HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12, PERSONAL IDENTITY VERIFICATION, CREDENTIAL MANAGEMENT PROGRAM

1. **REASON FOR ISSUE**: This handbook defines roles, responsibilities, processes, and procedures, in conjunction with Department of Veterans Affairs (VA) Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) Credential Management Program, for the use, administration, and governance of PIV card credentialing services within VA.

2. **SUMMARY OF CONTENT/MAJOR CHANGES:** This handbook sets forth updated roles and responsibilities for an HSPD-12 Program that integrates PIV card and Physical Access Control System (PACS) capabilities within VA. This Handbook:

   a. Provides information about the processes and procedures that are performed by PIV credentialing services role holders to support the operations of the General Services Administration's (GSA) managed and shared PIV credentialing services system, "USAccess," for the VA enterprise.

   b. Provides additional details about the credential types to reflect the transition from PIV, Non-PIV, and Flash PIV cards under VA's legacy Credential Management System (CMS) to PIV, PIV-I, and PIV-I Flash cards under the USAccess system.

   c. Updates the facial image capture policy to include information on acceptable religious head coverings.

   d. Updates PIV card requirements consistent with the December 15, 2020, Office of Personnel Management (OPM) Memorandum. "Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirements for Suspension or Revocation of Eligibility for PIV cards (Credentialing Procedures)", and Federal Information Processing Standards (FIPS) Publication 201-3, or its successors.

3. **BACKGROUND:** VA has leveraged USAccess as the CMS, a managed shared service from GSA. The VA credentialing services role holders can access the USAccess portal to perform credentialing services for the VA staff. USAccess is VA's next-generation (NextGen) PIV Credential solution that replaced the VA legacy CMS PIV card equipment and systems across the VA enterprise. The USAccess system provides participating Government agencies with all the key components necessary to manage the entire lifecycle of a PIV card with secure and efficient Identity Credentialing and Access Management (ICAM) solutions. USAccess allows for a single system to enroll applicants, activate, manage, suspend, reprint, or revoke PIV cards, and manage appointments and sponsorship, maintaining a common identity credential for each applicant by including built-in workflow processes at every stage of the credentialing process.

4. **RESPONSIBLE OFFICE**: Office of Human Resources and Administration/ Operations, Security, and Preparedness (006), Office of Operations, Security, and Preparedness (007), Office of Personnel Vetting and Credentialing Management (PVCM), HSPD-12 and Credential Management.

5. **RELATED DIRECTIVES AND HANDBOOK**: VA Directive 0735; VA Directive and Handbook 6510, VA Identity and Access Management; VA Directive 6500, VA Cybersecurity Program; and VA Handbook 6500, Risk Management Framework for VA Information Systems.

6. **RESCISSIONS**: VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, dated March 14, 2014.

CERTIFIED BY:

/s/
Nathan T. Sanfilippo
Acting Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Mark R. Engelbaum
Assistant Secretary for
Human Resources and Administration/
Operations, Security, and Preparedness

DISTRIBUTION: Electronic Only

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12, PERSONAL IDENTITY VERIFICATION, CREDENTIAL MANAGEMENT PROGRAM

TABLE OF CONTENTS

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) PROGRAM

1. **INTRODUCTION.**

a. Background:

(1) Office of Management and Budget (OMB) Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, sets forth the Federal Government's Identity, Credential, and Access Management (ICAM) policy and includes guidance for contextualizing identity in the Federal Government; managing identities, credentials, and access in modern Government; adapting the Government's approach to Homeland Security Presidential Directive 12 (HSPD-12); shifting the operating model beyond the perimeter; improving digital interactions with the American public; and enumerating Government-wide responsibilities.

(2) HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors, mandates the issuance of a standard and reliable form of identification for Federal employees and contractors in compliance with technical and procedural requirements defined in the latest version of FIPS 201-3 publication, Personal Identity Verification (PIV) of Federal Employees and Contractors.

(3) HSPD-12 directs all Federal Departments and Agencies to issue Government employees, contractors, and affiliates an identity verification credential that provides the attributes of security, authentication, trust, and privacy and that can be used to verify identities to enter Federal buildings or gain access to Federal computer networks.

(4) As the Federal Government’s Credentialing Executive Agent (CEA), OPM issued guidance in December 2020 that provided updated Government-wide credentialing standards procedures to be used by all Executive Branch Departments and Agencies (D/As) in issuing, suspending, or revoking eligibility for HSPD-12 PIV cards to their employees, contractors, and affiliates, including non-United States (U.S.) nationals.

b. Purpose:

(1) The purpose of VA Handbook 0735 *Homeland Security Presidential Directive 12 (HSPD-12) Program*, in alignment with the policies and responsibilities defined in VA Directive 0735 *Homeland Security Presidential Directive 12, Personal Identity Verification, Credential*

Management Program, is to provide guidance regarding the usage, administration, and governance of VA identity credentials.

(2) The VA credentialing services role holders supporting the PIV credential processes at VA facilities must read this handbook and use it as a reference to understand the roles and responsibilities necessary for implementing VA Directive 0735 *Homeland Security Presidential Directive 12, Personal Identity Verification, Credential Management Program*.

c. Scope: This Handbook:

(1) Defines the roles of the VA credentialing services role holders supporting the PIV processes under USAccess at VA facilities.

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

(3) Provides guidance for issuing PIV, PIV-I, and PIV-I Flash cards in USAccess for access by VA employees, contractors, and affiliates.

(4) Provides guidance on using identity credentials for physical and logical access.

d. Applicability:

(1) Applies to VA facilities that issue PIV cards, referred to as a VA PIV Credential Issuance Facility (PCIF).

(2) Applies to VA-owned, leased, and contracted facilities, other Government agencies that support VA's mission requirements, or any other third-party utilizing VA's information to perform a VA-authorized activity.

(3) Applies to VA employees, contractors, and affiliates requiring long-term or short-term access to VA facilities or information systems to perform a VA-authorized activity.

(4) Applies to VA credentialing services role holders and other roles that support PIV credential processes and functionality.

(5) Applies to any office that is unable to comply with specific requirements in the VA Directive and Handbook 0735 can submit a written waiver (policy exception) request memorandum to the VA Secretary through the VA HSPD-12 Credential Program Management Office and the VA Chief, Operations, Security, and

Preparedness (OSP). The Chief, OSP will coordinate the consideration of any waivers and policy exceptions with the appropriate offices such as the Office of General Counsel (OGC). Policy waivers and exceptions and associated risk acceptance determinations will need to be approved by the VA Secretary, or Deputy Secretary.

2. HSPD-12 PROGRAM ROLES AND RESPONSIBILITIES.

a. Senior Authorizing Official (SAO):

(1) In accordance with VA Directive 0735, *HSPD-12 PIV Credential Management Program*, the Chief, OSP is the SAO for the VA HSPD-12 Program.

(2) The SAO provides oversight for the VA's HSPD-12 PIV Credential Management Program.

b. Designated Authorizing Official (DAO):

(1) Designated by the Assistant Secretary for Information and Technology, Chief Information Officer, or designee.

(2) Reviews certification documentation and the recommendation prepared by the Assessor/Certification Agent and issue appropriate Authorities to Operate (ATOs) for VA PCIFs.

(3) Issues appropriate ATOs for VA identity management systems that may be implemented on the VA network in support of the creation, issuance, usage, maintenance, distribution, and revocation of identities and identity credentials for all VA employees, contractors, and affiliates accessing VA facilities and information systems and any users who require logical access to VA information services.

c. Assessor:

(1) The Assessor for the VA HSPD-12 PIV Credential Management Program is the Chief, OSP.

(2) The Assessor shall:

(a) Be organizationally separate from the person(s) and the office(s) and not directly responsible for the day-to-day operation of identity management for VA. The correction of deficiencies and discrepancies identified during the assessing process will be completed using independent reviews from the

Assessor, who is organizationally separate from the day-to-day operations.

(b) Conduct reviews, by National Institute for Standards and Technology (NIST) Special Publication (SP) Guidelines for the Accreditation of Personal Identity Verification Card Issuers 800-79-2, of the programs and procedures established in this document for the issuance of PIV cards.

(c) Assure that VA has adopted and uses approved identity proofing, registration, issuance, and lifecycle maintenance processes as required in FIPS 201-3 and that all the necessary roles, responsibilities, activities, and actions specified in the approved model are adequately documented. For additional information, see VA Handbook 6510, *VA Identity, Credential, and Access Management*.

d. Organization Identity Management Official (OIMO):

(1) The OIMO for the VA HSPD-12 PIV Credential Management Program is the Executive Director of the Office of Personnel Vetting and Credential Management (PVCM). The OIMO or designee shall:

(a) Implement the organization's policies, ensuring that all procedures are performed, and provide guidance and assistance to VA PCIFs.

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

(c) Ensure that all credential issuance services, equipment, and processes meet FIPS 201-3 requirements and NIST SP 800-79-2 standards.

(d) Monitor and coordinate activities with VA PCIF Managers.

(e) Support and maintain the NIST SP 800-79-2 assessment and authorization process.

(f) Develop and issue policies and procedures through guidance, such as guides, handbooks, directives, and memoranda, regarding the implementation of the HSPD-12 Program.

(g) Address policy and program questions and issues that arise during all phases of the PIV Credential management lifecycle through the HSPD-12 CM Help Desk mailbox vacohspd12pmo@va.gov.

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

(i) Work with the VA Technical Team within the Office of Information and Technology (OIT) and GSA to monitor system issues and resolve any identified operational problems with the USAccess system operations.

(j) Ensure that an accurate inventory is maintained to account for all active PIV cards and for PIV cards reported as lost, stolen, destroyed, or deactivated.

e. VA HSPD-12 PIV Credential Management Team (HSPD-12 CM team):

(1) VA Technical Team within the Site Office of Information and Technology (OIT Technical Team), in collaboration with the HSPD-12 CM team and GSA team, provides support for the infrastructure for USAccess. HSPD-12 CM team also coordinates for resolution of any USAccess issues identified that may require support and assistance from both GSA and VA teams. HSPD-12 CM team shall:

(a) Address technical credential management issues during all phases of the PIV credential management lifecycle for the VA PIV system identified in this document. For USAccess, the HSPD-12 CM team will coordinate primarily with GSA and the OIT Technical Team (as needed) to address technical credential management issues.

(b) Work with local information resource managers, information security officers, and the Enterprise Service Desk (ESD) to address credential issuance hardware and software support issues with the HSPD-12 CM team and GSA. Perform HSPD-12 help desk responsibilities for USAccess: the current OIT Service Desk process will document issues and provide tickets to OIT to validate that VA’s information technology (IT) infrastructure is not the cause of system issues impacting USAccess operations.

(c) Serve as the primary point of contact for vendors involved in USAccess maintenance and operation. The HSPD-12 CM team will work with GSA and serve as the primary point of contact for USAccess; the HSPD-12 CM team will communicate with the OIT Technical Team as required to validate that VA’s IT infrastructure is not the cause of system issues impacting USAccess maintenance and operations.

f. OIT Staff shall:

(1) Address all initial service requests related to VA USAccess PIV system credential issuance hardware and software; escalate service requests to the OIT Technical Team, as necessary; and coordinate with the HSPD-12 CM team, which will work with GSA to submit service requests related to the USAccess system.

(2) For the USAccess PIV system, the OIT Technical Team will coordinate with the HSPD-12 CM team, who will work with GSA to address hardware and software support issues related to the USAccess system.

g. OIT Enterprise Service Desk (ESD):

(1) Shall work with the HSPD-12 CM team, who will collaborate with GSA to provide help desk support for USAccess system users.

h. The USAccess Help Desk, under the purview of the OIMO, shall:

(1) Provide help desk support for the USAccess role holders. These personnel have designated roles and responsibilities in USAccess related to PIV credential issuance, enrollment, and hardware/software troubleshooting.

(2) Work with local OIT staff to address USAccess hardware and software issues.

i. PIV Credential Issuance Facility (PCIF) Roles:

(1) General:

(a) FIPS 201-3 requires a separation of duties in PIV credential issuance whereby no single individual has the power to issue a credential without the cooperation of another authorized person.

(b) Within the USAccess system, the PIV Sponsor, PIV Adjudicator, and PIV Registrar roles are mutually exclusive for issuing a single credential, thus maintaining separation of duties. The separation of duty rules dictate that no single role holder can act as an individual Applicant's PIV Sponsor, PIV Adjudicator, and PIV Registrar. For example, the same person who sponsored an Applicant cannot adjudicate that Applicant or enroll that Applicant and vice versa.

(c) PIV responsibilities may be assigned as a full-time or collateral duty to designated VA Agency personnel and VA contractors with other primary responsibilities.

(d) Role holders in VA's USAccess system are required to take USAccess training specific to their assigned role. USAccess official role certification training is valid for a period of three (3) years, at which time recertification must occur; OSP will track certification training compliance.

(2) Role Mapping: USAccess Roles:

(a) The table below presents the list of roles within the USAccess system:

Table 1: USAccess System Roles

VA's USAccess System Roles
Agency Site Manager
Agency Role Administrator
Agency Security Officer
Local Site Manager
PIV Adjudicator
PIV Sponsor
PIV Registrar
PIV Activator
PIV Print Operator
PIV Credential Inventory Tool Operator
Report Viewer

(b) Under the USAccess system, the roles of Agency Site Manager, Agency Security Officer, and Agency Role Administrator are not considered full-time duties.

(c) All individuals fulfilling an official PCIF role: PIV Registrar, PIV Activator, and PIV Print Operator under the USAccess system shall be formally appointed in writing by the PCIF Manager. The office appoints the PCIF Manager and is responsible for the management and operation of the PCIF at that facility location. In the case of most Veterans Health Administration (VHA) facilities, Chief Human Resource Officials (CHROs) should appoint PCI Managers because the PIV staff fall under Human Resources.

(d) The PCIF Manager shall appoint a backup for each role to ensure continuous PCIF operations.

(e) All individuals holding an official PIV role must be issued and possess a VA USAccess-issued PIV card.

(f) Once the appropriate level of background investigation has been verified, all individuals holding an official PIV role will be granted and possess the appropriate access to the USAccess system.

(g) All designated requirements for Federal employees, contractors, or affiliates per role are at the discretion of VA.

(3) VA USAccess Roles:

(a) PCIF Manager, Agency Security Officer, and Agency Site Manager:

i Is a Federal Government employee.

ii Must have completed the VA or GSA training specific to PCIF Manager and/or Agency Security Officer training.

iii Shall be appointed within each VA organization as designated below:

(A) Veterans Benefits Administration (VBA): Appointment by the Chief of Support Services (CSS), the Officer in Charge, if there is no CSS or a position as designated in writing by the Facility Director.

(B) VHA: Appointment by the Facility Director/ Medical Center Director or is appointed by the office responsible for the management and operation of the PCIF at that facility location. In the case of most VHA facilities, CHROs should appoint PCI Managers because the PIV staff falls under Human Resources.

(C) All other facilities: Appointment by the VA office having responsibility for management and operation of the PCIF at that facility location or by the position equivalent to a Facility Director/ Regional Office Director, Medical Center Director, or a position as designated in writing by the role equivalent to a Facility Director/ Regional Office Director, or Medical Center Director.

(D) Will, in place of or in conjunction with the PIV Registrar, have a completed favorable background investigation (Tier 2 minimum) and be granted access to the OPM Personnel Investigations Processing System (PIPS) and Veterans Affairs Centralized Adjudication Background Investigation System (VA-CABS) to validate the initiation and status of Applicant background investigations. See VA Handbook 0710, *Personnel Security and Suitability Program* for additional information.

iv Manages PCIF staff performing credential issuance duties at that PCIF.

v Ensures the PCIF has enough supply of all materials necessary to issue credentials, including card stock, electromagnetically opaque sleeves, lanyards, printer ribbons, laminate, and other appropriate office supplies.

vi Delegates and authorizes individuals to perform a PIV official role at that PCIF.

vii Maintains a record of all PIV role appointment letters, certification letters, and Talent Management System (TMS) certificates of completion (scanned electronic versions are sufficient).

viii Manages the entire PIV system at the PCIF.

ix Ensures that the badging lifecycle at the PCIF complies with FIPS 201-3, NIST SP 800-79-2, and this handbook.

x Corrects any irregularities to existing local processes that may occur during the credential lifecycle and Applicant processing at the PCIF.

xi Is the authoritative official that assumes responsibility and accountability for the complete PCIF credential issuance process and lifecycle.

xii Ensures the separation of duties between the PIV Sponsor and PIV Registrar roles under USAccess.

(b) PIV Sponsor:

i Is a Federal Government employee.

ii Has a completed favorable background investigation (Tier 2 or higher).

iii Must have completed USAccess PIV Sponsor training.

iv Notifies the Applicant of all requirements for obtaining a credential, including acceptable identity documents and completion of appropriate background investigation requirements, and assists them in completing registration requirements.

v Validates that an Applicant performing work for their organization need access to VA facilities or network assets.

vi Assures that the background investigation level selected for the Applicant is appropriate for the position.

vii The PIV Sponsor is required to validate if the individual is assigned to a position designated as a Federal Emergency Response Official. The PIV Sponsor will validate the designation with the employee's supervisor or with the OSP Office of Emergency Management and Resilience (OEMR) before the individual can be authorized for issuance of a PIV card with a red stripe.

viii The PIV Sponsor role is designated by the Program Office (Mission Owner) authorized official, and the Agency Role Administrator assigns the role in the USAccess system.

ix The PIV Sponsor is responsible for ensuring proper issuance and collection of the PIV card when it is no longer

needed. The PIV Sponsor may hold different positions as it relates to the identified PIV Applicant affiliation:

(A) For VA employees, a Human Resources (HR) representative and/or designated supervisor.

(B) For VA contractors, an authorized official and/or a designated supervisor assigned by the Program Office (Mission Owner).

(C) For affiliates, the program coordinator, authorized supervisor of a specific program, or an authorized administrator.

x The PIV Sponsor ensures that PIV cards have been returned by an Applicant to the appropriate VA authorities, such as to the PIV Sponsor of record, Supervisors, Program Offices' authorized officials, and PCIFs for termination and de-activation when the VA PIV cardholder no longer requires access to VA information systems, controlled facilities, and secured areas. The PIV card must be returned or collected no later than five (5) days from the last day of employment.

(c) PIV Adjudicator:

i Is a Federal Government employee.

ii Has a completed favorable background investigation (Tier 2 or higher).

iii Must have completed USAccess PIV Adjudicator training.

iv Updates and records the status of adjudication results for the National Agency Check with Inquiries (NACI), the Federal Bureau of Investigation (FBI) National Criminal History Checks (NCHC), and the Agency-Specific Criteria of an Applicant in the USAccess system. A positive adjudication result will initiate the PIV card issuance process.

v The PIV Adjudicator is designated by the Program Office (Mission Owner), and the Agency Role Administrator assigns the role in the USAccess system.

(d) PIV Registrar:

i The PIV Registrar role is designated by the PCIF Manager.

ii Is a Federal Government employee, contractor, or affiliate.

iii Has a completed favorable background investigation (Tier 2 or higher).

iv Must have completed USAccess Registrar training.

v Holds no other role in the PIV credential issuance process for a given Applicant within USAccess except for PIV Activator, PIV Print Operator, PIV Credential Inventory Tool Operator, and Report Viewer.

vi Has either (a) a completed favorable background investigation (Tier 2 or higher) and is granted access to the OPM PIPS to validate whether the investigation has been scheduled and the status of Applicant background investigations, or (b) the ability to validate whether the investigation has been scheduled and the status of Applicant background investigations with an authorized VA user of PIPS.

vii Reviews and validates the Applicant's identity proofing documents by acceptable identity documents (see List 1), OMB guidelines, and VA Directive and Handbook 6510.

viii Reports to Agency Security Officer, VA Police, Federal Protective Service, Office of Inspector General (OIG), or other local Federal law enforcement officials when there is a reasonable suspicion that an Applicant presents fraudulent identity documentation as proof of identity.

ix Validates that the Applicant has met the PIV issuance criteria as shown in the Enrollment screen of the USAccess system.

x Collects the Applicant's biometrics and photograph.

xi Collects and destroys old cards when issuing a new card to a cardholder in compliance with VA enterprise-wide PIV credential accountability processes defined by OSP.

(e) Agency Role Administrator:

i Is a U.S. Citizen and a Federal Government employee.

ii Must have completed Agency Role Administrator training.

iii Is the OSP/PVCM/HSPD-12 Credential Management Director.

iv Is the authorized official. Assigns all USAccess roles (i.e., Agency Role Administrator, PIV Sponsor, PIV Adjudicator, Agency Security Officer, PIV Registrar, PIV Activator, etc.).

v Has a working knowledge of VA's structure, including populations and missions of VA's sites.

(f) PIV Activator:

i The PIV Activator role is designated by the PCIF Manager, and the Agency Role Administrator assigns the role in the USAccess system.

ii Is a Federal Government employee, contractor, or affiliate.

iii Has a completed favorable background investigation (Tier 2 or higher).

iv Must have completed USAccess Activator training.

v Performs a visual verification of the Applicant's face against the photograph printed on the credential and the photographic image stored in the credential and verifies the Applicant's identity by ensuring a one-to-one (1:1) fingerprint biometric match of the Applicant's fingerprints with the fingerprint images stored in the PIV card or chain of trust record.

vi Informs the Applicant of their responsibilities as a cardholder before issuing the credential.

vii After the Applicant establishes a Personal Identification Number (PIN), observes the Applicant sign for taking possession of the PIV card, officially releases the credential to the Applicant, and provides the Applicant with the approved electromagnetically opaque sleeve and lanyard.

(g) PIV Print Operator:

i The PIV Print Operator role is designated by the PCIF Manager, and the Agency Role Administrator assigns the role in the USAccess system.

ii Is a Federal Government employee, contractor, or affiliate.

iii Has a completed favorable background investigation (Tier 2 or higher).

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

(h) USAccess Report Viewer:

i The Report Viewer Operator role is assigned by the Agency Role Administrator.

ii Is a Federal Government employee, contractor, or affiliate.

iii The Reports Portal is available to the Report Viewer in the roles of PIV Sponsor, PIV Adjudicator, Agency Role Administrator, and Agency Security Officer.

iv The types of information that can be retrieved for the reports and the selection of reports provided by the USAccess system are based on the user’s access authorization level (role). The USAccess role holders can see only the reports within their role's scope.

v The Report Viewer Role has access to all USAccess reports.

(i) Applicant:

i An individual applying for a PIV card or derived PIV card. The applicant may be a current or prospective Federal hire, a Federal employee, a contractor, or a new or current VA employee requiring access to VA facilities or IT resources.

ii Provides all required demographic data, biometrics, and identity documents, in addition to being photographed during enrollment.

iii Completes, signs, and releases forms required for employment and/or background investigation (Optional Form 306, Standard Form 85, Standard Form 85P, Standard Form 86) and any future updated required forms.

iv Establishes the PIN that will be associated with the credential.

v Signs for acceptance of the credential and acknowledges cardholder responsibilities for handling, protecting, and using the credential.

vi Is referred to as the “cardholder” upon acceptance of the credential.

(j) Cardholder:

i Begins as a VA employee, contractor, or affiliate with a PIV card, PIV-I, or PIV-I Flash card.

ii Protects the credential’s physical integrity and operability of the contactless and contact devices on the credential.

iii Always maintain possession of the credential on or about their person while on official duty. The credential must not be left unattended, as doing so risks unauthorized access, tampering, exploitation, or loss, and it must be properly secured during off-duty hours.

iv Ensures the credential is stored in a FIPS-approved electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV card when not in a Card reader for logical access or when presented to a Card reader for physical access. The PCIF may provide credential storage sleeve.

v Always displays the credential while at a VA facility inside the electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV card and shall be worn visibly above the waist on the outermost garment with the photo side visible. The only exception is that displaying the credential may cause a safety risk to a cardholder patient, or others. The cardholder shall follow appropriate occupational safety requirements when conducting specific

medical procedures, patient interactions, or working around machinery with moving parts.

vi Visits the PCIF to unlock the PIV card. USAccess-issued Credentials will be locked after the Applicant has six (6) consecutive invalid PIN entry attempts.

vii Ensures that pins, buttons, credentials, decals, or similar items are not added to the PIV card.

viii Schedules credential renewal and Fingerprint (FP) Special Agreement Check (SAC) appointments if needed. It is recommended that these appointments be scheduled at least six (6) weeks before credential expiration.

ix Renews the PIV card before expiration.

x Notifies the PCIF when:

(A) The PIV card is lost or stolen.

(B) The PIV card does not operate properly, or personal information that appears on the PIV card changes (e.g., changes in affiliation or a name change).

xi Notifies the Supervisor of local PCIF and files a police report with the VA Police, Information Security System Officer (SSO), and local PCIF personnel within 24 hours or by the next business day when their PIV card, PIV-I card, or PIV-I Flash card is lost or stolen.

xii Handles PIV cards found unattended as sensitive Personally Identifiable Information and returns them to local PCIF personnel.

xiii Ensures that PIV cards have been returned to the appropriate VA authorities, such as the PIV Sponsor of record, Supervisors, Program Offices' authorized officials, and PCIFs for termination and de-activation when the VA PIV cardholder no longer requires access to VA information systems, controlled facilities, and secured areas.

3. CREDENTIAL TYPES, ELIGIBILITY, AND AFFILIATIONS.

a. General Guidance:

(1) PIV, PIV-I, and PIV-I Flash cards under the USAccess system issued in accordance with HSPD-12 and the current version of FIPS 201 are the sole forms of Federal credentials used by VA for identity verification of employees, contractors, and affiliates.

(2) Under the USAccess system, the official names of the identity credentials issued by VA are PIV, PIV-I, or PIV-I Flash cards. “PIV card” or “credential” may refer to all three credential types.

(3) PIV cards 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, this handbook and alignment with the December 15, 2020, OPM Memorandum, “Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirements for Suspension or Revocation of Eligibility for PIV cards (Credentialing Procedures).”

(4) Non-expired PIV cards 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, OIG Inspectors, and health care professionals, establish the authority and rights of the position of the individual carrying the credential but not the individual's identity. These credentials must be combined with the PIV card to verify the cardholder’s identity.

(6) Employment transfers (without an interruption in service with VA) between VA facilities should NOT result in the PIV card being returned to the PCIF.

(7) Appendix D “USAccess Applicant Eligibility and Access Type” describes the criteria for Applicants who will receive a USAccess PIV, PIV-I, or PIV-I Flash card, 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 levels are also dependent on the Applicant’s access requirements.

(8) Appendix E “Employment Eligibility Verification” describes the criteria for identity proofing for Applicants who will receive a PIV, PIV-I, and PIV-I Flashcard under the USAccess system.

(9) Appendix F “Credential Topologies” provides a list of fields included on PIV cards, PIV-I cards, and PIV-I Flash cards, and visual examples of each card.

(10) Appendix J “Credentialing Eligibility of Non-United States Nationals” describes the requirements to apply the OPM credentialing standards procedures to non-U.S. nationals who work as employees or contractors for Federal Departments or Agencies or others who require long-term logical or physical access to Federal Government facilities, whether overseas or in the United States.

b. Credential Type.

(1) PIV cards:

(a) Allow access to VA facilities and information systems.

(b) May be issued to employees, contractors, and affiliates, including non-U.S. nationals, who have a verified need to access VA facilities and information systems for a period of more than six (6) months.

(c) They are issued following a favorable interim PIV eligibility determination that is dependent, at minimum, upon the completion and favorable adjudication of a FP SAC, and the individual has a Tier 1 or higher background investigation scheduled, as indicated in OPM PIPS.

(d) Are issued following a review of two (2) acceptable identity documents (see List 1). One (1) identity document must be a state or Federal Government-issued photo identification (ID).

(e) Require favorable adjudication of a Tier 1 or higher background investigation for a final PIV eligibility determination and continued possession and use.

(f) Are valid for a period from the PIV card issuance date not to exceed five (5) years for employees issued under the USAccess system. PIV card expiration dates may be set for less than the maximum expiration date, when appropriate, to coincide with the contract's expiration or the length of the employee or affiliate’s appointment. USAccess PIV card certificates are valid for three (3) years and must be updated at a PCIF before their expiration to avoid card termination.

(2) PIV-I Flash Cards:

(a) Can only be issued by USAccess.

(b) Are visually different from PIV cards and PIV-I (See Appendix F).

(c) Allow access to standard VA physical facilities and do not allow access to VA information systems or restricted areas.

(d) May be issued to contractors and affiliates, including non-U.S. nationals, who have a verified need to access common VA physical locations for six (6) months or less.

(e) Are issued following, at a minimum, the completion and favorable adjudication of an FP SAC. The use of pseudo-social security numbers for Applicants without a social security number is not permitted.

(f) Are valid for not exceeding six (6) months from the issuance date.

(g) Cannot be used for logical access.

(3) PIV-I Cards:

(a) Can only be issued by USAccess.

(b) Are visually different from PIV cards and PIV-I Flashcards (See Appendix F).

(c) Allow access to VA facilities and information systems.

(d) May be issued to contractors and affiliates, including non-U.S. nationals, who have a verified need to access VA facilities and information systems for a limited period of no more than 180 days or less.

(e) Are issued following a favorable interim PIV eligibility determination that is dependent, at minimum, upon the completion and favorable adjudication of a FP SAC, and the individual has a Tier 1 or higher background investigation scheduled, as indicated in OPM PIPS.

(f) Are valid for a period from the credential issuance date, not to exceed 180 days.

(4) Non-FIPS 201-3 Compliant Credentials:

(a) Other credentials not mentioned in this document may not be used for FIPS 201-3 identity verification.

(b) Facilities and organizations may issue other types of credentials (i.e., hangtags, visitor passes) for use at their

facility or within their organization. These credentials 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 credentials may include position titles, names and photos in any size or color variation deemed appropriate by the facility or organization. These credentials may not be issued in place of and may only be used in concert with (to supplement) a PIV card, PIV-I card, or PIV-I Flash card.

(c) Other credentials must be printed in a manner that does not resemble a PIV card.

(5) For additional information on credential requirements for affiliates, including some Health Professional Trainees (HPTs), refer to Appendix D.

c. Applicant Type.

(1) VA Employee.

(a) 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.

(2) Contractor.

(a) An individual, business, or organization that contracts with the VA to provide goods or services, furnishing supplies and/or services to VA who will have access to VA information systems and/or physical access to VA facilities, and is not an employee.

(3) Affiliate.

(a) 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.

(b) Examples include but are not limited to: Veteran Service Organization (VSO) representatives, Joint Commission Reviewers, volunteers, HPTs who are not appointed, childcare staff, credit union staff, Union Officials, and union support staff. (Note: There are a number of training programs (e.g., nursing employee-based Registered Nurse transition to practice

[RNTTP] program) in VHA that are not sponsored by Office of Academic Affiliations (OAA)).

d. Exemptions.

(1) A Personal Identity Verification Interoperable (PIV-I) card will be issued to all individuals who work at or for VA, whether paid or unpaid for 180 days or less. All PIV-I cards will be terminated in accordance with the specific length of an individual's appointment. No PIV-I will be active for greater than 180 days.

(2) All VA personnel are required to have a PIV card. Individuals exempt from undergoing a background investigation (Tier 1 or higher) in accordance with VA Directive 0710, *Personnel Security and Suitability Program*, shall be issued a PIV-I card.

(3) Intermittent, seasonal, per diem, or temporary positions designated as national security in scope are not exempt from investigation regardless of the length of appointment.

(4) Individuals obtaining a PIV card replacement, reissuance, or renewal are exempt from undergoing a FP SAC check.

(5) For more specific information regarding the exemption process, see VA Directive 0710, *Personnel Security and Suitability Program*.

4. IDENTITY VERIFICATION AND CREDENTIAL ISSUANCE.

a. Manage Credential Request in USAccess.

(1) The PIV Sponsor initiates a credential request in the Assured Identity Sponsor Portal. The credential request contains the following data:

(a) Applicant Biographical Data.

(b) Sponsor Information (e.g., Agency, Employment Type, User Principal Name).

(c) Card Information (e.g., type of credential).

(d) Credential Information (e.g., required certificates, card expiration date); and

(e) Print Location.

(2) The PIV Sponsor and/or Applicant will receive an email notification confirming Sponsorship.

(3) Following the implementation of the VA Onboarding Solution, the collection and submission of the credential request will be automated.

b. Registration in USAccess (See Appendix H for more details).

(1) The PIV Registrar verifies the Applicant's identity through review and validation of identity source documents (see List 1). These identity source documents will be scanned during enrollment. All identity source documents must be current and unexpired.

(2) The PIV Registrar will also capture the Applicant’s biometrics, photo, and fingerprints.

(3) Once the fingerprints are verified, the PIV Registrar will save the profile, which is then sent to USAccess.

c. Adjudication in USAccess.

(1) The PIV Adjudicator verifies the Applicant’s background investigation status using OPM PIPS or VA-CABS, or by communicating with VA personnel who have access to OPM PIPS (or VA-CABS) to obtain background investigation status.

(a) For a PIV and PIV-I card, the Applicant requires a scheduled or reciprocally acceptable Tier 1 or higher background investigation, as indicated in Central Verification System PIPS, and a favorably adjudicated FP SAC. For PIV-I Flash card, the Applicant requires a favorably adjudicated FP SAC. The FP SAC must be dated within 120 days.

(b) If no investigation is on file or scheduled at OPM, the appropriate personnel (e.g., a Human Resource or Personnel Security and Suitability representative) initiates an invitation to the OPM Electronic Questionnaire for Investigations Processing eApp for the Applicant to complete the appropriate background investigation forms. The investigation has been accepted by OPM prior to PIV card issuance.

d. PIV card Issuance in USAccess.

(1) The PIV Print Operator prints the credential and verifies that no errors were made in printing. If errors were made, the credential is

reprinted. Rejected credentials are documented as rejected and destroyed.

(2) The PIV Activator activates/encodes the card, which includes the Applicant's photograph, fingerprint templates, four required digital certificates (i.e., Digital Signature, Encryption, PIV Authentication and Card Authentication certificates) and any historical encryption certificates from previously issued credentials for PIV and PIV-I Cards and two required digital certificates (i.e., Digital Signature and Card Authentication certificates) for PIV-I Flash cards.

(3) The PIV Activator performs a visual verification of the Applicant's face against the photograph printed on the credential.

(4) The PIV Activator verifies the Applicant's identity by performing a one-to-one (1:1) biometric match comparing the biometrics stored on the credential against those of the Applicant. If the match is unsuccessful, or if no biometric data are available, the cardholder shall provide two identity source documents, and an attending operator shall inspect these and compare the cardholder with the facial image printed on the PIV card.

(5) The Applicant sets their PIN (between six and eight digits) to securely lock the credential.

(6) The Applicant reviews and acknowledges the USAccess Privacy Act Statement.

(7) The PIV Activator officially releases the credential to the Applicant and provides them with a lanyard and FIPS-approved electromagnetically opaque sleeve. Lanyards that meet local requirements (e.g., breakaway, organizationally unique) may be substituted at the discretion of the local PCIF Manager.

e. Security Requirements for PIV card Issuance.

(1) In December 2020, OPM issued updated credentialing standards and procedures that established a two-step process for the issuance of HSPD-12 PIV cards. Step 1 consists of an interim PIV eligibility determination that enables VA to bring a new appointee or contract employee on board pending completion and favorable adjudication of the required background investigation. Step 2 consists of a determination of final PIV eligibility and is dependent of the completion and favorable adjudication of the prerequisite background investigation.

(2) FIPS 201-3 states that a credential can only be issued after a Tier 1 or higher-level background investigation is initiated (scheduled) and the FBI criminal record check is completed. FIPS 201-3 states that "initiated" means the background investigation submission has been accepted (scheduled) by the Investigative Service Provider. For VA, this is the Defense Counterintelligence and Security Agency (DCSA). Investigations are considered scheduled when the Electronic Application (eApp) or National Background Investigation Service (NBIS) case has been released to DCSA for processing and passes DCSA's initial quality review step. This is verifiable through DCSA's Central Verification System (CVS)/PIPS. The requirement to have a "completed FBI criminal record check" is satisfied once the FP SAC is favorably adjudicated (also verifiable in CVS/PIPS and VA-CABS).

(3) PIV Adjudicators in the USAccess system must, prior to making an interim PIV eligibility determination for issuing a PIV card, verify that FP SACs are favorably adjudicated, and investigations are "Scheduled" in DCSA's CVS/PIPS. For employees with completed investigations, the closed and adjudicated investigation dates are enough to issue a PIV card. Other than the FP SAC conducted for initial appointment to, or in support of, VA, if a previous favorably adjudicated background investigation exists that meets the requirements of the encumbered position, there are no additional FBI criminal record checks or FP SAC requirements. Additional FP SACs are not required in cases of VA-to-VA internal Department of Veterans Affairs transfer/reassignments or PIV renewal/reissuance because the FBI criminal record check is part of the previous Favorably Adjudicated background investigation. A new FP SAC should only be conducted when a higher-level investigation is required due to a change in position risk or sensitivity.

(4) As a reminder, to ensure timely PIV issuance in support of an interim PIV eligibility determination, it is essential that the prospective new employee (or contractor and affiliates) complete their NBIS/eApp submission to initiate their background investigation prior to entry on duty (EOD).

5. CREDENTIAL MANAGEMENT LIFECYCLE.

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

b. PIV card Use:

(1) PIV cards, PIV-I cards, and PIV-I Flash cards 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; reporting 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 a 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 penalties and/or administrative sanctions, including disciplinary or adverse personnel action and/or restricted or denied access to VA resources.

(3) PIV cards should be collected on the last day of association with VA by the appropriate VA authorities such as to the PIV Sponsor of record, Supervisors, Program Offices' authorized officials, and or PCIFs for termination and de-activation when the VA PIV cardholder no longer requires access to VA information systems, controlled facilities, and secured areas. If physical collection is not possible, the PIV card should be returned no later than five (5) days from the last day of association with VA to appropriate VA authorities such as to the PIV Sponsor of record, Supervisors, Program Offices' authorized officials, and/or PCIFs for termination and de-activation. PIV cards 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 always be displayed while at a VA facility inside the provided electromagnetically opaque sleeve and shall be worn visibly, 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 individuals. 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 any other device (e.g., tenure pin, service pin, lapel pin, etc.).

c. Card Inventory.

(1) The PCIF Manager or other appropriate authority (such as the Agency Security Officer or Local Site Manager (LSM)), 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), and card reader(s) always.

(3) USAccess card stock shall be ordered, distributed, and managed/monitored using the USAccess Card Stock Inventory Management Tool (CSIMT), which is accessible only by Agency and Local Site Managers through the Site Manager Tool.

(4) Credentials that are lost, stolen, or unaccounted for while in storage shall be reported immediately to the PCIF Manager. The PCIF Manager (or Agency Security Officer or LSM) shall report incidents of lost or stolen credentials to the Information Security Officer (ISO) within 24 hours or by the next business day in accordance with VA Directive 6500, *VA Cybersecurity Program* and VA Handbook 6500.

(5) The PCIF Manager (or Agency Security Officer or LSM) 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-for credentials.

d. Facility, Organization and Office Transfers.

(1) VA Credentials shall not be confiscated when a VA cardholder transfers between VA facilities, organizations, 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 cards 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 System (PACS) on an as-needed basis in compliance with access policies established by that facility.

(3) VA PIV cards 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 acceptable identity documents (see List 1).

(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. PIN Reset.

(1) USAccess-issued Credentials that are locked due to a maximum of six (6) consecutive invalid PIN entry attempts must have the PIN reset. Cardholder should visit the PCIF to unlock the card.

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

(3) Prior to providing the reset card to the cardholder, the operator performing the PIN reset shall perform a one-to-one (1:1) biometric match to ensure that the cardholder’s biometric matches either the stored biometric on the PIV card or biometric data stored in the chain of trust.

(4) In cases where a biometric match is not possible, the cardholder shall provide the PIV card to be reset and another primary identity source document. The operator shall inspect these and compare the

cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the card.

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

h. Credential Renewal.

(1) It is the responsibility of the cardholder to ensure they renew the PIV card prior to expiration. USAccess will send notification emails 90, 60, 30, 14 and 7 days prior to the card's expiration to the cardholder and the PIV Sponsor in the cardholder's' record.

(2) An FP SAC is not required for PIV reissuance and renewal.

(3) The PIV Sponsor verifies that the Applicant remains in good standing and requests the credential renewal. Renewals can be requested by bulk renewal in USAccess or in the individual's USAccess Sponsorship record.

(4) In the USAccess system, a renewal will initiate a card print request. If the user's 12-year enrollment has expired, a reissue request made by the PIV Sponsor will require the user to re-enroll.

(5) The PIV Activator under USAccess verifies the cardholder's identity against the biometric information stored on the expiring credential. If the match is unsuccessful, or if no biometric data are available, the cardholder shall provide two (2) valid identity source documents, and an attending operator shall inspect these and compare the cardholder with the facial image printed on the PIV card.

(6) The PIV Activator under USAccess shall inspect the two (2) valid identity source documents (see List 1) and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the new PIV card.

(7) The expiring PIV card is collected by the PIV Activator under USAccess 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. Certificate Renewal/Update under USAccess.

(1) Under USAccess, certificates on PIV cards are valid for three (3) years. The cardholder is responsible for renewing/updating the digital certificates and will be automatically notified of their certificate

expiration date 90, 60, 30, 14, and 7 days prior to the expiration with instructions to schedule an appointment to update their certificates.

(2) It is the responsibility of the cardholder to visit a PCIF to receive a certificate update prior to the certificate expiration date. If the certificates expire, the card will automatically be terminated, and a new card issuance will have to be requested by the PIV Sponsor.

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

j. Credential Reissuance.

(1) Cardholders are expected to apply for credential reissuance when the PIV card 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 (see Section k) below for more details regarding lost or stolen credentials.

(2) It is the responsibility of the cardholder to monitor the credential expiration date and coordinate with their PIV Sponsor to obtain a new credential.

(3) The entire registration and issuance process is conducted, including biometric fingerprint and facial image capture.

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

k. Lost and Stolen Credentials.

(1) Lost or stolen credentials must be reported to the supervisor, ISSO, local police, and local PCIF personnel within 24 hours or the next business day after discovery of the loss/theft. The local PCIF shall report the loss/theft and account for lost and stolen credentials in the monthly reports to the HSPD-12 PIV Credential Management PMO.

(2) Upon notification of a lost or stolen credential, local PCIF personnel shall, terminate the credential within 18 hours and notify the HSPD-12 PIV Credential Management PMO.

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

(4) Credential Recovery

(5) Credentials delivered to a PCIF as having been left unattended should be handled as confidential media and treated as recovered credentials.

(6) The PCIF will attempt to notify the cardholder to pick up their credential via email using a lookup of their Active Directory address.

(7) Recovered credentials that cannot be returned to the cardholder within 18 hours or by the next business day shall be treated as a lost credential and shall be terminated.

(8) It is the responsibility of each VA facility to establish additional procedures for handling recovered credentials and repeatedly lost credentials. Facility Managers may not charge cardholders a fee for lost or stolen credential reissuance. Facilities may adopt any of the below methods for handling recovered or lost credentials or develop a policy of their own:

(a) Require the cardholder's Manager to approve the issuance of a visitor pass.

(b) In the event of a forgotten Credential, require the cardholder to retrieve the credential prior to allowing entrance to the facility.

(c) Allow issuance of a visitor pass to the cardholder with verification of identity through acceptable identity documents (see List 1), such as a driver's license.

l. PIV Credential Termination.

(1) Credential termination deactivates the electronic aspects of the credential, making the credential non-functional in PACS and Logical Access Control System (LACS) and schedules the credential for destruction.

(2) Credentials must be terminated within 18 hours after receipt of the credential by the PCIF or notification of a lost or stolen credential.

(3) Credentials 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 because of renewal or reissuance.

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

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

(e) The cardholder has violated the Public Key Infrastructure (PKI) subscriber agreement or cardholder agreement.

(f) Access to federally controlled buildings or information systems is no longer required (this includes completing or terminating a contract and replacing or separating contractor personnel).

(4) Credential termination process:

(a) The credential is deactivated.

(b) The certificates on the credential are revoked.

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

(d) The credential is collected and scheduled for destruction by the local PCIF.

m. PIV 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 two mm wide cuts), or incineration. See Appendix H for additional information.

(4) Notifications shall be made to VA HSPD-12 PIV Credential Management PMO and accounted for in monthly reports to the PMO.

6. CREDENTIALING PROCESS FOR NON-U.S. NATIONALS.

a. Due to limitations in an Investigative Service Provider’s (such as the DCSA) ability to collect background investigation information in locations outside the United States, special investigative considerations apply when

a PIV card is needed for a non-U.S. national in either U.S.-based locations or foreign locations. Refer to Appendix J, “Credentialing Eligibility of Non-United States Nationals,” for additional instructions.

7. PIV ELIGIBILITY – STANDARDS AND PROCEDURES FOR RECIPROCITY, SUSPENSION, UNFAVORABLE DETERMINATIONS, AND APPEALS PROCESSES.

a. Individuals found ineligible for a PIV under the OPM credentialing standards may not access VA or other federally controlled facilities and information systems for which a PIV is required and may not be issued an alternate PIV for these purposes. In cases in which it is determined that PIV card access is no longer needed for an individual who has been issued a PIV card, access shall be withdrawn for the PIV card and any pertinent systems. The database must also be updated to revoke PIV card tokens and terminate access. Any VA facility or system access previously granted must be immediately withdrawn from the PIV card. Additionally, any databases showing current PIV card eligibility must be immediately updated to include CVS and any of its follow-on systems, such as the new NBIS, the DCSA plans to implement as a replacement for CVS.

b. OSP shall ensure that effective procedures are developed between Chief, OSP, VA law enforcement and security staffs, personnel security offices, human resource offices, contracting offices, OIT cybersecurity, etc., to enable them to work together to address issues or changes that may affect PIV eligibility. For instance, communication between internal VA offices is essential to ensure an individual does not inappropriately retain physical or logical access when they have been subject to unfavorable administrative action (such as when a contractor is removed from a contract) or adverse action (such as when an employee is suspended or removed for conduct reasons). Similarly, communication with other Federal Departments and Agencies is also essential and personnel security staff will consult CVS or any successor system to identify any other Departments or agencies that may have a current affiliation with the individual, with the individual having been granted access to other Department and Agency systems and facilities.

c. OSP will be responsible for assessing any derogatory information affecting PIV card eligibility that may be reportable under the minimum standards and guidelines for insider threat reporting under EO 13587.

d. If the PIV card cannot be collected and destroyed, then the certification authority shall be notified and informed by OSP in coordination with OIT and the certificates corresponding to the PIV Authentication key and asymmetric Credential Authentication key on the PIV card shall be

revoked. If present, the certificates corresponding to the digital signature key and the key management key shall also be revoked.

e. VA standards and procedures for reciprocity of PIV eligibility, suspension of PIV eligibility, unfavorable determinations, and denial of an individual's PIV eligibility, and associated appeals processes shall comply with the OPM credentialing standards procedures issued in December 2020.

f. The appeals process is:

(1) The applicant or appointee is sent a written letter by Servicing Human Resources Office (SHRO)/PIV Sponsor and is afforded 30 calendar days from the date of the Proposed Action Letter (PAL) to refute, explain, clarify, or mitigate the unfavorable information.

(2) The applicant or appointee will be provided with the PAL written notice of the reasons for denial of eligibility for a PIV card. This PAL notice will contain information on submitting a written and/or oral appeal.

(3) The applicant may submit a written appeal containing an explanation of the basis for the appeal within 30 days of receiving the decision.

(4) The written appeal must be submitted to the appropriate SHRO or other designated official that was included in the PAL notice containing the information on submitting a written and/or oral appeal.

(5) The applicant or appointee may also arrange for an oral response by following the steps outlined in the PAL notice.

(6) The applicant or appointee will receive a written decision on the appeal within 30 days of their written and/or oral response.

g. Below are reasons for PIV card refusals identified in the appeals process.

(1) Identity Proofing.

(a) Applicants will not be issued a PIV card until appropriate, valid, and authentic identity source documentation is provided. Applicants are granted two (2) chances to provide acceptable identity documentation: the initial identity documentation presentation and the subsequent presentation to remedy the unacceptable documentation.

(b) The Applicant or appointee is sent a written letter by SHRO/PIV Sponsor and is afforded 30 calendar days from the date of the PAL to refute, explain, clarify, or mitigate the unfavorable information. The Applicant shall be present and shall furnish acceptable identity source documentation; and

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

(c) Final determination to allow additional attempts to provide acceptable identity documentation is at the sole discretion of the PCIF Manager and shall be made within 2 business days of receiving the appeal request, in a written form.

(d) VA reserves the right and authority to direct that any denial decision be held in abeyance pending additional discretionary guidance from the OIMO for HSPD-12.

(2) Refusal to Sign (acknowledge) the VA Card Acceptance Agreement.

(a) Applicants will not be issued a PIV card until they have signed (acknowledged) the VA or USAccess Card Acceptance Agreement during the issuance process.

(b) Applicants who have been denied a PIV card resulting from refusal to sign (acknowledge) the VA or USAccess Card Acceptance Agreement must meet with their PIV Sponsor within 2 business days of the denial if they wish to begin the appeals process. Failure to meet this requirement constitutes a non-contest, and no PIV card will be issued. Under this policy, this requirement is not appealable.

(3) Applicant Non-Appealable Conditions Under this Policy:

(a) The Department, Administration, or OPM has determined that the Applicant is not suitable for Federal employment or employment at VA under the provisions of 5 C.F.R. Part 731.

(b) The Department or the 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.

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). (SOURCE: FIPS 201-3)

2. **Affiliate:** A non-Federal employee or contract individual who requires logical access to VA information systems and/or physical access to VA facilities to perform their duties. Examples of affiliates include (but are not limited to) students, researchers, residents, Veterans Service Organization Officers, volunteers, accredited attorneys, union officials, and interns. (SOURCE: VA Directive 0710)

3. **Applicant:** An individual applying for a VA PIV, PIV-I, or PIV-I Flash credential. 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. (SOURCE: FIPS 201-3)

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 or fit for the job and/or eligible for a for a non-sensitive low risk, public trust, or sensitive position, 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. (SOURCE: FIPS 201-3)

6. **Biometric Authentication (BIO, BIO-A):** A form of authentication in which authenticity is established by biometric verification of a new biometric sample from a cardholder to a biometric data record read from the cardholder's activated PIV card. In BIO, the biometric sample may be captured from the cardholder in isolation, while in BIO-A, an attendant must oversee the process of biometric capture.

7. **Biometric Capture Device:** Device that collects a signal from a biometric characteristic and converts it to a captured biometric sample. (SOURCE: ISO 2382-37)

8. **Biometric Characteristic:** Biological attribute of an individual from which distinctive and repeatable values can be extracted for the purpose of automated recognition. Fingerprint ridge structure and face topography are examples of biometric characteristics. (SOURCE: ISO 2382-37, adapted)

9. **Biometric Data:** Biometric sample or aggregation of biometric samples at any stage of processing. (SOURCE: ISO 2382-37, adapted)

10. **Biometric Data Record:** Electronic data record containing biometric data. This information can be in terms of raw or compressed pixels or in terms of some biometric characteristic (e.g., patterns). (SOURCE: ISO 2382-37, adapted)

11. **Biometric On-Card Comparison (OCC):** A one-to-one comparison of fingerprint biometric data records transmitted to the PIV card with a biometric reference previously stored on the PIV card. In this Standard, OCC is used as a means of performing card activation and as part of Biometric On-Card Comparison Authentication (OCC-AUTH).

12. **Biometric On-Card Comparison Authentication (OCC-AUTH):** An authentication mechanism where biometric on-card comparison (OCC) is used instead of a PIN to activate a PIV card for authentication.

13. **Biometric Verification:** Automated process of confirming a biometric claim through biometric comparison. (SOURCE: ISO 2382-37, adapted)

14. **Biometric Verification Decision:** A determination of whether biometric probe(s) and biometric reference(s) have the same biometric source based on comparison score(s) during a biometric verification transaction. (SOURCE: ISO 2382-37, adapted)

15. **Certification:** The formal process of assessing the attributes (e.g., knowledge, availability, accountability, trustworthiness, 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.

16. **CHUID:** Card Holder Unique Identifier (SOURCE: NIST SP 800-73-5)

17. **Contractor:** An individual, business or organization that contracts with VA to provide goods or services, furnishing supplies and/or services to VA who will have access to VA information systems and/or physical access to VA facilities, and is not an employee or contractor

18. **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, PIV-I card, and/or PIV-I Flash card.

19. **Derived PIV card:** The Derived PIV card is a Derived PIV Authentication certificate, which is an X. 509 public-key certificate issued in accordance with the requirements of this document and the X. 509 Certificate Policy for the

U.S. Federal PKI Common Policy Framework; (SOURCE: NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*)

20. **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.

21. **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*, *National Infrastructure Protection Plan*, *National Incident Management System* and/or the *National Continuity Policy Implementation Plan* (NCPIP). The NCPIP includes Continuity of Operations and Continuity of Government members. P.L. 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 VA Emergency Relocation Group to include Crisis Response Team; Integrated Operations Center Team; those with Devolution and Reconstitution roles (Devolution Emergency Response Group and Reconstitution Emergency Relocation Group) will be authorized to be designated as a FERO.

22. **Federal Information Processing Standards (FIPS):** A standard for adoption and use by Federal Departments and Agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce under 40 U.S.C. § 11331. FIPS covers some topic in IT to achieve a common level of quality or some level of interoperability. (SOURCE: FIPS 201-3)

23. **FIPS 201 Approved Products List (APL):** A list of products and services that are in compliance with the current version of the FIPS 201 and its supporting publications. The list may be found at FIPS 201 Approved Product List. Only those products and services (service providers) listed on the FIPS 201 APL are recognized as being in compliance with HSPD-12. (SOURCE: FIPS 201 APL)

24. **Non-U.S. National:** All Applicant types (VA employee, contractor, or affiliate) who are not citizens or nationals of the United States (US) .

25. **Identification:** The process of discovering the identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. (SOURCE: FIPS 201-3)

26. **Identity:** The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (SOURCE: FIPS 201-3)

27. **Identity Proofing:** The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity. (SOURCE: FIPS 201-3)

28. **Interoperability:** For the purposes of the HSPD-12 Presidential Directive, interoperability allows any Federal Government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV card. (SOURCE: HSPD-12 Presidential Directive)

29. **Logical Access Control System (LACS):** Protection mechanisms that limit users' access to information and restrict access in the system to only what is appropriate for them. These systems may be built into an operating system or application or maybe an added system. (SOURCE: Logical Access Control)

30. **Personal Identity Verification (PIV) Card Issuer (PCI):** An authorized HSPD-12 compliant PIV card 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. (SOURCE: NIST SP 800-79-2)

31. **PIV Credential Issuing Facility (PCIF):** An installation 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. (SOURCE: NIST SP 800-79-2)

32. **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.

33. **Physical Access Control System (PACS):** An electronic system that controls the ability of people to enter a protected area, by means of authentication and authorization at access control points. (SOURCE: NIST SP 800-116)

34. **PIV card:** A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains a PIV card application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable). USAccess PIV cards are normally issued with a five (5) year expiration, requiring a digital certificate update three (3) years after issuance. (SOURCE: FIPS 201-3).

35. **PIV credential:** The term PIV credential encompasses all PIV cards issued by USAccess to VA employees, contractors, and affiliates. VA maintains three types of PIV credentials: a PIV card that requires a favorably adjudicated FP SAC, a minimum of a Tier 1 background investigation, is valid for physical access to VA facilities, and access to information security systems; a PIV-I 4-Certificates card that requires a favorably adjudicated FP SAC, a minimum of a Tier 1 background investigation, is valid for physical access to VA facilities, and access to information security systems for 180 or less; a PIV-I 2-Certificates card also called PIV-I Flashcard that requires a favorably adjudicated FP SAC and is only valid for physical access to VA facilities for no longer than 180 days; PIV credentials are issued to persons requiring routine access to VA facilities or information systems.

36. **PIV-Interoperable (PIV-I) Credential:** A PIV-I card meets the technical removing specifications to work with Federal PIV infrastructure elements such as card readers and is issued in a manner that allows Federal Government Relying Parties to trust the card. The PIV-I card is suitable for Identity Assurance Level 3 (IAL3) and Authenticator Assurance Level 3 (AAL3) as defined in NIST SP 800-63-4, as well as multi-factor authentication as defined in NIST SP 800-116. PIV-I credentials replaced VA Non-PIV cards. (SOURCE: HSPD-12 Presidential Directive)

37. **PIV-I Flashcard:** A VA ID credential containing a photograph issued to an individual for infrequent access to VA public areas only (such as cafeterias, lobbies, libraries, and credit unions) for a period not to exceed 180 days.

38. **Privacy Impact Assessment (PIA):** Is an assessment that is conducted every 3 years by OIT and sooner if there is a change to the system. It 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 card, how the information will be protected and the complete set of uses of the credential and related information at 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*. (SOURCE: VA Directive 6502)

39. **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 IT.

40. **Special Agreement Check (SAC):** Also known as Fingerprint Special Agreement Check (FP SAC), is a fingerprint-only automated records check conducted by the FBI in collaboration with OPM. PIV cards are issued following, at a minimum, the completion and favorable adjudication of a SAC and a Tier 1 or higher background investigation received as indicated by OPM PIPS.

41. **Tier 1 (T1) Background Investigation:** Low Risk/Non-Sensitive Investigations conducted to this standard are for positions designated at low risk, non-sensitive and for physical and/or logical access, pursuant to FIPS 201 and HSPD-12, using Standard Form-85.

42. **Tier 2 (T2) Background Investigation:** Investigations conducted to this standard are for non-sensitive positions designated as moderate risk public trust, using Standard Form-85P.

43. **Tier 3 (T3) Background Investigation:** Non-Critical-Sensitive Investigations conducted to this standard are for positions designated as potential for damaged to the national security; requiring eligibility for “L” access or access to Confidential or Secret information, using Standard Form-86.

44. **Tier 4 (T4) Background Investigation:** Investigations conducted to this standard are for non-national security sensitive positions designated as high-risk public trust, using Standard Form-85P.

45. **Tier 5 (T5) Background Investigation:** Investigations conducted to this standard are for position designation as Critical-Sensitive, Special-Sensitive, and/or requiring eligibility for “Q” access or access to Top Secret or Sensitive Compartmented Information (SCI), using Standard Form-86. This investigation is similar to the Single Scope Background Investigation (SSBI).

46. **USAccess:** A GSA shared service that provides Federal agencies, boards, and commissions with an end-to-end service to enroll Applicants and issue HSPD-12 compliant identity management credentials. USAccess streamlines sponsoring, enrolling, adjudicating, and credentialing processes while maintaining each credential throughout its lifecycle.

47. **Visitor:** Any individual requiring escorted access and is on VA property fewer than 15 days in a 365-day period. Visitor passes, as stated in paragraph 3.b. of VA Handbook 0735, are not governed by HSPD-12 policies. Issuance of visitor passes is the responsibility and at the discretion of each Facility Director.

48. **Volunteer:** The Volunteer Protection Act of 1997 (codified at 42 U.S.C. § 14505) defines Volunteer as an individual performing services for a nonprofit organization or a governmental entity who does not receive— (A)

compensation (other than reasonable reimbursement or allowance for expenses actually incurred); or (B) any other thing of value in lieu of compensation, in excess of $500 per year, and such term includes a volunteer serving as a director, officer, trustee, or direct service volunteer.

APPENDIX B: ROLE HOLDER DEFINITIONS.

Below are the definitions for each of the roles in USAccess. Role definitions are based on VA Directive and Handbook 0735 and USAccess role definitions.

1. **Agency Role Administrator:** The individual within USAccess who is responsible for managing the Agency's PIV Sponsor, PIV Adjudicator, PIV Registrar, Agency Security Officer, and PIV Activator roles within USAccess. The Agency Role Administrator is the OSP/PVCM/HSPD-12 Credential Management Director. It is the Agency Role Administrator's responsibility to verify that the separation of duties policy is followed and that all training certification requirements have been met. The Agency Role Administrator cannot hold any other role in the PIV process to adhere to the separation of duties requirement.

2. **Agency Site Manager:** The individual assigned this role in the USAccess Site Manager Tool who facilitates coordination and deployment for their Agency or Sub-Agency, as well as resolves any broader HSPD-12 challenges with the LSM under their scope and the Credential Management PMO.

3. **Local Site Manager:** The individual assigned this role in the USAccess Site Manager Tool who facilitates coordination and deployment within their Local Site(s), as well as resolves any broader HSPD-12 challenges with the Agency Site Manager. LSM also performs additional duties such as adjusting site/PCIF badging operational hours and closures, adding new workstations, and purchasing/obtaining new PIV card stock and printer consumables.

4. **Agency Security Officer:** The individual responsible for batch importing sponsorship records, reviewing identity documents flagged by the PIV Registrar as requiring more validation and investigating any potential identity impersonation events, suspending, and terminating credentials for security-related threats, collecting, and destroying credentials at termination of employment and acting as the interface for any inquiries about identity issues as related to law enforcement activities.

5. **PIV Sponsor:** The individual who establishes 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 checks. In USAccess, the PIV Sponsor is responsible for creating PIV records and is the only individual who can create, edit, and manage USAccess PIV records. A PIV Sponsor can edit biographic data and sponsorship information, select the address where an Applicant's credential will be delivered, reassign sponsorship, request credential issuance, prints, and certificate updates, and resend sponsorship complete and credential check-in emails.

6. **PIV Registrar:** The individual or entity who establishes and vouches for the identity of an Applicant to a PIV card Issuer. The PIV Registrar authenticates the Applicant's identity by checking identity source documents and identity proofing before the credential is issued. Under USAccess, PIV Registrars are required to take training on the USAccess program, managing and operating the credentialing unit, proper procedures for identity proofing and fingerprinting Applicants and application of security measures and protecting personal privacy information.

7. **PIV Activator:** The individual responsible for processing USAccess PIV card activations, verifying that an Applicant is the proper person the credential is issued to, and guiding Applicants through the activation process. PIV Activators may also create requests to unlock credentials and reset cards.

8. **PIV Print Operator:** The individual within USAccess who is responsible for printing USAccess PIV cards at a local printing site. The PIV Print Operator verifies that a PIV card is properly printed before being activated. The PIV Print Operator role can be held along with any other role.

9. **PIV Adjudicator:** The individual authorized to record or update the status of an Applicant's adjudication result in USAccess. A positive adjudication for an Applicant will result in initiating the PIV card issuance process.

10. **PIV Card Inventory Tool (CIT) Operator:** The individual who checks in USAccess PIV cards into the Credential Inventory Tool. Upon check-in, the CIT Operator will have the option to send the Applicant an email stating that the PIV card is ready for pick up. The CIT Operator will also destroy the credentials and mark the PIV card as destroyed in the USAccess system.

11. **USAccess Report Viewer:** The individual can access and filter all USAccess reports from the Assured Identity Reports Portal. Note: PIV Sponsors, Agency Security Officers, PIV Adjudicators, and Agency Site Managers have access to Role Specific reports granted automatically with their Role assignment.

APPENDIX C: ACRONYMS.

Acronym	Definition
APL	Approved Products List
CISO	Chief Information Security Officer
CMS	Card Management System
CSS	Chief of Support Services
DAO	Designated Authorizing Official
eApplication (eApp)	Electronic Questionnaires for Investigations Processing
ESD	Enterprise Service Desk
FERO	Federal Emergency Response Official
FIPS	Federal Information Processing Standards
FP SAC	Fingerprint Special Agreement Check
GSA	General Services Administration
HR	Human Resources
HSPD	Homeland Security Presidential Directive
ID	Identification. A form of identification, an ID card.
ISO	Information Security Officer
IT	Information Technology
LACS	Logical Access Control System
NCPIP	National Continuity Policy Implementation Plan
NIST	National Institute for Standards and Technology
OIT	Office of Information and Technology
OGC	Office of General Counsel
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 Credential Issuance
PCIF	PIV Credential Issuance Facility

Acronym	Definition
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PIPS	Personnel Investigations Processing System
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKI	Public Key Infrastructure
PMO	Program Management Office
PVTS	Privacy Violation Tracking System
SAC	Special Agreement Check
SES	Senior Executive Service
SORN	System of Records Notice
SP	Special Publication
U.S.	United States
U.S.C.	United States Code
VA	Department of Veterans Affairs
VSO	Veterans Service Organization

APPENDIX D: USACCESS APPLICANT ELIGIBILITY AND ACCESS TYPE.

1. The following criteria must be reviewed by the PIV Sponsor for all VA employees, contractors, and affiliates in order to determine the USAccess PIV card type to be issued to the Applicant based on physical and logical access requirements and the length of time access is needed. VA must use these OPM credentialing standards and procedures for making all decisions regarding the eligibility of individuals for a PIV card for physical or logical access to federally controlled facilities and/or information systems, including VA Federal employees and employees of Government contractors who are performing work for or on behalf of VA, members of the armed forces, non-appropriated fund employees, as well as specific categories of individuals that may be unique to VA, such as guest researchers, volunteers, intermittent employees, seasonal employees, or employees on temporary appointments likely to continue for at least 6 months. For this guidance, short-term employment is the employment of less than 6 continuous months.

2. VA will consider the benefits of PIV eligibility determinations for intermittent or temporary employees whose affiliation is repeatedly terminated and reinstated and for any employees who are expected to serve intermittently over multiple years, such as Health Professions Trainees (HPTs). Intermittent employees with affiliation that extends beyond 6 continuous months are not considered “short-term.” Similarly, seasonal employees, i.e., employees on permanent appointments who work a seasonal schedule of 6 months or more on a recurring basis are not considered “short-term.”

3. VA has specific categories of personnel such as HPTs, guest researchers, or volunteers who may be unique to VA. The OPM credentialing standards and procedures generally apply to such VA personnel unless they are short-term (i.e., less than 6 continuous months) employees, in which case VA has discretion to vet those personnel for PIV card based on risk and other factors, or to issue an alternative identity credential with appropriate restrictions and alternative security protections.

4. Note that an alternative identity credential (such as PIV-I) is an identity credential that does not meet the standards outlined in the OPM Credentialing Procedures and is visually and electronically distinguishable from PIV cards (that do meet these requirements). The employing agency (VA) assumes all risk in managing alternative credentials and alternative identity credentials are not reciprocally acceptable.

5. VA must apply the Adjudicative Guidelines provided in 2008 Final Credentialing Standards, or any successor document and the Performance Accountability Council (PAC) Memorandum to Heads of Executive Departments and Agencies, *Guidance on Executive Branch-Wide Requirements for Issuing PIV Credentials and Suspension Mechanism*, of March 2, 2016, in order to determine whether to find an individual eligible for

a Federal PIV card permitting physical and logical access to federally controlled facilities and federally controlled information systems. VA must determine whether:

a. There is proof that the person is who they say they are,

b. Terrorism or IT security concerns exist; and

c. There are any other issues that indicate issuance of a PIV card to an individual will pose an unacceptable risk to any of the following:

(1) The life, safety, property or health of employees, contractors, vendors, or visitors to a Federal facility.

(2) The Government's physical assets or information systems.

(3) Records, including privileged, proprietary, financial, or medical records; or

(4) The privacy of the individuals whose data the Government holds in its systems.

6. VA may not waive, modify, or replace the OPM credentialing guidelines.

7. VA uses the **Two-Step** process prescribed by OPM as the Federal Government's CEA.

a. Step 1 consists of an interim PIV eligibility determination which enables VA to bring a new appointee or contract employee on board pending completion of the required background investigation. VA must ensure all the following is complete before making a favorable interim PIV eligibility determination:

(1) Presentation by the appointee or employee of two identity source documents, at least one of which is a state or Federal Government-issued picture identification.

(2) Favorable review by VA of the intended PIV recipients completed investigative questionnaire.

(3) Initiation of the intended PIV recipient's required background investigation (Tier 1 or higher) request, meaning VA has submitted the request for investigation to the DCSA and the DCSA has scheduled the investigation; and,

(a) Favorable review by VA of the results of the intended PIV recipient's FBI NCHC (FBI fingerprint check) portion of the required background investigation.

(b) Interim PIV eligibility determinations are temporary and will be recorded in OPM's CVS, or successor database. Instructions for recording interim PIV eligibility in CVS will be provided in separate guidance from OPM. Because the interim PIV eligibility issued is based on a fingerprint check, VA must manage this risk by putting adequate procedures in place to monitor the completion of the investigation and its prompt adjudication.

b. Step 2 in the Two-Step process consists of the final PIV eligibility determination and is based on a favorable adjudication of the completed investigation. If the final credentialing decision is unfavorable, VA will need to record the unfavorable determination in CVS or any successor database, while also taking steps to recover the PIV card and render it physically inoperable.

Table 2: USAccess Applicant Eligibility and Access Type

PIV card Type	PIV	PIV-I	PIV- I Flash
VA Positions	Employee, Contractor, Affiliate	Employee, Contractor, Affiliate	Employee, Contractor, Affiliate
Employment Appointment/Contract Duration Requirements	More than 180 aggregate days in a one-year period or is expected to be renewed for multiple years	six (6) months (or less) in a 1-year period	six (6) months (or less) in a 1-year period
Access Requirements (Logical Access)	Yes	Yes	No
Access Requirements (Common Physical Access[1])	Yes	Yes	Yes
Access Requirements (Restricted Physical Access[2])	Yes	Yes	No

[1] Building access provided by showing PIV card to security guard.
[2] Building access provided by scanning PIV card on Physical Access Control System Readers

PIV card Type	PIV	PIV-I	PIV- I Flash
Access Requirements (Access to Sensitive Records)	Yes	Yes	No
Investigation Requirements (Special Agreement Check)	Adjudicated SAC Required	Adjudicated SAC Required	Adjudicated SAC Required
Investigation Requirements (Background Investigation[3])	Background Investigation Initiated (for Interim PIV Eligibility; Favorably Adjudicated Investigation for Final PIV Eligibility)	Background Investigation Initiated (for Interim PIV-I Eligibility; Favorably Adjudicated Investigation for Final PIV Eligibility)	No Background Investigation Required
Investigation Requirements (Number of IDs Required[4])	Two I-9 Compliant IDs (Two IDs from Lists 1 and 2, provided one is a state or federally issued photo ID)	Two I-9 Compliant IDs (Two IDs from Lists 1 and 2, provided one is a state or federally issued photo ID)	Two I-9 Compliant IDs (Two IDs from Lists 1 and 2, provided one is a state or federally issued photo ID)

(1) Contractors and Affiliates which may include Health Professional Trainee (HPTs) include all title 38 and title 38-Hybrid occupations.

(2) Paid and Without Compensation (WOC).

8. Undergraduate, graduate, and post-graduate students, interns, residents, and fellows.

9. HPTs will be provisioned with the appropriate PIV card before their Training Program begins.

10. VA will consider the benefits of PIV eligibility determinations for intermittent or temporary employees whose affiliation is repeatedly terminated and reinstated and for any employees who are expected to serve intermittently over multiple years, such as HPTs. Intermittent employees with affiliation extending beyond 6 continuous months are not considered “short-term.” Seasonal employees, i.e., employees on permanent appointments who work

[3] Background investigations are Tier I or higher.
[4] IDs are presented to PIV Registrar for identity proofing of an Applicant.

a seasonal schedule of 6 months or more on a recurring basis, are not considered “short-term.”

11. OPM credentialing standards and procedures generally apply to contractors and affiliates personnel unless they are short-term (i.e., less than 6 continuous months) employees, in which case VA has discretion to vet those personnel for PIV cards based on risk and other factors, and to issue an alternative identity credential (such as the PIV-I credential) with appropriate restrictions and alternative security protections.

12. Contractors and Affiliates can be issued a PIV-I Flashcard, PIV-I card, or PIV card dependent on the program, length of the agreement, and/or position requirements.

13. Contractors and Affiliates will receive a PIV-I Flash card, which is limited to 180 days if:

    a. Appointed for 180 days or less in a 1-year period, and they have no need for logical access.

14. Contractors and Affiliates receive a PIV-I card if:

    a. Appointed for 180 days or less in a 1-year period or are non-US nationals.

15. Contractors and Affiliates receive a PIV card if:

    a. They are appointed for more than 6 months in programs that provide intermittent employment that extends for multiple years.

16. Contractors and Affiliates transferring from one VA facility to another should retain their originally issued credentials for use at the new VA facility.

17. Contractors and Affiliates who require access to VA information systems and facilities will need to complete a Tier 1 background investigation at a minimum.

APPENDIX E: EMPLOYMENT ELIGIBILITY VERIFICATION

All VA employees, contractors, and affiliates must meet the following criteria before issuing a PIV card.

1. **FIPS 201-3, Section 2.7** 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 FIPS 201-3. At least one document shall be a valid state or Federal Government-issued picture identification.

2. Identity Document Criteria.

    a. The PIV Registrar must examine each acceptable identity document (see List 1, List 2) provided by the Applicant.

    b. All identity source documents must be unexpired.

    c. Any document that appears invalid (e.g., fails electronic verification, 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 PIV Registrar and reported to the PCIF Manager for review.

    d. Handwritten or photocopied documents are not acceptable.

3. Acceptable Identity Documents.

    a. Two forms of identification are required from List 1, PIV card Identity Verification Matrix, for all PIV, PIV-I, and PIV-I Flash. The following combinations are accepted:

        (1) Two forms of identification from Column A (Government-Issued Photo ID).

        (2) One form of identification is from Column A, and one form is from Column B (Non-Picture ID or Acceptable Picture ID not issued by state or Federal Government).

4. 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 sources 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.

    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 two forms of ID compliant with PIV Guidelines if she provides a marriage license displaying both her maiden name and married name.

d. The REAL ID Act establishes minimum security standards for license issuance and production and prohibits Federal agencies from accepting, for certain purposes, driver's licenses and identification cards from states not meeting the Act's minimum standards. The purposes covered by the Act include accessing Federal facilities, entering nuclear power plants, and boarding federally regulated commercial aircraft. A full list of state IDs that are acceptable for identity proofing under the REAL ID Act can be found on the DHS REAL ID site. States that have not finalized and issued REAL ID-compliant identification may have been granted REAL ID Compliance Extensions. Facilities should reference the Department of Homeland Security (DHS) REAL ID Compliance Extensions Update site for a full list of states that have been granted extensions. If a state has been granted a compliance extension, the state ID can be accepted for proof of PIV identity.

List 1: USAccess Primary Acceptable Forms of ID.

(1) U.S. Passport or a U.S. Passport Card

(2) Permanent Resident Card or an Alien Registration Receipt Card (Form I-551).

(3) Foreign passport.

(4) Employment Authorization Document that contains a photograph (Form I-766)

(5) a Driver's license that is compliant with REAL ID or an ID card issued by a state or possession of the United States, provided it contains a photograph.

(6) U.S. Military ID card.

(7) U.S. Military dependent's ID card; or

(8) PIV card.

Note: Photos are required for all forms of primary identification above.

List 2: USAccess Acceptable Secondary Forms of Identification.

(1) U.S. Social Security Card issued by the Social Security Administration (SSA)
Note: Laminated SSA cards cannot be used without the Agency Security Officer's approval).

(2) Original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal.

(3) Voter's registration card.

(4) U.S. Coast Guard Merchant Mariner Card.

(5) Certificate of U.S. Citizenship (Form N-560 or N-561).

(6) Certificate of Naturalization (Form N-550 or N-570).

(7) U.S. Citizen ID Card (Form I-197).

(8) Identification Card for the use of a Resident Citizen in the United States (Form I-179).

(9) Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS 545 or Form DS-1350).

(10) Employment authorization Document issued by the Department of Homeland Security (DHS).

(11) Employment Authorization Document issued by DHS with photograph (Form I-766).

(12) Driver's license issued by a Canadian government entity.

(13) Native American tribal documents.

(14) Veteran Health Identification Card.

(15) Agency ID badge issue by Federal, state, local government agency – not a facility access badge.

(16) Another piece of evidence that meets the requirement of NIST SP 800-63-4

Table 3: Acceptable Name Mismatches

Name	Sponsorship Record Shows	Identity Document Shows
First	Single first name: “Mary L.” (with “L.” given as middle initial)	First name as two words: “Mary Lou”
First	First name as two words: “Mary Lou”	Single first name: “Mary L.” (with “L.” given as middle initial)
Middle	Single letter as middle initial: Example: “L.”	Middle name spelled out; first letter of the name matches the single letter: Example: “Lawrence”
Middle	Middle name spelled out; first letter of the name matches the single letter: Example: “Lawrence”	Single letter as middle initial: Example: “L.”
Middle	Compressed middle name: Example “Heewan”	Properly formed expansion of middle name: Example: “Hee-Wan”
Middle	Properly formed expansion of middle name: Example: “Hee-Wan”	Compressed middle name: Example “Heewan”
Last	Hyphenated last name: “Smith-Jones”	Non-hyphenated last name: “Smith Jones”
Last	Non-hyphenated last name: “Smith Jones”	Hyphenated last name: “Smith-Jones”

Table 4: Not Acceptable Name Mismatches

Not Acceptable Mismatches	Sponsorship Record	Identity Document
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”

Table 5: Enrollment Procedures for Suffix Mismatch in USAccess

Sponsorship Record	Identity Document	PIV Registrar Action
John Smith II or John Smith	John Smith or John Smith II	Verify the last four digits of the Applicant’s social security number on the ID document with the social security number in the Applicant’s record. If there is a match, the PIV Registrar can enroll the Applicant. If neither ID document contains a social security number, the Applicant must return with a document showing the social security number.
John Smith II or John Smith Jr.	John Smith Jr. or John Smith II	There is no need to have social security number verification. The PIV Registrar can enroll the Applicant.

APPENDIX F: CREDENTIAL TOPOLOGIES.

1. PIV card Topology can be found under *VA USAccess PIV card Examples and Information* below. Refer to *FIPS 201-3, Section 4.1.4 PIV Visual Card Topography* for additional information.

2. PIV-I card Topology can be found under *VA USAccess PIV-I card Examples and Information* below.

3. PIV-I Flashcard Topology can be found under *VA USAccess PIV-I Flash card Examples and Information* below.

4. Color-Coding for Employee Affiliation.

    a. 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) Employee – White/No Name Bar or Photograph Border

        (2) Contractor – “Kelly Green” Name Bar and Photograph Border

        (3) Affiliate/Associate – White/No Name Bar and Orange Photograph Border

        (4) Non-U.S. National – Blue Name Bar and Blue Photograph Border

        (5) Federal Emergency Response Official – Red Bar

    b. PIV-I Flash cards have a black photograph border and the name bar has no color.

5. The back of each credential includes the Applicant’s identifying physical characteristics traits: height, hair, and eye color.

6. PIV cards issued under the auspice of the National Nurses United agreement have the Registered Nurse (RN) and/or Advanced Practice Registered Nurse (APRN) designation.

VA USAccess PIV card Examples and Information

See some of the PIV card attributes below.

1. Top Left Section of the PIV card.
    a. “United States Government” header
    b. Photograph with affiliation color border
    c. Name with affiliation color bar.
2. Top Right Section of the PIV card
    a. Department Seal.
    b. Expiration Date: MMMYYYY format
    c. Affiliation: Employee, Contractor, Affiliate, Foreign National
    d. Agency/Department: Department of Veterans Affairs
    e. Credential Issued Date: YYYYMMMDD format.
    f. Credential Expiration Date: YYYYMMMDD format.
3. Bottom Center Section of the PIV card:
    a. Integrated Circuit Chip.
    b. Federal Emergency Response Official: “Federal Emergency Response Official” in red font at bottom center. (See figures 5-6 for an example)

Examples of the VA USAccess PIV cards are below.

Figure 1- Employee PIV card.

Figure 2- Contractor PIV card.

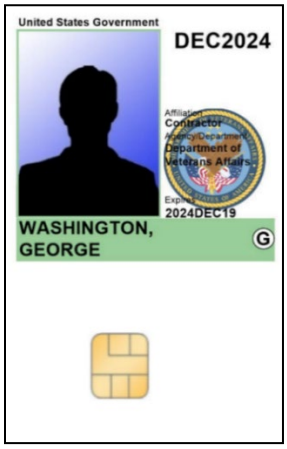


Figure 3 - Affiliate PIV card.

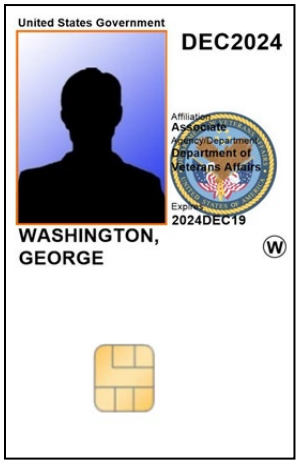


Figure 4 - Non-U.S. National PIV card.

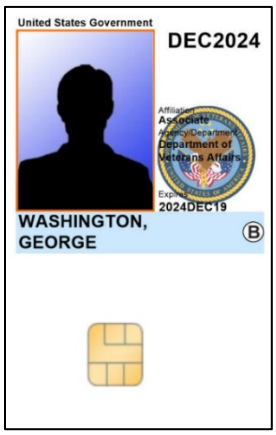


Figure 5 - Federal Emergency Responder PIV card - Example 1.

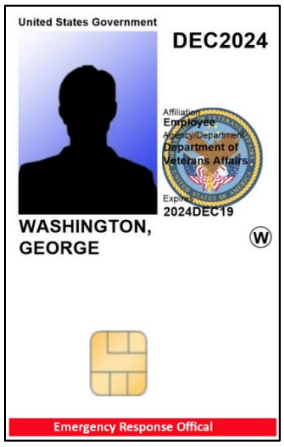


Figure 6 - Federal Emergency Responder PIV card - Example 2.

VA USAccess PIV-I card Examples and Information

See some of the PIV-I card attributes below.

1. Left Section of PIV-I card.
    a. “United States Government” header
    b. Cardholder photograph
    c. Name with or without affiliation color bar Name with no affiliation color bar.
2. Center section of the PIV-I card.
    a. “Department of Veterans Affairs” sub-header
    b. Department Seal with or without medical designation
    c. Expiration Date: YYYYMMMDD format
3. Bottom Center Section of the PIV-I card Example.
    a. Expiration Month and Year: MMMYYYY format
    b. Integrated Circuit Chip
    c. USAccess PIV-I logo

Examples of the VA USAccess PIV-I cards are below.

Figure 7 - Employee PIV-I Card Example.

Figure 8 - Contractor PIV-I Card Example.

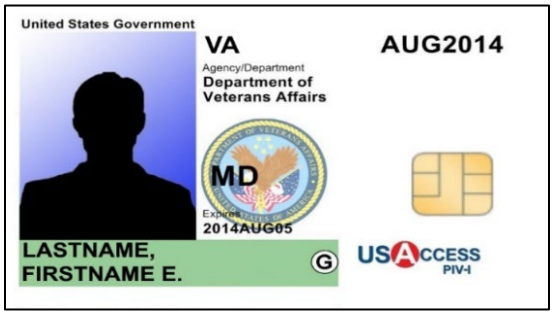


Figure 9 - Non-U.S. National PIV-I Card Example.

VA USAccess PIV-I Flash card Examples and Information.

See some of the PIV-I Flash card attributes below.

1. Left Section of PIV-I Flash card.
    a. “United States Government” header.
    b. Cardholder photograph with black border.

c. Name with or without affiliation color bar.

d. Name with no affiliation color bar.

2. Center Section of PIV-I Flash card.

a. “Department of Veterans Affairs” sub-header.

b. Department Seal with or without medical designation Expiration Date: YYYYMMMDD format.

3. Right Section of PIV-Flash card.

a. Expiration Month and Year: MMMYYYY format.

b. FLASH.

c. Integrated Circuit Chip.

d. USAccess PIV-I logo.

Examples of VA USAccess PIV-I Flash cards are below.

Figure 10 - Employee PIV-I Flash Card Example.

Figure 11 - Contractor PIV-I Flash Card Example.

Figure 12 - Non-U.S. National PIV-I Flash Card Example.

APPENDIX G: BIOMETRIC DATA CAPTURE

(SOURCE: NIST SP 800-76-2: Biometrics Specifications, and VA PIV card Issuance Office Standard Operating Procedures, November 2024, v.1.6) The PIV Registrar captures the Applicant's fingerprints in accordance with the requirements below:

a. 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 PIV 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.

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

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

e. 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.

f. 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.

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

a. Preferred index finger.

b. Another index finger.

c. Preferred middle finger.

d. Another middle finger.

e. Preferred thumb finger.

f. Another thumb finger.

g. Preferred ring finger.

h. Another ring finger.

i. Preferred little finger; and

j. Another little finger.

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

   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 **(unless the head covering is for religious purposes).**

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

   d. Eye patches, dark glasses, or non-prescription glasses are allowed for medical reasons only. Medical certificates must be presented by the Applicant to validate the need for the covering when such need is not obvious. Any such medical documentation must be returned to the Applicant. PIV cards 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 card 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.

4. VA's standards are informed by those of the Department of State under which a reasonable likeness is generally obtained when the full face is visible, and the religious headwear does not cast a shadow on the face. Some types of religious headwear cover all or part of an individual's face, and the portion that covers the individual's face must be adjusted or removed to make the full face visible and avoid casting a shadow. Other types of headwear, although they do not cover the face, may need to be adjusted in order to reveal an individual's crown, chin, or sides of the face, or to prevent a shadow being cast across the face in the photograph. Headwear does not need to be removed if the Applicant adjusts it to meet photograph requirements. This means the PIV Applicant must adjust their headwear so that 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 is visible. VA's interest in documenting or verifying the appearance of an individual with a photograph generally can be achieved while accommodating individuals who wear headwear as part of

their daily religious observance as long as the face is not obscured, and a reasonable likeness can be obtained. If the Applicant is not willing to comply with the above requirements, the request will be assessed on a case-by-case basis. [5]

5. Federal agencies, including VA, are subject to the Religious Freedom Restoration Act of 1993 (RFRA), 42 U.S.C. §§ 2000bb et seq., which prohibits any Federal Government practice that substantially burdens a person's exercise of religion, unless the Government demonstrates that the practice represents the least restrictive means of furthering a compelling governmental interest. This statement does not address VA's compliance with RFRA; it is only a statement of VA policy.

[5] HSPD-12 Policy on Headwear in PIV Photo. May 5, 2015.

APPENDIX H: CREDENTIAL DESTRUCTION.

1. In accordance with VA Credential Management PMO policy, the following cases will result in credential destruction:

    a. A Federal employee, contractor, or affiliate separate (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. PCIF Managers are responsible for ensuring and verifying that PCIFs are in compliance with PIV card stock destruction policies as outlined in VA Credential Management PMO guidance. PCIF Managers or facility directors have the following options regarding PIV card/Card destruction depending on the volume produced:

    a. Destruction by Cutting:

        (1) Cut the PIV card 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. (See Figures 13-16)

    b. Destruction by Strip Shredder:

        (1) A strip shredder that reduces the credential to nominal two mm strip width cut shreds.

c. Destruction by Disintegration/Incineration:

(1) A commercial disintegration or incineration service provider complying with incineration or disintegration to nominal two mm size particles.

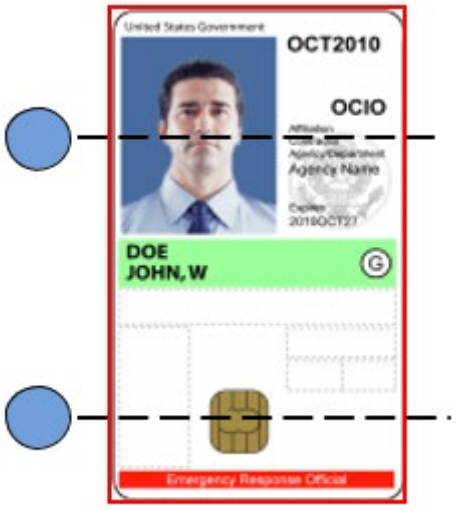
d. Destruction by an authorized vendor:

(1) Authorized vendors utilizing personnel with proper background investigations that provide on or off-site secure destruction services and reduce the credential to nominal two mm strip width cut shredding or via licensed incineration.

e. Destruction by Cutting Steps:

(1) Step 1: Cut the card horizontally into three parts. The first cut through the face, and the second cut directly through the middle of the smart chip, as seen in Figure 13.

Figure 13: Step 1 of PIV card destruction.

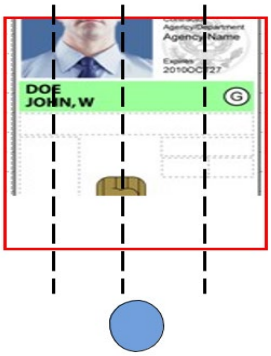


(2) Step 2: Cut card vertically into three parts; first cut through the remainder of the facial image; second cut directly through remaining half, as seen in Figure 14.

Figure 14: Step 2 of PIV card destruction.

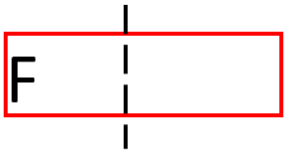
(3) Step 3: Cut card vertically into three parts; first cut through the remainder of the facial image; second cut directly through the remaining half of the smart chip, as seen in Figure 15.

Figure 15: Step 3 of PIV card destruction.



(4) Step 4: Cut card vertically into two parts; cut directly through the remaining half of the smart chip, as seen in Figure 16.

Figure 16: Step 4 of PIV card destruction.



APPENDIX I: BACKGROUND INVESTIGATION TIERS.

Table 6: Background Investigation Tiers

RISK LEVELS	CRITERIA
Tier 5/ Special-Sensitive	Positions with the potential to cause inestimable damage to national security, including: • Access to Sensitive Compartmented Information (SCI) • Access to any other intelligence-related Special-Sensitive information or involvement in Top Secret Special Access Programs (SAP) • Any other position the agency head determines to be at a higher level than Critical-Sensitive due to special requirements that complement EO 10450 and EO 12968
Tier 5/ Critical-Sensitive	Potential for exceptionally grave damage to national security. Includes positions involving any of the following: • Access to Top Secret or "Q" classified information. • Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war. • National security policymaking or policy-determining positions, the duties of which have the potential to cause exceptional or grave damage to the national security Investigative duties, the issuance of personnel security clearances, or duty on personnel security boards. • The adjudication, recommendation of adjudicative determinations, and/or granting of personnel security clearances. • Duty on personnel security boards. • Other positions related to national security, regardless of duties that require the same degree of trust.
Tier 4/ High Risk Public Trust	Positions included are those that have the potential for exceptionally serious impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority: • Policy making, policy determination, and policy implementation. • Assignments with major program or line management responsibilities (for example, Senior Executive Service (SES) positions or SES equivalents). • Independent spokesperson or non-management positions with authority for independent action. • Other positions designated by the agency head or designee that require the same degree of Public Trust.
Tier 3/ Noncritical-Sensitive	Potential for damage to national security. Includes positions that involve any of the following: • Access to Secret, "L," or Confidential national security information. • Duties that may directly or indirectly adversely affect the national security operations of the agency and do not rise to the level of the positions listed above.

RISK LEVELS	CRITERIA
Tier 2/ Moderate Risk Public Trust	Positions included are those that have the potential for Tier 2/moderate to serious impact involving duties of considerable importance to the agency or program mission with significant program responsibilities and delivery of customer services to the public such as: • Senior staff assistants to positions with policy making, determining, and implementation authority. • Mid-level management assignments such as supervisory or managerial positions that report directly to an SES position or SES equivalent. • Non-management positions with authority for independent or semi-independent action. • Other positions designated by the agency head or designee that require the same degree of Public Trust.
Tier 1/ Low Risk	Potential for impact involving duties of limited relation to the agency mission with program responsibilities that affect the efficiency of the Federal service. Computer positions not included in the criteria for Public Trust levels.

APPENDIX J: CREDENTIALING ELIGIBILITY OF NON-UNITED STATES NATIONALS.

1. VA is required to apply the OPM credentialing standards procedures to non-U.S. nationals[6] who work as employees or contractors for Federal Departments or Agencies or others who require long-term logical or physical access to Federal Government facilities whether overseas or in the United States.

2. Due to limitations that apply to the employment of non-U.S. nationals and the ability to collect background investigation information in locations outside the United States, special considerations apply when a PIV card is needed for a non-U.S. national in either U.S-based locations or foreign locations. In many circumstances investigative standards cannot be met and therefore a PIV may not be issued. Agencies may elect to issue alternative identity credentials (such as a PIV-I card) in these cases if they wish to accept the risk. Reciprocity rules do NOT apply to VA issued alternative identity credentials.

3. The special considerations that apply to the requirements for non-U.S. nationals are outlined below:

Table 7:Employment Authorization Verification

Location	**Employment Authorization Verification Requirements for Non-U.S. National Federal Employees or Contractors**
U.S. Based Locations	Verify employment eligibility through E-Verify.
U.S. Territories (Other than American Samoa[7])	Verify immigration status through the United States Citizenship and Immigration Services (USCIS)' Systematic Alien Verification for Entitlements (SAVE) system.[8]
Foreign Locations	Not Applicable (N/A)

[6] The term “United States national” includes both U.S. citizens and U.S. non-citizen nationals (i.e., American Samoans https://www.opm.gov/suitability/suitability-executive-agent/policy/cred-standards.pdf).
[7] The U.S. territory of American Samoa is not included in the "United States" as defined by the Immigration and Nationality Act and therefore the DHS E-Verify and SAVE verification programs are unable to verify work authorization or immigration status of individuals in American Samoa. Agencies should conduct such background investigation as may be possible and appropriate under the circumstances in this territory. Prior to 2008, the Commonwealth of the Northern Mariana Islands (CNMI) was also not included in the “United States”; however, on May 8, 2008, the Consolidated Natural Resources Act extended most provisions of the U.S. Immigration Law to the CNMI. The transition of U.S Immigration Law in the CNMI began on November 28, 2009 and was scheduled to end on December 31, 2019. DHS E-Verify may now be available for employment authorization verification in CNMI.
[8] https://www.uscis.gov/save

Table 8:Background Investigation Requirements

Location:	If the person has been in the U.S. or U.S. Territory for:	Investigation Requirements and Exceptions
U.S. Based Locations or U.S. Territories	3 or more years, **continuously and immediately preceding** the start of Federal affiliation	Initiate the Tier 1 investigation or equivalent after employment authorization or immigration status is verified**.**
U.S. Based Locations or U.S. Territories	Less than 3 continuous years preceding the start of Federal affiliation	A Tier 1 investigation may NOT be requested on Non-U.S. Nationals in the U.S. or U.S. Territory for less than 3 years. At the discretion of the agency, based on a risk determination, an alternative facility access (PIV-I) identity card[9] may be issued until the employee or contractor in question has resided for 3 years in the U.S. or U.S. Territory. If an alternative facility access identity card is issued, the following checks are still required: [10] • FBI fingerprint-based NCHC must be completed before an alternative facility access identity card is issued. • FBI Investigations files (Names Check). • Names check against the Terrorist Screening database. • USCIS Check against SAVE. The above checks will provide limited results, will not constitute a Tier 1 investigation, and will not be documented as a Tier 1 investigation.
Foreign Locations	**N/A**	It is generally not possible to conduct a Tier 1 investigation on a Non-U.S. national in a foreign location. (Exceptions are possible for Non-U.S. Nationals who have resided in the U.S. or U.S. Territory for 3 years prior to the conduct of a Tier 1 investigation.)

[9] Reciprocity rules do NOT apply to agency issued alternative facility access identity cards.
[10] Agencies may establish a Special Agreement Check (SAC) with DCSA for the purpose of conducting these checks on non-U.S. Nationals. Contact DCSA Customer Liaison at 724-794-5612.

Location:	If the person has been in the U.S. or U.S. Territory for:	Investigation Requirements and Exceptions
		If an investigation that is equivalent to a Tier 1 investigation cannot be performed, an alternative facility access identity card may be issued at the discretion of the Department of State Chief of Mission Authority, Department of Defense Installation Commander and/or other agency official, as appropriate, based on a risk determination.