA facilities for access to Non-restricted areas at the facility.

(2) Access to restricted or exclusionary areas at each facility is handled through visual inspection by security guards or by use of Physical Access Control Systems (PACS) on an as-needed basis in compliance with access policies established by that facility.

(3) VA PIV Credentials will be accepted at all VA facilities for access to information systems on an as-needed basis in compliance with access policies established by that facility.

### **(f) Name changes**

(1) Cardholders who have legally changed their name must submit a request for a credential reissuance.

(2) The Cardholder shall undergo reissuance procedures and provide two (2) Form I-9

approved identity documents.

(3) One (1) identity document must reflect the name change and the other may reflect the name change or use the original name in combination with a legal name change document linking the two.

**(g) Personal Identification Number (PIN) Reset**

(1) Credentials that are locked due to a maximum of six consecutive invalid PIN entry attempts must have the PIN reset.

(2) It is the responsibility of the Cardholder to arrange for a PIN reset to occur.

(3) Verification of the Applicant's biometrics to those stored on the credential must occur prior to the PIN reset.

(4) PIN reset does not require the reissuance of a credential

**(h) Credential Renewal.**

(1) A Cardholder will be permitted to apply for a renewal 6 weeks prior to expiration of the credential.

(2) Prior to a PIV Credential renewal appointment, Applicants must have a new Special Agreement Check (SAC) completed, with no issues reported by OPM. This applies even if the Applicant has a NACI on record. Exception: If a SAC has been completed in the previous 120 days, the Registrar will accept the results of that recent SAC.

(3) The Sponsor verifies that the Applicant remains in good standing and approves the credential renewal.

(4) The Registrar verifies the Applicant's Form I-9 approved identity document(s) and the background investigation status of the Applicant.

(5) The Registrar collects a new facial image and new fingerprints from the Applicant.

(6) The Issuer verifies the Cardholder's identity against the biometric information stored on the expiring credential.

(7) The expiring PIV Credential is collected by the PIV Issuer and scheduled to be destroyed

(8) New digital certificates are generated and stored on the new credential. Historical certificates, if available, are stored on the new credential.

**(i) Credential Reissuance.**

(1) Cardholders are expected to apply for credential reissuance when the PIV Credential has been compromised, lost, stolen, or damaged; in the event of an employee, contractor, or affiliate status or attribute change, or if one or more digital certificates have been compromised or expired.

## VA HANDBOOK 0735

(2) Prior to PIV Credential reissuance, Applicants must have a new Special Agreement Check (SAC) completed, with no issues reported by OPM.

(3) A Cardholder will be permitted to apply for a renewal 6 weeks prior to expiration of the credential.

(4) The entire registration and issuance process is conducted, including fingerprint and facial image capture; and

(5) The employee, contractor, or affiliate personnel are current before reissuing credential and associated digital certificates.

### **(j) Defective Credentials.**

(1) PIV Cards and Non-PIV Cards that fail to encode or are rejected or not recognized by a card reader must be reported by the PCI Manager to the PIV Technical Team within five (5) days of encoding failure.

(2) Included in the report to the PIV Technical Team will be the credential identification number, a description of the failure, and any other pertinent information regarding the circumstances of the defective credential.

### **(k) Lost and stolen credentials**

(1) Lost or stolen credentials must be reported to the PCI Facility within 24 hours or the next business day of discovery of the loss/theft.

(2) Upon notification of a lost or stolen credential, the PCI Facility shall electronically terminate the credential within 4 hours, removing all electronic physical and logical access rights, and disabling digital certificates.

(3) The Cardholder's identity record and certificates shall not be deleted so that they can be recovered for reissuance.

(4) The Cardholder shall, within five (5) business days of reporting the loss or theft to the PCI Facility, report the loss or theft to their manager, must have a new Special Agreement Check (SAC) completed, with no issues reported by OPM (if one has not been completed within 120 days), appear in person at the PCI Facility with a signed memorandum from their manager acknowledging the loss or theft, undergo identity verification with two forms of Form I-9 approved identity documents, and be issued a new credential.

### **(l) Credential Recovery**

(1) Credentials that are delivered to the PCI Facility as having been left unattended should be handled as confidential media and treated as a recovered credential.

(2) The PCI Facility will attempt to notify the Cardholder to pick up their credential.

(3) Recovered credentials that cannot be returned to the Cardholder within 24 hours or by the next business day shall be treated as a lost credential and terminated.

(4) It is the responsibility of each VA Facility to establish additional procedures for handling recovered credentials and repeatedly lost credentials. Facilities may adopt any of the below methods for handling recovered or lost credentials or develop a policy of their own:

(a) Facility managers may not charge Cardholders a fee for lost or stolen credential reissuance.

(b) Require the Cardholder's manager approve issuance of a visitor pass;

(c) In the event of a forgotten PIV Credential, require the Cardholder to retrieve the credential prior to allowing entrance to the facility; or

(d) Allow issuance of a visitor pass to the Cardholder with verification of identity through a Form I-9 approved identity document such as a driver's license.

**(m) Credential Revocation**

(1) Credential must be recovered from the Cardholder under the following circumstances:

(a) Termination of employment or end of period of performance (contractor);

(b) Unfavorable fingerprint check (SAC) or background investigation adjudication; or

(c) Death of the Cardholder.

(d) An Applicant does not complete required actions for the appropriate level background investigations.

(e) An e-QIP application expires

(2) Revoked credentials require the following actions:

(a) The credential and all physical and logical access privileges are terminated;

(b) The credential is collected from the Cardholder; and

(c) The Sponsor is notified of the revocation.

**(n) Credential termination.**

(1) Credential termination deactivates the electronic aspects of the credential, making the credential non-functional in physical and logical access control systems, and schedules the credential for destruction

(2) Credentials must be terminated within 24 hours or by the next business day after receipt of the credential by the PCI Facility or notification of a lost or stolen credential.

(3) Credential may be terminated for any of the following reasons:

(a) The credential has been compromised (e.g., damaged, stolen, or lost).

(b) The credential was replaced as a result of renewal or reissuance.

## VA HANDBOOK 0735

(c) Cardholder separation from VA employment (death, retirement, resignation, end of period of performance or contract, separation from contract, or an end of VA affiliation).

(d) Cardholder is determined to have established a fraudulent identity.

(e) Cardholder has violated the Public Key Infrastructure (PKI) subscriber agreement or card holder agreement.

(f) Access to Federally controlled buildings or information systems is no longer required (this includes completion or termination of a contract and replacement or separation of contractor personnel).

(4) Credential termination process

(a) The credential is deactivated.

(b) The certificates on the credential are deactivated.

(c) The Sponsor and Cardholder are informed of the termination.

(d) The credential is collected and scheduled for destruction.

**(o) Credential destruction.**

(1) Credentials scheduled for destruction are those that have been terminated or have expired.

(2) Credentials will be destroyed within 5 business days of termination.

(3) Credentials are destroyed through cutting or crushing of the smart card's internal memory chip using metals snips, a pair of scissors, a strip or cross cut shredder (nominal 2 mm wide cuts), or incineration.

(4) PCI Manager keeps record of credential destruction by serial number for 3 years, which is subject to inspection.

## 6. APPEALS PROCESS

**(a) Background Investigation.** Denial of a PIV Credential resulting from unfavorable background adjudications shall be addressed in accordance with VA Directive and Handbook 0710, Personnel Security and Suitability Program.

**(b) Identity Proofing**

(1) Applicants will not be issued a PIV Credential until appropriate, valid, and authentic identity source documentation is provided. Applicants are granted two chances to provide acceptable identity documentation: the initial identity documentation presentation and the subsequent presentation to remedy the unacceptable documentation.



(2) The Sponsor shall make a determination, in consultation with the Applicant, to appeal to the PCI Manager for an additional attempt to provide acceptable identity documentation. The appeal shall be presented to the PCI Manager in-person with the following conditions:

(a) The Applicant shall be present and shall furnish acceptable identity source documentation; and

(b) The Sponsor shall be present. In cases where the Sponsor is unavailable to appear in-person because they work in a facility greater than a 1 hour commute from the PCI Manager's location, a signed and written letter stating the reason for the appeal shall be delivered to the PCI Manager. Delivery shall be accomplished through the fastest means possible, including e-mail or fax. The Applicant shall not be allowed to deliver the Sponsor's letter.

(3) Final determination to allow additional attempts to provide acceptable identity documentation is at the sole discretion of the PCI Manager and shall be made within two (2) business days of receiving the appeal request. .

(4) VA reserves the right and authority to direct that any denial decision be held in abeyance pending additional discretionary review by the Organization Identity Management Official (OIMO) for HSPD-12.

**c. Refusal to sign VA Card Acceptance**

(1) Applicants will not be issued a PIV Credential until they have signed the VA Card Acceptance agreement during the issuance process.

(2) Applicants who have been denied a PIV Credential resulting from refusal to sign the VA Card Acceptance must meet with their Sponsor within two (2) business days of the denial if they wish to begin the appeals process. Failure to meet this requirement constitutes a non-contest, no appeal will be granted, and no PIV Credential will be issued.

(3) The Sponsor shall make a determination, in consultation with the Applicant, to appeal an adverse PCI Manager decision to the Office of the General Counsel (OGC) to review the appeal for consideration.

(4) The OGC shall, in consultation with the OIMO for HSPD-12, review the terms of the appeal and make a determination within five (5) business days. The Applicant and Sponsor may be requested to provide information and/or participate in the determination process. Failure to provide information and/or participation, upon request by the OGC, renders no responsibility on the part of OGC and a determination shall be made based on the available information.

(5) Final results of the appeal decision shall be made available to the OIMO for HSPD-12, the PCI Manager, the Applicant, and the Sponsor. Further review of the decision is not provided for the following:

(a) The individual is known to be or reasonably suspected of being a terrorist;

(b) The employer is unable to verify the individual's claimed identity;

(c) There is a reasonable basis to believe the individual will attempt to gain unauthorized

## VA HANDBOOK 0735

access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;

(d) There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or

(e) There is a reasonable basis to believe the individual will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

(f) An Applicant does not have a right to appeal under the following circumstances:

(1) The Department, Administration, or the Office of Personnel Management (OPM) has determined that the Applicant is not suitable for Federal employment or employment at VA under the provisions of 5 CFR part 731.

(2) The Applicant's background investigation results are unfavorable for employment in a position held at the VA and the Department or Administration has removed the Applicant from employment or is proposing his/her removal.

(3) The Department or Administration has determined that the Applicant is not fit to hold a position in the excepted service or work on a VA contract and the Applicant is being removed from his/her position or from work on the contract, and will no longer have a need for regular access to a VA facility or information system.

(4) The Applicant fails or no longer meets any of the criteria for being issued a VA credential.

## 7. PIV PRIVACY GUIDELINES

(a) HSPD-12 Privacy Requirements. In addition to HSPD-12 privacy provisions, the following documents also apply to the PIV Credential issuance process: The Privacy Act of 1974 (5 U.S.C. 522a) and the E-Government Act of 2002 (Pub. L. 107-347, Titles I-III, 116 STAT. 2899-296), H.R. 2458 and S. 803, Office of Management and Budget (OMB) Memorandum 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003).

(2) Posting the Privacy Policy. It is a requirement of FIPS 201 to publish and post visibly in a PCI Facility, a clear and comprehensive document defining the types of information that will be collected for the VA PIV project and the use of that information. The VA PIV Privacy Policy is available from the HSPD-12 Program Management Office.

(3) Consent Policy. The VA PIV Enrollment Portal is the electronic system used for processing VA PIV credential requests. This portal requires the Applicant's digital signature and spells out in detail the use of personal information. By signing the form, the Applicant gives consent for the PCI Facility and the systems used during the lifecycle of the PIV Credential to maintain personal data in forms consistent with the privacy stipulations described in the Enrollment Portal as well as other privacy documents.

(4) **Limiting Collection.** Personal data is only collected on the PIV Enrollment Portal. Protections are in place, consistent with the System of Records Notice (SORN) and Privacy Impact Assessment (PIA) to restrict the data to only information that is necessary for the PIV process.

(5) **Ensuring Accuracy.** Data collected for the PIV system will be confirmed by PIV Officials and verified with the PIV Applicant during each step of the issuance process. Data is considered to be accurate at time of collection and it is the responsibility of the PIV Applicant to notify the Sponsor and PIV issuance office of any updates to the PIV information (name changed due to marriage, etc.).

(6) **Identifying Purposes for Collection of Data.** The reasons for collecting personal information during the HSPD-12 processes are clearly stated on all information collection forms. This positively identifies all PIV Applicants and establishes a chain of trust prior to issuing the PIV Credential. Employee, contractor, and affiliate information will be collected and maintained from individuals requesting a PIV Card, Non-PIV Card, and Flash Badge, for access to VA facilities and information systems. Information collected is as follows:

(a) PIV data collected, and its potential uses, shall be managed in accordance with the public SORN. The SORN can be found at: [Federal Register / Vol. 73, No. 58- SOR Records](#)

(b) A Privacy Impact Assessment (PIA) is conducted yearly by the Office of Information and Technology (OIT), which describes the types of information collected on Applicants, the purpose of that collection, what information may be disclosed to whom during the life of the PIV Credential, how the information will be protected, and the complete set of uses of the credential and related information at the VA. The PIA is an examination designed to identify and reduce the privacy and security risks associated with the use of personal information by a project, system or practice. The PIA provides a framework for ensuring that privacy, security and other vital data stewardship issues are identified, addressed and incorporated into the conception, design, operation, redesign, maintenance, and disposal of electronic information systems. The PIA forms the basis for yearly privacy reviews of all privacy-protected data as mandated by VA Directive 6502, VA Enterprise Privacy Program.

(7) VA maintains a Privacy Impact Assessment (PIA) which lists the types of information collected on PIV Applicants, the purpose of that collection.

(8) **Protecting Data Safeguards.** All documents with personal data on them are maintained in a secure location. Only certified PIV Officials are permitted access to the documents and only during specific phases of the issuance process. Data entered into computer systems are secured with the strongest known mechanisms of security that include PKI-based digital encryption or Role Based Access Control security models. Access to data is based on specific PIV roles and controlled based on the PIV process requirements.

(9) **Maintain Openness.** All documents describing the privacy requirements are available to the public and are posted in public spaces for easy access such as the [HSPD-12 Program intranet](#) and [internet](#) sites. Procedures for issuing credentials and the forms/data required for issuance are provided to the PIV Applicant before the issuance process begins.

(10) **Enable Avenues for Challenging Compliance.** If a violation of the policies and procedures is observed, that violation is handled in accordance with VA Directive 6502 and VA Directive 6500 as appropriate. Any complaints that are recorded should follow the

## VA HANDBOOK 0735

regulations cited in VA Handbook 6502.1, *Privacy Violation Tracking System (PVTS)*. Violations of the PIV privacy regulations should be reported immediately to the Facility Privacy Officer. The Facility PCI Manager and the Applicant's Sponsor should also be notified.

(11) Limited Access. VA enforces limited access to information in PIV systems to those persons with a legitimate need to know.

(12) Privacy Violations Policy. VA Directive 6502 and VA Handbook 6502.1 established a VA Privacy Security Event Tracking System (PSETS). Privacy violations that occur as part of the PIV project must adhere to this policy. In summary, the VA Handbook 6502.3 provides the following:

(a) Federal privacy regulations and guidance provide individuals with a right to complain about the manner in which VA maintains their privacy-protected data, or any other private information, and any observed or perceived lapses in protection of private information. The PSETS provides a VA-wide centralized, auditable database of all privacy complaints and violations.

(b) All sanctions are handled by the Office of Human Resources through the employee's manager/supervisor. Sanctions will be handled on a case-by-case basis, but will be consistent with possible sanctions listed in VA Handbook 5021, *Employee/Management Relations*, for "failure to safeguard confidential matter" and "violations of the Privacy Act." Sanctions for contractors and affiliates will be consistent with sanctions dictated within their contract.

## APPENDIX A: DEFINITIONS

1. **Access Control:** The process of granting or denying specific requests to obtain and use information and/or related information processing services (that is, logical access to VA information and information systems) and to enter specific physical facilities (that is, physical access to VA owned or leased buildings and spaces).
2. **Affiliate:** Individuals who require logical access to VA information systems and/or physical access to VA facilities to perform their jobs and who do not fall under the category of Federal employee or contractor. Examples include but are not limited to: Veteran Service Organizations (VSO) representatives, Joint Commission Reviewers, childcare staff, credit union staff, Union Officials and union support staff.
3. **Applicant:** An individual applying for a VA PIV, Non-PIV, or Flash Badge. An applicant may be a current or prospective Federal employee, contractor, or other individual requiring access to VA facilities, services, and/or VA information systems.
4. **Background Investigation:** The process by which the U.S Government establishes that applicants or incumbents, either employed by the Government or working for the Government under contract, are suitable for the job and/or eligible for a public trust or sensitive position.
5. **Biometric:** A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
6. **Certification:** The formal process of assessing the attributes (e.g., knowledge, availability, accountability, trustworthy, security) of a process, role, or task using various methods of assessment (e.g., interviews, document reviews, test results, evaluations, validation reports) that support the assertion of reliability and capability to perform the process, role, or task.
7. **Contractor:** An individual who is under contract for furnishing supplies and/or services to VA who will have access to VA information systems and/or physical access to VA facilities regardless of frequency or length of time.
8. **Credential:** Documentary evidence that attests to an individual's identity used to grant authorization to access VA facilities, services, and/or VA information systems. In this Handbook, a credential can be a PIV Card, Non-PIV Card, or Flash Badge.
9. **Employee:** Defined in title 5 U.S.C. 2105(a) as an individual who is appointed in the civil service and engaged in the performance of a Federal function under supervision by a Federal officer or employee. Title 38 Hybrid employee is an individual appointed on a temporary or permanent basis (full-time, part-time, or without compensation) under 38 U.S.C., chapters 73 and 74 in occupations (positions) identified in 38 U.S.C. 7401 (1) or (3).
10. **Federal information Processing Standards (FIPS):** A standard for Federal computer systems, for adoption and use by Federal agencies or a contractor or organization acting on behalf of a Federal agency, that has been developed and issued by the National Institute of Standards and Technology (NIST) and the Department of Commerce under 40 USC 11331.
11. **FIPS 201 Approved Products List (APL):** A list of products and services that are in

**VA HANDBOOK 0735**  
**APPENDIX A**

compliance with the current version of the Federal Information Processing Standard 201 and its supporting publications. Only those products and services (service providers) listed on the FIPS 201 APL are recognized as being in compliance with HSPD-12 and are authorized for procurement at VA.

12. **Flash Badge:** A VA identification (ID) credential containing a photograph issued to an individual for infrequent access to VA public areas only (such as cafeterias, lobbies, libraries, credit unions) for a period not to exceed one (1) year.
13. **Identification:** The process of discovering the true identity of a person defined by known or recognized characteristics such as birth place, age, and residence of a person.
14. **Identity:** The set of physical and behavioral characteristics by which an individual is uniquely recognizable.
15. **Identity Proofing:** The process of analyzing identity source documents provided by an applicant to determine if they are authentic and to perform background checks of the applicant to determine if the claim of identity is correct.
16. **Initiated:** The formal acceptance of an investigation for processing by OPM, denoted by a status of "scheduled" in the OPM PIPS.
17. **Interoperability:** For the purposes of this Handbook, interoperability allows any Federal government facility or information system, regardless of the PIV Issuer, to verify a Cardholder's identity using the certificates on the PIV Credentials.
18. **Logical Access Control System (LACS):** An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, credential, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.
19. **National Agency Check with Written Inquiries (NACI):** Conducted by OPM, this investigation covers a period of 5 years and consists of a review of current records in the OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and an FBI fingerprint check as well as written inquiries to previous employers and references listed on the application for employment. It is used for Non-sensitive or Low Risk positions in VA.
20. **Non-PIV Card:** A VA PIV Credential containing a photograph issued to persons who do not require a PIV Card but need unaccompanied, infrequent access to VA facilities or information systems for a period not to exceed three (3) years. In the case of health professions trainees in accredited training programs appointed under 38 U.S.C. Section 7405 or 7406, a Non-PIV Card may be used for access to VA facilities and information systems for the full duration of their training program however not to exceed three (3) years and Non-PIV Cards are collected and maintained at the facilities at the end of the individuals tenure or program.
21. **Personal Identity Verification (PIV) Card Issuer (PCI):** An authorized HSPD-12

compliant PIV Credential issuing organization that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the credentials with the identity credentials of the authorized subjects, and delivers the personalized credentials to the authorized subjects along with appropriate instructions for protection and use.

22. **PCI Facility:** PIV Card Issuance Facility that adequately houses and supports PCI personnel, storage of vital and sensitive records, test systems and associated components (hardware/software/firmware), and other operational components.

23. **PCI Manager:** The individual or entity responsible for the operations required of identity proofing and PIV Credential issuance performed by PIV role holders.

24. **PIV Card:** An identification credential that complies with FIPS 201 and related guidance that contains a photograph and stored identity information so that the claimed identity of the Cardholder can be verified by another person or an automated process. PIV Cards are issued to persons requiring more than 180 days access to VA facilities or information systems for a period not to exceed three (3) years.

25. **PIV Registrar:** The individual or entity who validates and vouches for the identity of an applicant to a PIV Issuer. The PIV Registrar authenticates the applicant's identity by checking identity source documents, identity proofing, and ensures a proper background investigations has been completed before the credential is issued.

26. **PIV Sponsor:** The individual who validates the need for a relationship between VA and the applicant and requests that a credential be issued to an applicant pending appropriate identity proofing and background investigations. This PIV official role must be performed by a Federal government employee.

27. **Physical Access:** Access to areas within or on a VA facility that may or may not be controlled by locks, card readers, guards, or other security devices.

28. **Physical Access Control System (PACS):** An automated system that manages the passage of people or assets through an opening (s) in a secure perimeter (s) based on a set of authorization rules.

29. **Resource:** For purposes of this Handbook, the term "resource" refers to any physical or logical asset including but not limited to buildings, rooms, data (electronic and paper), and information technology.

30. **Special Agreement Check (SAC):** A SAC is a fingerprint-only check. A successful recording of a SAC, with no issues reported by OPM, is required to obtain a PIV and Non-PIV Card.

31. **Visitor:** Any individual requiring escorted access and is on VA property fewer than fifteen (15) days in a 365 day period. Visitor Passes as stated in paragraph 2.a. are not governed by HSPD-12 policies. Issuance of visitor passes is the responsibility and at the discretion of each Facility Director.





**APPENDIX B: ACRONYMS**

Acronym	Definition
AOP	Agency Official for Privacy
CHUID	Card Holder Unique Identifier
COG	Continuity of Government
COOP	Continuity of Operations
COR	Contracting Officer Representative
CSS	Chief of Support Services
DAA	Designated Accreditation Authority
DCII	Defense Central Investigations Index
DOD	Department of Defense
e-QIP	Electronic Questionnaires for Investigations Processing
FBI	Federal Bureau of Investigations
FERO	Federal Emergency Response Official
FIPS	Federal Information Processing Standards
FTE	Full Time Equivalent
HR	Human Resources
HSPD	Homeland Security Presidential Directive
ID	Identification
ISO	Information Security Officer
IT	Information Technology
LACS	Logical Access Control System
LPR	Lawful Permanent Resident
MBI	Moderate Background Investigation
NACI	National Agency Check with Written Inquiries
NCPIP	National Continuity Policy Implementation Plan
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NRF	National Response Framework

**VA HANDBOOK 0735**  
**APPENDIX B**

Acronym	Definition
NSD	National Service Desk
OIT	Office of Information and Technology
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSP	Office of Operations, Security, and Preparedness
OIMO	Organization Identity Management Official
PACS	Physical Access Control System
PCI	PIV Card Issuing
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PIPS	Personnel Investigations Processing System
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SAO	Senior Agency Official
SAOP	Senior Agency Official for Privacy
SAC	Special Agreement Check
SF	Standard Form
SII	Security Investigations Index
SORN	System of Records Notice
SP	Special Publication
TMS	Talent Management System
U.S.	United States
U.S.C.	United States Code
VA	Department of Veterans Affairs
VSO	Veterans Service Organizations

**APPENDIX C: APPLICANT ELIGIBILITY AND ACCESS TYPE**

1. The following criteria must be reviewed by the Sponsor for all VA employees, contractors, and affiliates in order to determine the PIV Credential type to be issued to the Applicant based on physical and logical access requirements and the length of time the access is needed.

		PIV Credential Type		
		Flash Badge	Non-PIV Card	PIV Card
<b>PIV Credential Decision Criteria</b>		<b>Less</b> than 6 months or less than 180 aggregate days in a one year period	<b>Less</b> than 6 months or less than 180 aggregate days in a one year period	<b>More</b> than 6 months or more than 180 aggregate days in a one year period
<b>Access Requirements</b>	<b>Common Physical Access</b>	Yes	Yes	Yes
	<b>Restricted Physical Access</b>	No	Yes	Yes
	<b>Access to Sensitive Records</b>	No	Yes	Yes
	<b>Logical Access</b>	No	Yes/No*	Yes/No*
<b>Investigation Requirements</b>	<b>NACI (or higher B/I)</b>	No	No	Initiated
	<b>SAC</b>	No	Adjudicated	Adjudicated
	<b>Number of ID's</b>	1	2	2

\* An applicant may be issued a PIV Card or Non-PIV Card even though they do not require logical access



## APPENDIX D: EMPLOYMENT ELIGIBILITY VERIFICATION

1. The following criteria must be met by all VA employees, contractors, and affiliates prior to being issued a PIV Credential.
2. FIPS 201, Section 2.2 requires Applicants to provide two original forms of identity source documents. The identity source documents are taken from the list of acceptable documents included in *Form I-9, OMB No. 1615-0407, Employment Eligibility Verification*, dated March 8, 2013. At least one document shall be a valid State or Federal government-issued picture identification (ID).

### 3. Identity Document Criteria

- a. The Registrar must examine each Form I-9 approved identity document provided by the Applicant.
- b. All identity source documents must be unexpired.
- c. Any document that appears invalid (e.g., absence of security hologram, or other known security features, on a State issued driver's license; absence of security features on a birth certificate or passport; smeared ink; missing information; etc.) is to be rejected by the Registrar and reported to the facility PCI Manager for review.
- d. Handwritten or photocopied documents are not acceptable.

### 4. Acceptable Identity Documents.

- a. Two forms of identification are required from Table 1, Acceptable Identity Documents, for all PIV and Non-PIV Credentials. Flash Badges may be issued following review of a single identity document from Column A or B. The following combinations are accepted:
  - (1) Two forms of identification from Column A (Government Issued Photo ID);
  - (2) One form of identification from Column A and one form from Column B (Non-Picture ID or Acceptable Picture ID not issued by Federal or State Government);
- b. Persons under the age of 18 who are unable to present a document from Column A, may submit the following documents:
  - (1) School record or report credential, or
  - (2) Clinic, doctor, or hospital record.

### 5. Applicant Names

- a. The name of the Applicant in the credential request must match the name exactly as printed on at least one of the identity source documents. The names on the identity source documents must match using the examples in Table 2, Acceptable Name Mismatches and Table 3, Not Acceptable Name Mismatches.

**VA HANDBOOK 0735**  
**APPENDIX D**

- b. Applicants with multiple last names may use the guidance for middle names in Table 2, Acceptable Name Mismatches.
- c. An ID issued before a legal name change (e.g. birth certificate or driver's license) may be presented as one form of ID if a legal document (e.g. marriage certificate/license or a court order) is also presented linking the previous name to the current legal name. The linking document must display both the former and current legal names. Both documents must be valid and not expired. For example, a married woman may use both a certified copy of her birth certificate displaying her maiden name and a driver's license displaying her married name as the 2 forms of ID compliant with PIV Guidelines as long as she provides a marriage license displaying both her maiden name and married name.

Table 1. Acceptable Identity Documents

COLUMN A	COLUMN B
Government Issued Photo ID	Non-Picture ID and/or Acceptable Picture ID not issued by Federal or State Government
<ul style="list-style-type: none"> <li>• U.S. Passport or U.S. Passport Card</li> <li>• Permanent Resident Card or Alien Registration Receipt Card (Form I-551)</li> <li>• Foreign passport that contains a temporary I-551 stamp</li> <li>• Employment Authorization Document that contains a photograph (Form I-766)</li> <li>• Foreign passport with Form I-94 or Form I- 94A</li> <li>• Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A</li> <li>• Driver's license or Federal, state, or local government issued ID card with a photograph</li> <li>• School ID with photograph</li> <li>• U.S. Military Card</li> <li>• Military dependent's ID Card</li> <li>• U.S. Coast Guard Merchant Mariner Card</li> </ul>	<ul style="list-style-type: none"> <li>• Social Security Card</li> <li>• Original or certified Birth Certificate</li> <li>• Certification of Birth Abroad Issued by the Department of State (Form FS-545)</li> <li>• Certification of Report of Birth issued by the Department of State (Form DS-1350)</li> <li>• Voter's Registration Card</li> <li>• Native American Tribal Document</li> <li>• U.S. Citizen ID Card (Form I-197)</li> <li>• Identification Card for Use of Resident Citizen in the United States (Form I-179)</li> <li>• Employment Authorization document issued by the Department of Homeland Security</li> <li>• Canadian Driver's License</li> </ul>

Table 2. Acceptable Name Mismatches

Name	Acceptable First Name Mismatch	Acceptable Second Name Mismatch
First	"Mary L." (with "L." given as middle initial)	"Mary Lou"
Middle	Single letter as middle initial: "L." Compressed middle name: "Heewan"	Middle name spelled out, first letter of the name matches the single letter: "Lawrence" Properly-formed expansion of middle name: Hee-Wan
Last	"Smith-Jones"	"Smith Jones"

Table 3. Not Acceptable Name Mismatches

Not Acceptable Mismatches	First Name Source	Second Name Source
Apparent typo or transposition of letters	"John Smith"	"John Smyth"
Mismatch between given name and alias or nickname	"James"	"Jim"
First and Middle names swapped	"Eldon S. Smith"	"Scott Smith"
Mismatch of suffix	"Tom Smith Jr."	"Tom Smith"





## APPENDIX E: PIV CREDENTIAL TOPOLOGIES

1. PIV Card Topology can be found in Table 4, PIV Card Examples and Information. Refer to *NIST Special Publication 800-104, A Scheme for PIV Visual Card Topography* for additional information.
2. Non-PIV Card Topology can be found in Table 5, Non-PIV Card Examples and Information.
3. Flash Badge Topology can be found in Table 6, Flash Badge Example and Information.
4. Affiliation Coloration.
  - a. PIV and Non-PIV Cards contain a color coded photograph border based on the affiliation of the Cardholder. PIV Cards include a colored bar surrounding the name based on the affiliation of the Cardholder. Affiliations are colored in the following order priority:
    - (1) Foreign National – Blue Stripe
    - (2) Federal Emergency Response Official – Red Stripe
    - (3) Employee – White/No Stripe
    - (4) Contractor – Kelley Green Stripe
    - (5) Affiliate – Light Green Stripe
  - b. Flash Badges have a black photograph border and the name stripe has no color.
5. The back of each credential includes the information listed in Table 7, Credential Information (Back).
6. PIV Cards issued under the auspice of the Nation Nurses United (NNU) agreement have the RN designation. See examples listed in Table 8, RN Designation.

Table 4. PIV Card Examples and Information


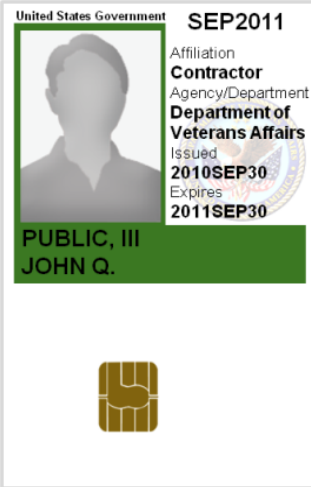













<p style="text-align: center;"><b>Employee</b></p>  <p>United States Government SEP2011 Affiliation <b>Employee</b> Agency/Department <b>Department of Veterans Affairs</b> Issued 2010SEP30 Expires 2011SEP30 <b>PUBLIC, III JOHN Q.</b></p>	<p style="text-align: center;"><b>Contractor</b></p>  <p>United States Government SEP2011 Affiliation <b>Contractor</b> Agency/Department <b>Department of Veterans Affairs</b> Issued 2010SEP30 Expires 2011SEP30 <b>PUBLIC, III JOHN Q.</b></p>	<p style="text-align: center;"><b>Top Left Section</b></p> <ul style="list-style-type: none"> <li>• “United States Government” header</li> <li>• Expiration Date: MMMYYYY format</li> <li>• Photograph with affiliation color border</li> <li>• Name with affiliation color bar</li> </ul> <p style="text-align: center;"><b>Top Right Section</b></p> <ul style="list-style-type: none"> <li>• Department Seal</li> <li>• Affiliation: Employee, Contractor, Affiliate, Foreign National</li> <li>• Agency/Department: Department of Veterans Affairs</li> <li>• Credential Issued Date: YYYYMMDD format</li> <li>• Credential Expiration Date: YYYYMMDD format</li> </ul> <p style="text-align: center;"><b>Bottom Center Section</b></p> <ul style="list-style-type: none"> <li>• Integrated Circuit Chip</li> <li>• Federal Emergency Response Official: “Federal Emergency Response Official” in red font at bottom center</li> </ul>
<p style="text-align: center;"><b>Affiliate</b></p>  <p>United States Government SEP2011 Affiliation <b>Affiliate</b> Agency/Department <b>Department of Veterans Affairs</b> Issued 2010SEP30 Expires 2011SEP30 <b>PUBLIC, III JOHN Q.</b></p>	<p style="text-align: center;"><b>Foreign National</b></p>  <p>United States Government SEP2011 Affiliation <b>Affiliate</b> Agency/Department <b>Department of Veterans Affairs</b> Issued 2010SEP30 Expires 2011SEP30 <b>PUBLIC, III JOHN Q.</b></p>	
<p style="text-align: center;"><b>Federal Emergency Responder</b></p>  <p>United States Government SEP2011 Affiliation <b>Employee</b> Agency/Department <b>Department of Veterans Affairs</b> Issued 2010SEP30 Expires 2011SEP30 <b>PUBLIC, III JOHN Q.</b>  <b>FEDERAL EMERGENCY RESPONSE OFFICIAL</b></p>		

Table 5. Non-PIV Card Examples and Information

<p style="text-align: center;"><b>Contractor</b></p> <p style="text-align: center;">United States Department of Veterans Affairs</p>  <p style="text-align: center;">PUBLIC, III JOHN Q.</p>   <p style="text-align: right;">Expires: 2011SEP30</p>	<p style="text-align: center;"><b>Affiliate</b></p> <p style="text-align: center;">United States Department of Veterans Affairs</p>  <p style="text-align: center;">PUBLIC, III JOHN Q.</p>   <p style="text-align: right;">Expires: 2011SEP30</p>	<p style="text-align: center;"><b>Top Center Section</b></p> <ul style="list-style-type: none"> <li>• “United States Government” header</li> <li>• “Department of Veterans Affairs” sub header</li> <li>• Expiration Date: MMMYYYY format</li> <li>• Photograph with affiliation color border in center</li> <li>• Name with no affiliation color bar</li> </ul> <p style="text-align: center;"><b>Bottom Center Section</b></p> <ul style="list-style-type: none"> <li>• Department Seal at bottom left</li> <li>• Integrated Circuit Chip</li> <li>• Credential Expiration Date at bottom right: YYYYMMDD format</li> <li>• Federal Emergency Response Official: “Federal Emergency Response Official” in red font at bottom center</li> </ul>
<p style="text-align: center;"><b>Foreign National</b></p> <p style="text-align: center;">United States Department of Veterans Affairs</p>  <p style="text-align: center;">PUBLIC, III JOHN Q.</p>   <p style="text-align: right;">Expires: 2011SEP30</p>		

**Table 6. Flash Badge Example and Information**

	<p style="text-align: center;"><b>Top Center Section</b></p> <ul style="list-style-type: none"> <li>• “United States Government” header</li> <li>• “Veterans Affairs” sub header</li> <li>• Photograph with black border</li> <li>• Name with no color bar</li> </ul> <p style="text-align: center;"><b>Bottom Center Section</b></p> <ul style="list-style-type: none"> <li>• Integrated Circuit Chip</li> <li>• Department Seal</li> <li>• Credential Expiration Date: YYYYMMDD format</li> <li>• FIPS 201 disclaimer: “This card is not FIPS 201 Compliant”</li> </ul>
---	---

**Table 7. Credential Information (Back)**

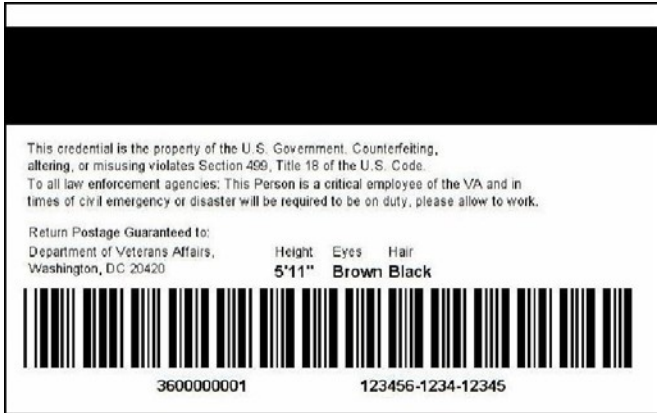

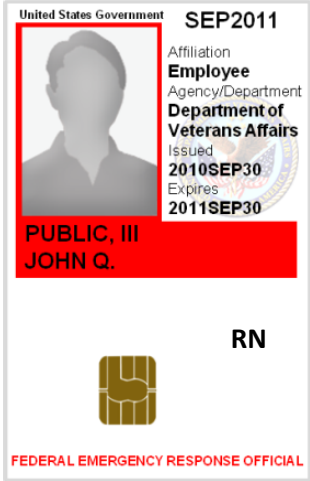
	<ul style="list-style-type: none"> <li>• Agency Card Serial number</li> <li>• Issuer Identification</li> <li>• Return if lost statement: “Return Postage Guaranteed to: Department of Veterans Affairs, Washington, DC 20420”</li> <li>• Federal Emergency Response Official Claimer: “The bearer of this card is a designated Emergency Responder. After PIV Card verification, bearer should be given access to controlled areas.”</li> <li>• Federal Property Claimer: “This credential is the property of the U.S. Government. Counterfeiting, altering, or misusing this credential violates section 499, Title 18 of the U.S. Code.”</li> <li>• Applicant information: Height, Eyes, Hair</li> </ul>
---	--

Table 8. RN Designation

RN, Employee	RN, Federal Emergency Responder
 <p>United States Government SEP2011 Affiliation <b>Employee</b> Agency/Department <b>Department of Veterans Affairs</b> Issued <b>2010SEP30</b> Expires <b>2011SEP30</b> PUBLIC, III JOHN Q. RN</p>	 <p>United States Government SEP2011 Affiliation <b>Employee</b> Agency/Department <b>Department of Veterans Affairs</b> Issued <b>2010SEP30</b> Expires <b>2011SEP30</b> PUBLIC, III JOHN Q. RN FEDERAL EMERGENCY RESPONSE OFFICIAL</p>



## APPENDIX F: BIOMETRIC DATA CAPTURE

1. The Registrar captures the Applicant's fingerprints in accordance with the below requirements:

a. The fingerprint capture method is determined based on the status of the Applicant's investigation.

(1) If a background investigation is on file or in progress, only flat fingerprints are required to be captured.

(2) If no background investigation is on file or in progress, both flat and rolled fingerprints are required to be captured.

b. Fingerprint Capture Issues. In cases where the fingerprint is impossible to capture due to damage, injury, or deformity, the Registrar should record those fingerprints or the entire hand, as applicable, as unable to be captured. In cases where the fingerprint is merely difficult to capture, the following procedures should be followed. If these techniques are unsuccessful, individual fingers should be recorded as unable to capture.

(1) Hands should be washed with soap and water prior to being fingerprinted to remove dirt and oils.

(2) If hands are moist, wipe each finger with rubbing alcohol (as it will dry out the skin) or other drying agent such as corn starch.

(3) If hands are dry or flaky, moisten the fingers with a small amount of water or use a small amount of hand lotion and wipe off any residue.

(4) An individual, by the nature of their work or age, may have very thin or worn ridges in the pattern area. Apply light pressure to record these types of fingerprint impressions. A technique known as "milking the finger" can be used to raise the fingerprint ridges prior to printing. This technique involves applying pressure or rubbing the fingers in a downward motion from palm to fingertip.

c. Fingerprint Capture Order. Capture fingerprints in the following order:

(1) Right index finger

(2) Left index finger

(3) Right thumb

(4) Left thumb

(5) Right middle finger

(6) Left middle finger

(7) Right ring finger

**VA HANDBOOK 0735**  
**APPENDIX F**

- (8) Left ring finger
- (9) Right little finger
- (10) Left little finger

2. The Registrar captures the Applicant's facial image with a photograph in accordance with the below requirements:

a. The Applicant's facial expression shall be neutral (non-smiling) with the mouth closed.

b. The photograph must include the entire face, from natural hairline to the chin and from ear to ear at the point which the head and ear connect in the front. The face may not be obscured by dark glasses, hats, scarves, or other facial or head coverings.

c. Eye patches that do not obscure an excessive portion of the face need not be removed.

d. Eye patches, dark glasses, non-prescription glasses, or head coverings are allowed for medical reasons only. Medical certificates must be provided to validate the need for the covering. PIV Credentials issued to individuals with medically certified coverings must be issued with an expiration date not to exceed the length of treatment for temporary medical conditions. A full expiration PIV Credential may be issued to individuals with permanent conditions or when the covering is no longer necessary and an un-obscured full-facial photograph can be captured.



**APPENDIX G: CREDENTIAL DESTRUCTION**

1. In accordance with NIST SP800-88, *Guidelines for Media Sanitization*, the following cases will result in credential destruction:

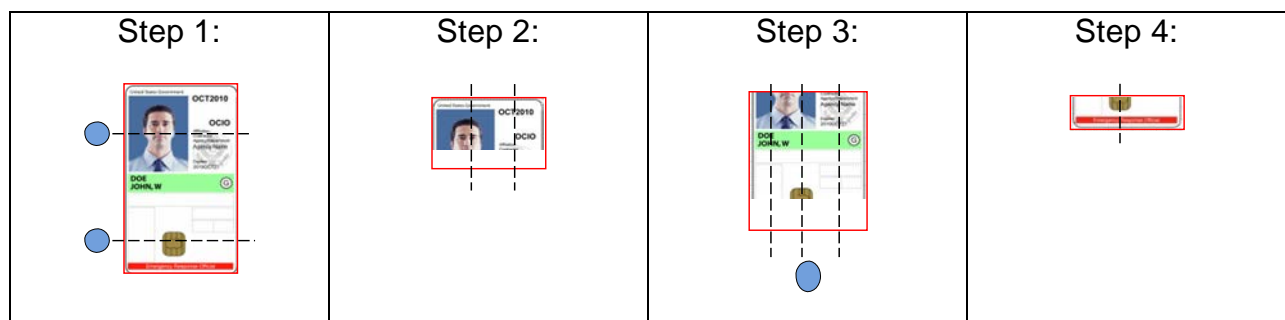
- a. A Federal employee, contractor or affiliate separates (voluntarily or involuntarily) from a Federal agency
- b. An employee, contractor or affiliate changes positions and no longer needs access to government owned or leased buildings, space or IT systems
- c. A credential holder is determined to hold a fraudulent identity
- d. A credential holder passes away
- e. A credential holder had his/her credential replaced due to a Reprint or Reissuance
- f. A credential holder’s final investigation is deemed unfavorable by OPM, Personnel Security and Suitability and HR
- g. The credential expires
- h. When a credential is returned after being out of direct control of the Credential Holder, in accordance with Federal PKI Policy

2. PCI-Managers are responsible for ensuring and verifying that PCI Facilities are in compliance with PIV card stock destruction policies as outlined in NIST policies. PCI-Managers or Facility Directors have the following options regarding PIV credential/card destruction depending on the volume produced:

a. Destruction by Cutting:

(1) Cut the PIV Credential along the lines shown in the diagram below, ensuring that the microchip is cut through the center. Dispose of the remains in a secure collection bin

Table 9: Destruction by Cutting



b. Destruction by Strip Shredder:

(1) A strip shredder that conforms to NIST SP 800-88 (“nominal 2 mm wide cuts”)

c. Destruction by Disintegration/Incineration:

**VA HANDBOOK 0735**

**APPENDIX G**

(1) A commercial Disintegration or Incineration service provider complying with NIST SP 800-88 (“destroy via incineration licensed incinerator or disintegration to 2mm size particles”)

d. Destruction by a Third Party:

(1) Third party vendors with proper background investigations that provide on or off site secure destruction services and conform to the NIST SP 800-88 guidelines (“cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts) or destroy via incineration licensed incinerator or disintegration to 2mm size particles”)

(2) Possible sources for compliant Shredders or Services can be found at <https://www.gsaadvantage.gov>