VA IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT

1. **REASON FOR ISSUE**: The Department of Veterans Affairs (VA) Handbook 6510 VA Identity, Credential and Access Management (ICAM), is updated to fulfill the Federal Government's ICAM policy requirement for the Department to define and maintain a single comprehensive ICAM policy that is consistent with agency authorities and operational mission needs. The VA ICAM policy guidance and supporting ICAM processes and technology solution roadmap will also enable the Department to perform more effective governance, coordination and oversight over other Department programs that make use of or rely on ICAM technologies and solutions.

2. **SUMMARY OF MAJOR CHANGES/SUMMARY OF CONTENT:**

   a. Change responsible office to Office of Information Technology (OIT) ICAM Program Management Office (ICAM PMO) – Office of Information Security (OIS).

   b. Scope of the VA 6510 Handbook has been expanded from its previous scope to address the Office of Management and Budget (OMB) Memorandum (M) -19-17's requirement that agencies have a single, comprehensive ICAM policy, based on an Office of Inspector General (OIG) notice of finding and recommendation.

   c. Update VA policies to meet or exceed the Federal standards listed in the full suite of National Institute of Standardization and Technology (NIST) Special Publication (SP) 800-63-3 - Digital Identity Guidelines publications (hereby referred to as NIST SP 800-63). This includes the entire suite of 800-63 publications: 800-63A - Enrollment and Identity Proofing, 800-63B - Authentication and Lifecycle Management and 800-63C - Federation and Assertions.

   d. Provide guidance to address requirements prescribed in OMB M-19-17 – Enabling Mission Delivery through Improved Identity, Credential and Access Management (hereby referred to as OMB M-19-17).

   e. Revise VA policies and provides guidance to incorporate President's Executive Order 14028 – Improving the Nation's Cybersecurity (hereby referred to as Executive Order 14028).

   f. Revise VA policies and provides guidance to incorporate OMB M-22-09 – Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (hereby referred to as OMB M-22-09).

g. Revise VA policies and provides guidance to incorporate Executive Order 14058 – Transforming Federal Customer Experience and Service Delivery (hereby referred to as Executive Order 14058).

h. Revise VA policies and provides guidance to incorporate Executive Order 13988 – Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation (hereby referred to as Executive Order 13988).

i. Update VA policies to meet or exceed the Federal standards listed in NIST SP 800-207 - Zero Trust Architecture (hereby referred to as NIST SP 800-207).

j. Provide additional clarification on VA policies on the Physical Access Control Systems (PACS).

k. Update roles and responsibilities for various offices for enterprise identity, credential and access management functions.

l. Provide criteria for telephone identity proofing (Appendix C) and address confirmation (Appendix D).

m. Provide tables for Assurance Level Guide (Appendix E), Authenticator Assurance Level Examples (Appendix F), Identity Proofing Levels (Appendix G), Risk Methodology (Appendix H) and Digital Identity Acceptance Statement (DIAS) template (Appendix I) from NIST SP 800-63.

3. **RESPONSIBLE OFFICE:** Office of Information Technology (005), Identity Credential Access Management Program Management Office, Office of Information Security (005R).

4. **RELATED DIRECTIVE:** VA Directive 6510, VA Identity, Credential and Access Management.

5. **RESCISSIONS:** VA Handbook 6510, VA Identity and Access Management, dated January 15, 2016.

Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 6510
Transmittal Sheet
September 27, 2024

CERTIFIED BY:

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

BY THE DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt D. DelBene
Assistant Secretary for
Information and Technology and Chief
Information Officer

DISTRIBUTION: Electronic Only

VA IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT

TABLE OF CONTENTS

VA IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT

1. PURPOSE.

a. VA Handbook 6510 establishes the foundation for VA comprehensive ICAM processes to effectively govern and enforce efforts across VA to adhere to Federal ICAM policies and guidance and foster accountability at all levels of the organization (per OMB M-19-17). VA ICAM PMO office is the business owner for ICAM and defines the business needs for ICAM within VA.

b. Apart from the guidance provided in this Handbook, all VA information technology systems shall be developed, operated and maintained to comply with the security control requirements for Identification and Authentication (IA), Access Control (AC) and Audit and Accountability (AU) that are specified in VA Directive 6500, VA Cybersecurity Program and Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, issued by the OIT. VA OIT is the ICAM information system owner (ISO) responsible for developing and maintaining the VA's ICAM technology solution roadmap, consistent with VA authorities and operational mission needs. OIT also manages, develops, operates and maintains enterprise-level ICAM technology for VA including support for the VA Personal Identity Verification (PIV) credentialing system, USAccess, which is a shared service operated by GSA.

c. The policies, processes and guidelines established in this Handbook further build on the established VA Directive 6500 – VA Cybersecurity Program to provide Federal Identity, Credential and Access Management (FICAM) guidance to address assurance levels, electronic authentication risk assessments, identity proofing, identity credential management, electronic signature, multifactor authentication (MFA) and access management.

d. The policies, processes and guidelines established in this Handbook are written to complement and in conjunction with the below VA Directives, Handbooks and memos to provide a comprehensive framework for ICAM initiatives for VA:

e. VA Directive 6500 - VA Cybersecurity Program and Handbook 6500 - Risk Management Framework for VA Information Systems VA Information Security Program. VA OIT issued 6500 Directive and Handbook and provide the risk-based processes for selecting VA information technology system security controls and operational requirements to implement VA Cybersecurity Program requirements.

f. The Office of Information Security (OIS) manages a policy portal known as the Information Security Knowledge Service (KS). This policy portal covers the Risk Management Framework extensively.

g. VA Directive and Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program - This Directive and Handbook establish Department-wide requirements, policies, roles and responsibilities for the creation, operation and maintenance of an HSPD-12 PIV Credential Management Program necessary to ensure Department compliance with HSPD-12.

h. VA Directive and Handbook 0710 “Personnel Security and Suitability Program” - This Directive and Handbook describe the purpose, responsibilities, requirements and procedures of VA’s Personnel Security and Suitability Program, applicable to Federal applicants, appointees, employees, contractors and affiliates who have access to departmental operations, facilities, information or information technology systems.

i. VA Directive and Handbook 0730 Security and Law Enforcement. The full series of Directive/Handbooks establishes mandatory procedures for protecting lives and property within VA’s jurisdiction. The Directive/Handbooks provides policies applicable to the management and administration of this program from VA Central Office and within VA facilities nationwide located on Department property.

j. VA Memo, Personal Identity Verification (PIV) Logical Access Policy Clarification (VA Integrated Enterprise Workflow Solution [VIEWS] 00155984) (reference ll). This establishes the VA’s requirement to ensure logical access to VA’s network and all information systems for internal users.

k. VA Memo, Requirement for Two Factor Authentication for VA Network Access for Individuals with Dual Identities (VA Intranet Quorum [VAIQ] 7735690) (reference mm). The memo provides the requirement that those VA users with dual identities (e.g., Employee and Contractor [moonlighter], etc.) will have unique sets of credentials for each user type that distinguish access rights (e.g., access rights associated with the contract they are employed as a contractor).

l. VA Memo, Multiple Exemption Management Policy (VIEWS 03979222) (reference nn). Pursuant to requiring a PIV card to access internal VA information systems, the temporary PIV exemption process is detailed.

m. VA Memo, Responsibilities of Business and System Owners (VIEWS 04250381) (reference oo). Provides clarification of the responsibilities of Business/System Owners to ensure connectivity with the VA network.

2. **SCOPE.** The scope of this Handbook is specifically focused on the roles, responsibilities and requirements associated with the following set of VA ICAM activities, functions, processes and services:

a. Assurance Levels and system Digital Identity Risk Assessments (DIRA) – The process to determine system Identity Assurance Levels (IAL),

Authentication Assurance Levels (AAL) and if applicable, Federation Assurance Levels (FAL). This process examines 1) system transactions, 2) potential for misuse of transaction information, 3) overall risk to individuals, 4) VA operations, 5) VA assets and 6) potential impact to the organization in determining the individual assurance levels for each VA system.

b. Enterprise Identity Proofing – The process of establishing and verifying the identity of a subject.

c. The identity proofing process to issue identity credentials to employees, contractors or affiliates requiring physical access to VA facilities and/or internal VA network logical access must also comply with VA Directive and Handbook 0735 HSPD-12 PIV Credential Management Program (reference bb) and VA Directive and Handbook 6500.

d. Identity proofing for external users, including public users, for logical access to VA resources must comply with NIST requirements. For external Federal users, VA must leverage existing agency credentials and identity federations that satisfy the VA's accepted risk level to accept identity and authentication assertions. For public consumers, VA must leverage either Federal or commercial shared services to deliver identity assurance and authentication services to the public.

e. Electronic Credential Management – The sponsorship, enrollment, issuance and revocation of authentication tokens including the use of phishing-resistant credentials. An authentication token binds a digital identity to a user as a credential.

f. Electronic Signatures – The process of applying any mark in electronic form with the intent to sign a data object.

g. Access Management – The management, review and control of the ways in which entities are granted or denied access to the resources of an organization and are authorized to perform a specific action(s) within a given resource to apply principles of least privilege and audited to ensure the right individual to access the right resource, at the right time for the right reason. Access management also includes, but not limited to, Logical Access Control System (LACS), PACS, Zero Trust Architecture (ZTA) principles, full compliance with OMB M-22-09 Federal Zero Trust Strategy (reference k) and phishing-resistant MFA methods.

h. The security and privacy controls in VA Handbook 6500 (reference e) represent VA's information technology security requirements as they apply to VA information systems/applications utilizing ICAM Services. The VA National Rules of Behavior (RoB) provides the specific responsibilities and expected behavior for organizational/non-organizational users of VA's ICAM Services.

i. Federal Information Processing Standards (FIPS) 201-3 (hereby referred to as FIPS 201) Personal Identity Verification (PIV) requirements are addressed in VA Handbook 0710 (reference f) and VA Handbook 0735 (reference bb).

3. ROLES & RESPONSIBILITIES. Handbook 6510 applies to all VA Administrations, Staff Offices, all VA staff who support ICAM functionality, Veterans, contractors, affiliates and any users who require logical and physical access to VA information systems including, resources internally and externally managed and offered through VA.

a. Identity Proofing Officials are responsible for providing vetting services for applicants:

(1) Reviewing identity source documentation.

(2) Comparing identity source documentation to ensure data matches.

(3) Verifying authenticity and validity of identity source documentation.

(4) Recording identity source documentation data.

(5) Notifying the local Information System Security Officer (ISSO) when there is reasonable suspicion that an applicant presents fraudulent identity documentation as proof of identity (reference bb).

b. Applicants for Identity Proofing are any users requesting a credential for VA Services and VA Information Services (reference dd). These individuals are responsible for:

(1) Initiating requests for access to VA services and VA information systems.

(2) Providing identity proofing data (e.g., Personal Identifiable Information [PII]).

(3) Providing identity source documentation.

c. ISSOs are responsible for ensuring that the appropriate operational security posture is maintained for an information system or program, ensuring proper processes are followed, including:

(1) Escalating reports of suspected impersonation or fraud to the appropriate person/group.

(2) Assisting ISO with performing the system DIRA process.

(3) Reviewing the system DIRA and verifying assurance level determinations.

(4) Ensuring information systems comply with all security requirements in VA Handbook 6500 (reference e).

(5) Reviewing and approving recommended assurance level determinations.

(6) Reviewing and approving/rejecting requests for use of the electronic signature service(s).

(7) Reviewing Authority to Operate (ATO) documents.

(8) Ensure compliance with MFA access to VA network and information systems.

d. Local Chief of VA Police is responsible for coordinating with the Regional Counsel, OIG and required legal officials per program policy to conduct necessary investigation(s) and background verification of any observed or reported suspicion of impersonation or identity fraud.

e. System DIRA Authority is responsible for providing official authority to ensure risk assessments are conducted to determine the proper Assurance Level for credentials for applications, including:

(1) Receiving system DIRA(s) from designated assessor such as an ISSO.

(2) Evaluating risk assessments for assurance level determinations.

(3) Approving or Rejecting assurance level determinations.

(4) Approving assurance level determinations that the ISSO has acknowledged.

(5) Ensuring a DIAS (Appendix I) is included with artifact documentation.

f. The ISO (in accordance with Handbook 6500) is responsible for:

(1) Carrying out their responsibilities under 38 U.S.C. § 5723.

(2) Planning and budgeting for security and privacy control implementation, assessment and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

(3) Ensure that subject matter experts (SME) are consulted in the design, development, implementation, modification, test and evaluation of the system architecture in compliance with the cybersecurity and privacy component of the VA Enterprise Architecture and to make maximum use of enterprise cybersecurity and privacy.

(4) Signing and abiding by the Memorandum of Understanding (MOU) between the application and the electronic signature service owners.

(5) Coordinating with VA Administrations and Staff Offices as well as VA procurement practices and policies prior to the acquisition of IT or the integration of IT into information systems when required.

(6) Ensuring systems are identified, designated as such and centrally registered in the VA approved system(s) (e.g., Enterprise Mission Assurance Support Service [eMASS]).

(7) Ensuring information systems utilize VA's MFA services for system access (reference ll).

(8) Maintaining systems in accordance with VA Memo, Responsibilities of Business and System Owners (reference oo).

(9) Ensuring systems have appropriate encryption for data at rest, in transit and in use (reference k).

(10) Ensuring that users comply with VA policies and procedures governing the generation, collection, processing, dissemination and disposal of specified information.

(11) Performing system DIRA for their system/application role transaction if designated as the assessor by the system DIRA Authority. The VA Chief Information Officer (CIO), or as delegated by the VA CIO, is the System DIRA Authority.

(12) Comply with the rules for appropriate use and protection of information shared, processed, stored or transmitted within VA.

g. The Facility Physical Security Specialist/Assistant (each facility decides the responsibility owner as per their physical security set up) administers the card reader system and is responsible for:

(1) Providing physical access control system management – Add/edit staff to PACS system.

(a) Add/Edit/Delete Card holder data as needed.

(b) Add/Edit/Delete access levels as needed.

(c) Create new access or group levels as needed.

(d) Review and understand business policies and directives for staff sponsorship.

(2) Supporting device/system additions and maintenance to comply with standards as defined in FICAM guidance.

(a) Assist with facility needs for additional security devices and/or maintenance/upgrades such as readers, cameras and others to meet the FICAM standards.

(b) Interact with OIT to inventory desktop/laptop locations related to duress operations (reference aa) to keep PACS inventory of systems updated.

(c) Maintain training requirements associated with PACS for card reader systems and all equipment connected to facility security systems.

(d) Ensure PACS is configured to meet FIPS 201 standards and accept VA MFA credentials.

(3) Providing access schema management.

(a) Add new access levels as authorized.

(b) Maintain access schema levels as needed.

(c) Review access schema and update on a bi-monthly basis.

(4) Providing audit reports to law enforcement.

(a) Assist law enforcement with investigative data as needed.

(b) Provide audit reports based on card holder entrance logistics and timeline data.

(c) Provide audit reports based on door access logistics and timeline data to a specific or group of doors.

(d) Assist law enforcement with policy and guidelines for analysis of card holder or access area data.

(5) Assisting facility law enforcement personnel with emergency responses.

(a) Interact with law enforcement staff to assist with security policies.

(b) Provide camera recordings related to facility law enforcement requests.

(c) Provide for “lock down” requests for any appropriate emergencies.

(d) Training law enforcement staff in the use of security systems.

(e) Create facility Standard Operating Procedure (SOP) on operational use of security systems. Maintain updates accordingly.

(6) Interacting with local facility OIT regarding system/technical software updates.

(a) Maintain PACS software technical updates and version updates as needed.

(b) Review OIT Technical Reference Model (TRM) on a quarterly basis to assess PACS version decisions and timeframes for version updates.

(c) Participate with all PACS enterprise-level interactions with OIT.

(7) Adhering to physical access policies and procedures as stated in OMB M-19-17 (*The Risk Management Process for Federal Facilities: An interagency Security Committee Standard* defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level and provides an integrated, single source of physical security countermeasures. The guidance is available at https://www.dhs.gov/publications).

(a) Implement all VA PACS policies and guidance directives.

(b) Review and implement FICAM PACS-related directives.

(c) Stay current with GSA Approved Product List (APL) for PACS devices and systems.

h. The Electronic Signature Service Credential User is responsible for:

(1) Enrolling and applying for electronic signature credentials to conduct electronic record transactions through VA applications.

(2) Using and protecting assigned or selected electronic signature service credentials in accordance with VA policies agreed upon during issuance procedures.

(3) Addressing the consequences resulting from disclosing the electronic signature service credential within his/her control.

(4) All activities associated with his/her assigned electronic signature service credential.

(5) Not circumventing electronic signature services as provided by applications.

i. The Electronic Signature Service Credential Administrator is responsible for:

(1) Maintaining the electronic signature service credentials (e.g., person, non-person entities [NPE]), including the associated password, passphrase or personal identification number (PIN).

(2) Terminating the electronic signature service credentials upon termination of association with VA or the issuing authority's direction.

j. A Credential User is responsible for:

(1) Safeguarding issued MFA credentials including the associated password, passphrase or PIN.

(2) Safeguarding each credential to ensure it is used only by the associated user and is not to be shared with others.

(3) Reporting the loss or false use of an electronic credential to the appropriate authorities (including but not limited to the Facility Security Specialist [PACS]).

(4) Surrendering electronic credentials upon termination of association with VA or upon the direction of the issuing authority (applies to AAL 2 and AAL 3 physical authenticators, e.g., PIV cards).

(5) Renewing MFA credentials or certificates prior to the listed end date if remaining in the service of VA.

(6) Completing annual security and privacy training as required, signing VA RoB and complying with VA Handbook 6500 (reference e).

(7) Completing the appropriate background screening as required in VA Directive and Handbook 0710 (reference f) and VA Handbook 6500 (reference e).

k. Delegate (i.e., Surrogates, Power of Attorney, Legal Guardian) is responsible for:

(1) Acting on behalf of the Delegator.

(2) Adhering to all responsibilities held by the Delegator.

(3) Maintaining their authenticators.

(4) Not delegating privileges further unless allowed by organizational policy.

l. Delegator (i.e., Veterans, Account Owner, Claimant) is responsible for:

(1) Authorizing the level of access and defining the validity period for access by each delegate to the delegate's own provisioned account(s).

(2) Delegating portions of their authority to another user on a short-term or long-term basis, when allowed by organizational policy based on a risk assessment.

4. PROCEDURES.

a. Assurance Levels and System DIRA.

(1) To gain access to identity, credential or access services, information system applications must undergo a system DIRA to receive an Assurance Level determination. The Assurance Level determination guides the choice of technologies and the details of their implementation. The level considers whether the technologies selected provide adequate measures to support the residual assurance risk associated with the ability to conduct transactions with VA systems. Assurance Level determinations shall be evaluated whenever additional access or transactions are changed within the application.

(2) NIST SP 800-63-3 defines three components of identity assurance:

(a) IAL: Refers to the robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing errors.

(b) AAL: Refers to the robustness of the authentication process itself and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication errors (i.e., a false claimant using a credential that is not rightfully theirs).

(c) FAL: Refers to the robustness of the assertion protocol that the federation uses to communicate authentication and attribute information (if applicable) to a relying party (RP). FAL is optional as not all digital systems will leverage federated identity architectures. FAL is selected to mitigate potential federation errors (an identity assertion is compromised).

(3) Each of the Assurance Level provides a graduated scale that governs the requirements users must meet to assure their identity and conduct transactions with VA systems. Each Assurance Level is rated on a scale from one to three:

(a) IAL.

i IAL1: At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.

ii IAL2: At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in-person or remotely using, at a minimum, the procedures given in NIST SP 800-63A.

iii IAL3: At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized Credential Service Provider representative by examining physical documentation as described in NIST SP 800-63A.

(b) AAL.

i AAL1: provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.

ii AAL2: provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.

iii AAL3: provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.

(c) FAL.

i FAL1: permits the RP to receive a bearer assertion from an Identity Provider (IdP). The IdP must sign the assertion using approved cryptography.

ii FAL2: adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.

iii FAL3: requires the subscriber to present proof of possession of a cryptographic key reference to in the assertion and the assertion artifact itself. The assertion must be signed using

approved cryptography and encrypted to the RP using approved cryptography.

(4) System DIRAs leverage the basic framework for existing security risk categorization, as defined in VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program. This framework is modified to assess each of the transactions available to a role in a system and assign risk to and determine the assurance level for each of those transactions. A self-assessment is also conducted for each transaction using a nine-point scale in six impact categories, defined in NIST SP 800-30-1 (NIST SP 800-30) – Guide for Conducting Risk Assessments.

(a) ISOs, working with lines of business, identify the user roles and individual transactions available to each of those roles in each system.

(b) A self-assessment is conducted by the ISOs and lines of business to assign scores for the impact and probability of each of the six impact categories for a given system. Voting scores Low (1-3), Moderate (4-6), High (7-9), refer to Appendix H. The following six considerations are provided for each impact category to assist in capturing all risks and impacting criteria:

i Damage to reputation - Consider inconveniences, distress or damages that occur to the standing or reputation of any involved party.

A Low - limited, short-term inconvenience, distress or embarrassment to any party.

B Moderate - serious short-term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.

C High - severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

ii Financial loss/liability - Consider potential unrecoverable financial losses incurred by involved parties and which liabilities VA would incur.

A Low - insignificant or inconsequential unrecoverable financial loss to any party or at worst, an insignificant or inconsequential agency liability.

B Moderate - a serious unrecoverable financial loss to any party, or a serious agency liability.

C High - severe or catastrophic unrecoverable financial loss to any party or severe or catastrophic agency liability.

iii Harm to VA programs or public interest - Determine how VA programs will be harmed or disrupted. Public interest may be tangible, such as an asset, building, program or anything that has value to the business. Public interest may be intangible, such as VA trustworthiness or integrity (note reputation is dealt with in statement 3b above).

A Low - a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (a) mission capability degradation to the extent and duration that the organization can perform its primary functions with noticeably reduced effectiveness, or (b) minor damage to organizational assets or public interests.

B Moderate - a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (a) significant mission capability degradation to the extent and duration that the organization can perform its primary functions with significantly reduced effectiveness; or (b) significant damage to organizational assets or public interests.

C High – a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (a) severe mission capability degradation or loss of the extent and duration that the organization cannot perform one or more of its primary functions; or (b) major damage to organizational assets or public interests.

iv Unauthorized release of sensitive information - Consider the effect(s) that result from an unauthorized release of VA sensitive information. In assessing the degree of impact, it is important to consider the type and number of records. The potential harm to VA or an individual's privacy is the focal point for determining the degree of impact.

A Low - a limited release of VA sensitive information to unauthorized parties resulting in a loss of confidentiality with a low-impact as defined in FIPS 199, Standards for

Security Categorization of Federal Information and Information Systems.

B Moderate - a release of VA sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate-impact as defined in FIPS 199.

C High – a release of VA sensitive information to unauthorized parties resulting in loss of confidentiality with a high-impact as defined in FIPS 199– Standards for Security Categorization of Federal Information and Information Systems.

v Personal safety - Any ability to modify health information poses risks to personal safety. Most other transactions would not impact personal safety and would be rated “not applicable” or “N/A.”

A Low - minor injury not requiring medical treatment.

B Moderate - moderate risk of minor injury or limited risk of injury requiring medical treatment.

C High - a risk of serious injury or death.

vi Civil/Criminal violations - Determine if VA be subjected to civil or criminal violations.

A Low - a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.

B Moderate - a risk of civil or criminal violations that may be subject to enforcement efforts.

C High - a risk of civil or criminal violations that are of special importance to enforcement programs.

(5) Risk scores shall be calculated for each transaction based on the assessed impact and probability score for each impact category. Assurance levels are determined based on the risk score for each impact category. The highest assurance determination from each impact category is the overall assurance level for a transaction.

(a) ISOs may accept a single assurance determination for all transactions performed by a single set of users; or

(b) ISOs may accept multiple assurance determinations for each transaction performed by a single set of users.

(c) Once an assurance determination has been assigned, compensating controls may be implemented to reduce the risk level and associated assurance determination for a given impact category. Compensating controls may influence the assurance determination of multiple impact categories and are selected in accordance with the policies in VA Handbook 6500 as they relate to risk reduction (risk methodology is provided in Appendix H).

(6) The final determination for Assurance Levels shall be approved by the system DIRA authority and the determination recommendation is provided to the ISO for acceptance. A Digital Identity Acceptance Statement will also be required for artifact creation and retention (Appendix I provides the DIAS template).

b. Identity Lifecycle Management (ILM).

(1) The VA shall implement the ILM process including the three distinct phases (Joiner-Mover-Leaver) with individual steps within each phase.

(a) Joiner – Stage 1:

i Creation – Establish a new Master User Record (MUR) or an identity associated with an existing MUR made of attributes that define a person or entity. Processes associated with creation include digital identity or authoritative attribute source.

ii Identity Vetting - The process by which information is collected, validated and verified about a person. For federal employees, contractors and anyone working for or on behalf of the Government this phase will include the prerequisite vetting investigation and adjudication. Processes associated with identity proofing include source document validation, identity verification, remote proofing or in-person proofing.

iii Provisioning - Create, manage and delete accounts and entitlements in dependent systems. Dependent systems are either authoritative attribute sources such as directories or consuming sources such as single sign-on (SSO) systems and applications with provisioning processes. Processes associated with provisioning include entitlement management, grant access, remove access, account management and account creation.

(b) Mover – Stage 2:

i Maintenance - Maintain accurate and current attributes and entitlements associated with a MUR. Processes associated with maintenance include attribute management or access

reviews.

ii Identity Aggregation - Find and connect disparate digital identities to a MUR. Processes associated with identity aggregation include identity reconciliation, identity resolution, MUR, account linking and separation of duty analysis.

(c) Leaver – Stage 3. Deactivation - Deactivate or remove a MUR or identities associated with a MUR. Processes associated with deactivation include suspension, archive or deletion.

(2) VA shall ensure and adopt an agency-wide commitment to implementing and operating an ILM process. Establishment of a MUR capable of tracking and maintaining user security training status, appropriate background investigation status, PIV eligibility status, employment information status and entitlements appropriate to a role assigned to a user.

For VA users with “multiple person types” (e.g., an Employee that is also a Contractor, aka moonlighter) requires the issuance of two distinct MFA credentials that are limited to the access rights of the job being conducted at the time of use (reference mm).

(3) VA shall employ an Identity Governance Administration (IGA) tool capable of inventorying, analyzing and reporting on access and entitlements within the VA enterprise. IGA must have a virtual directory feature to aggregate identity information from multiple other directories. By integrating with authoritative sources and applications, the IGA tool can report on who has access, what they can access and why they have access. The IGA tool will be a primary mechanism to perform access reviews.

Access Reviews – Each ISO will ensure a risk assessment is conducted to determine the ideal time frame to conduct regular access reviews. The minimum time frames to conduct access reviews within each application can be found in the Information Security KS security control AC – 2.22 and 2.23 as directed by VA Handbook 6500.

c. Enterprise Identity Proofing.

(1) Identity Proofing Controls.

(a) Chain of trust provides the following benefits:

i Links the claimed identity, application for access, supporting identity source documentation and verification decisions of reviewing authorities in a traceable and auditable manner.

ii Allows identity proofing to be performed outside the direct process for issuance of a credential when that process results in a traceable verification decision.

iii Allows acceptance of identity proofing results from third parties or other parties within VA.

(b) To ensure that access to PII is granted only to the individual to whom the information pertains, to their legal representative, a delegate or to a VA employee or contractor with a need-to-know, VA requires an AAL2 authenticator or above for access to PII in accordance with VA Directive 6502 – VA Enterprise Privacy Program.

(2) In-person Identity Proofing Process and Requirements.

(a) Collection of PII for establishing an identity shall be limited to what is legally authorized and necessary. Once the information has been collected, PII must be protected (reference gg).

(b) VA shall also manage the digital identity lifecycle and credentials for VA devices, NPEs and automated technologies that are identified through network and device scans.

(c) In-person identity proofing can only be used for issuance of credentials at IAL2 and IAL3. In-person identity proofing at IAL1 does not exist because all identities are accepted.

(d) In-person proofing can be performed in a VA Medical Center, Community Based Outpatient Clinic, Regional Office or other location staffed with trained and properly equipped VA identity proofing officials. These officials must be specifically trained on the in-person identity proofing process and have access to designated administrative tools to support identity proofing.

(e) To be in-person proofed:

i The applicant must present the required forms of identification (reference bb and reference cc) to the identity proofing official. Those legally authorized to act on behalf of a Veteran must present not only their own identification, but that of the Veteran on whose behalf they are legally authorized to act as well. Additionally, all documentation authorizing the Legal Guardianship or Power of Attorney must be presented and verified if verification cannot be obtained from existing records.

ii Identity proofing officials must validate that the identity source document(s) provided are valid and verify that the photo in an

identity source document matches the applicant. See Appendix G for proofing requirements for each Assurance Level.

iii When a second identity source document is provided, the information from the second document shall be used to verify that identifying information is consistent with the primary identity source document.

iv If the second identity source document is a financial or utility account, the account number supplied by the applicant must be verified through record checks or through credit bureaus or similar databases. The identity proofing official must confirm that identifying information is consistent with the primary identity source document.

v If a record exists for the applicant, the identity proofing official should verify that the identifying information provided in the identity source documentation is consistent with information found in the applicant's record.

vi If the applicant record lists a mailing address, an effort should be made to validate the address in record against an address in an identity source document (see Appendix D for acceptable documents). If an address is not on record, the applicant may provide an address, validated against acceptable identity source documents (reference cc) if available. Additional contact information such as home phone, mobile phone or email address may also be recorded.

vii Data from the identity source document such as identity document number, date of expiration and other pertinent identity data (address, date of birth [DOB], etc.) must be captured as part of the verification process (reference dd).

viii If the applicant cannot provide U.S. issued identification and can only provide foreign (non-U.S.) issued identification, the identity proofing official must attempt to verify the individual's identity by in-person identity proofing and asking the applicant to provide acceptable, unique data points to proof their identity. An example is provided in the Veteran Health Administration (VHA) Directive 1907.09, Identity Authentication for Health Care Services Appendix A.

(3) Remote Identity Proofing Process and Requirements.

(a) Remote identity proofing can be used for issuance of credentials at IAL1 or IAL2. IAL3 does not permit remote identity proofing.

(b) Remote proofing may be performed by a remote identity proofing official (e.g., over the telephone) or through automated identity proofing services (e.g., over the internet)

(c) To access any information or make changes to the user (Veteran and beneficiary) PII by telephone, the VA employee must ask the user, or person on behalf of the user, the user's full name or preferred name once on file. The employee must ask two additional questions from Appendix D. Figure 1 in Appendix D shows an example of a general telephone identity proofing process.

(d) A remote proofing request will be initiated when an applicant accesses a subscribing application or online portal linked to the identity proofing service.

(e) To be remotely identity proofed through automated identity proofing services:

i The applicant must initiate contact with a VA service that requires remote identity proofing.

ii The remote identity proofing official or service will determine the applicant's affiliation with VA and performs an initial identification of the applicant.

iii The applicant must present information from the required forms of identification (reference cc) to the remote identity proofing official or service. Those legally authorized to act on behalf of the Veteran must present not only their own identification, but that of the Veteran on whose behalf they are legally authorized to act as well. Additionally, all documentation authorizing the Legal Guardianship or Power of Attorney must be verified. If verification cannot be obtained in existing records, the applicant must use in-person identity proofing in accordance with the requirements listed in VHA Directive 1907.09 (reference cc).

iv If a record exists for the applicant, the identity proofing service will verify that identifying information provided during identity proofing is consistent with information found in the applicant's record.

v If the applicant record lists a mailing address, an effort will be made to validate the address in the record. If an address is not on record, the applicant may provide an address. Additional contact information such as home phone, mobile phone or email address may also be validated or recorded.

vi Data from the identity source document such as identity document number, date of expiration and other pertinent identity data (address, DOB, etc.) must be recorded as part of the verification process.

vii If the identity is confirmed, the remote identity proofing official, or service, will process the service request; initiating issuance of a credential to the applicant or providing services to the customer.

d. Electronic Credential Management.

(1) Applicability - VA shall use PIV credentials as the primary means for identification and authentication for access to VA systems and facilities. PIV credential issuance and credentials accepted for use with ICAM Services will be required to comply with the following requirements. In alignment with OMB M-22-09, VA shall centrally implement support for non-PIV authenticators (if any) in VA's identity management systems, so that these authenticators are centrally managed and connected to enterprise identities (to the maximum extent possible)

(2) Electronic Credential Management Controls - The controls will:

(a) Support multiple credentials for a given identity in accordance with VA memos and policy (reference mm).

(b) Support credentials at every Assurance Level for a given identity.

(c) Have the capability to place a limitation on the number of active credentials allowed for a given Assurance Level associated with a single identity enforced through administrative controls.

(d) Support creation of pseudonym identities and authenticators to support legal investigations.

(e) Restrict the ability to create pseudonym or role-affiliated identities or alternate authenticators as a controlled administrative over-ride function.

(f) Have the capability to accept and authenticate credentials created and issued externally to VA to support cross-Government identity federation and interoperability.

(g) Have the capability to accept identity data from credentials at IAL2 and IAL3 and AAL1, AAL2 and AAL3 that have been created and issued external to VA.

(h) Have the capability for higher assurance level credentials to be used to access lower levels of assurance data or services.

(3) Credential Categories.

(a) Hardware-based Authenticator.

(b) Software-based Authenticator.

(4) Credential Assurance Levels - Credentials at each assurance level are aligned with Appendix F.

(5) Credential Lifecycle.

(a) Issuance - Electronic credentials are issued following successful identity proofing and completion of an application for an electronic credential. Credentials will be issued in accordance with appropriate assurance level requirements (see Appendix F).

(b) Usage - All credential users are notified by the credential issuance authority at the time of issuance of their responsibilities for possession of their electronic credential. Forging, falsifying or allowing misuse of an electronic credential to gain unauthorized access to VA physical or logical resources is punishable under Federal law.

(c) Expiration - Expiration dates for electronic credentials are determined by the provider of the credential and may vary from limited to unlimited durations.

(d) Revocation - Revocation deactivates electronic credentials while maintaining the existence of the electronic credential to preserve the associated audit record. Electronic credentials will be revoked when:

i The user no longer has a legitimate need for the credential;

ii The user requests revocation of the credential; or

iii VA authorities deem it necessary to revoke or disable the credential.

iv A credential will be terminated within 24 hours of notification.

(e) Modification - Modification allows for binding, updates, usage and disassociation of non-Government furnished authenticators to their digital identity.

(f) Termination – Hardware-based authenticators must be destroyed when they are expired, replaced, defective or otherwise no longer active. Software-based authenticators associated with a terminated hardware-based authenticator must be revoked in these instances. Termination should occur within 24 hours of notification.

(g) Renewal - Renewal occurs when an active and un-expired electronic credential is nearing expiration. Users may complete renewal by presenting their active credential and being issued a new credential. The previous credential will be revoked.

(h) Re-issue - Reissuance occurs when a credential is no longer active because of expiration, revocation or failure. Users may apply for credential reissuance and complete identity proofing to be issued a new credential within two weeks.

(i) Lost/Stolen.

i If a cardholder loses or has their electronic credential stolen, they must notify the PIV Card Issuing (PCI) facility, VA police, the Information System Security Officer and other parties, in accordance with VA Directive and Handbook 0735, as soon as practicable or within 4 hours.

ii The lost/stolen electronic credential shall be revoked and terminated, as appropriate, removing all access rights associated with that electronic credential. The identity record shall not be deleted because of this action.

iii Lost/stolen electronic credentials will require replacement within two weeks of reporting the loss/theft.

(6) Derived Credentials.

(a) Deriving credentials is based on the process of an individual proving to a Credential Service Provider (CSP) that they are the rightful subject of an identity record (i.e., a credential) that is bound to one or more authenticators they possess. This process is made available by a CSP that wants individuals to have an opportunity to obtain new authenticators bound to the existing, identity proofed record or credential. Minimizing the number of times the identity proofing process is repeated benefits the individual and CSP. Deriving identity is accomplished by proving possession and successful authentication of an authenticator that is already bound to the original, proofed digital identity.

(b) The definition of derived in this section does *not* imply that an authenticator is cryptographically tied to a primary authenticator,

for example deriving a key from another key. Rather, an authenticator can be derived by simply issuing based on successful authentication with an authenticator already bound to a proofed identity, rather than unnecessarily repeating an identity proofing process.

(c) There are two specific use cases for deriving identity:

i A claimant seeks to obtain a derived PIV, bound to their identity record, for use only within the limits and authorizations of having a PIV smartcard.

ii An applicant seeks to establish a credential with a CSP with which the individual does not have a pre-existing relationship. For example, an applicant wants to switch from one CSP to another or have a separate authenticator from a new CSP for other uses (e.g., basic browsing vs. financial) (reference b).

e. Electronic Signatures.

(1) Applicability - This section provides policy on using electronic signatures for ICAM Services Signature Service.

(2) A digital signature is a specific electronic signature technology that allows the recipient to prove the origin of the document and protect against forgery. It has the attribute of independent verifiability, which means it can be shared outside VA. In this case, a digital signature would be useful to prevent repudiation and allegations of tampering by strongly binding the request and its content to the requestor.

(3) Electronic (including digital) signatures are legally acceptable signatures to the same extent as a signature executed with pen on paper binding the signor’s intent to the document. Some of the same features such as notarization are also available to improve assurance and trustworthiness.

(4) Electronic Signature Service Capabilities - Electronic Signature Service Capabilities will include:

(a) Ability to apply an electronic signature for documents, emails and, other artifacts is unique to the person making the signature.

(b) An electronic capability to authorize transactions equivalent to those carried out in person.

(c) Methods the user is already familiar with for transactions requiring a signature.

(d) Transactions that capture a signature for use on multiple forms shall require all forms to be signed using a signature from the highest Assurance Level required on any of the forms.

(e) Notification to the user with the date and/or time stamping method instituted in the electronic signature service.

(5) Electronic Signature Service Requirements:

(a) Electronically signed documents shall be coupled to the MUR to establish a historical record of signing activities.

(b) The ISO shall sign an MOU with the electronic signature service owner for each application that intends to integrate the functionality.

(c) The electronic signature service shall accept credentials developed and approved for VA use by OIT.

(d) Users shall be required to authenticate prior to using the electronic signature service.

(e) An AAL2 or higher credential shall be a prerequisite to obtaining and using a key certificate pair for signing documents digitally.

(f) Electronically signed documents shall include an indication that it has been signed.

(g) Credentials used to electronically sign shall be verified at the time of signature.

(6) Electronic Signature Service Approval Process:

(a) ISOs shall submit a request for the use of the electronic signature service to the electronic signature service owner. The request shall include the system name, the transaction(s) conducted by the application that requires a signature and a list of relevant PII captured in the transaction. ISOs shall be required to complete an electronic assurance risk assessment and include the Assurance Level determination in the service request.

(b) The electronic signature service request shall be reviewed by the electronic signature service owner and an Assurance Level shall be assigned based on the results of the assurance determination process. If an AAL3 is determined and access to the application is required by Veterans and/or their representatives, the Office of General Counsel may be consulted prior to approval. Please refer Appendix F's table for more information on AAL1 and AAL2.

(c) If the electronic signature request is approved by the electronic signature service owner, an MOU shall be signed between the ISOs of the consuming application and the electronic signature service owner detailing the requirements that will be met by the ISO and the services that will be provided by the electronic signature service owner.

(7) Memorandum of Understanding:

(a) ISOs of participating VA consuming applications shall sign an MOU with the ICAM Electronic Signature Service documenting specific roles and responsibilities of the application and the electronic signature service, including the following:

i Authentication of the user at an Assurance Level determined to be commensurate with the signing transaction through a System DIRA.

ii Presentation of identity proofing data in an approved form data structure.

iii A user interface for the signing event.

(b) The electronic signature service will provide:

i Electronic signature certificates.

ii A unique identifier appropriate for the signing transaction.

iii A user-generated PIN is used to unlock the signing credential for credentials AAL3 or higher.

iv Technical consultation to include best practices and security implementation guidance during implementation and use of electronic signatures.

f. Access Management.

(1) Applicability - This section provides policy on access control processes required to authorize and revoke privileges in a timely, consistent and compliant manner.

(2) Physical Access -The policies and responsibilities set forth in VA Directive and Handbook 0730, Security and Law Enforcement and VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, apply to common and secure physical access control system policies. The ICAM PMO is the ICAM business owner and will provide support for PACS policy and

guidance coordination for various aspects of PACS functions including the activities below (installation, operations, maintenance). (*The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard,* defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level and provides an integrated, sole source of physical security countermeasures. The guidance is available at https:/www.dhs.gov/ publications.)

(a) Disseminate PACS requirements to include:

i Compliance with Office of Construction and Facilities Management (CFM) Physical Security Design Manual, Chapter 10.2, PACS installation and standards guidelines.

ii Use of OIT approved TRM access control systems.

iii Compliance with OSLE 0730 guidelines, including 0730/4 Appendix B, Physical Security Requirements and Options.

iv Compliance with VA Cybersecurity Program guidance, (VA 6500 Directive and Handbook)

(b) Electronic PACS - The following are the minimum acceptable standards and requirements for PACS.

i Access Safeguard – To prevent learning codes through keyboard observations or the use of stolen or found access cards.

ii Time Sensitive – The ability to program access by user, by shift and day.

iii Area Sensitive – The ability to program access by door and area for each user.

iv Fail-Safe – The ability to maintain access security if the system goes down (i.e., bypasskey).

v Access Record/Audit Trail – The ability to provide for periodic (at a minimum annually) or on-demand print-out of names and times/dates of individuals who access facilities. Records of access or audit trails will not be used for employee time and attendance purposes. In accordance with VA Handbook 6300.1 Records Management Procedures.

vi User Coverage – The number of individual access codes the system will accommodate.

vii PIN Codes – A PIN code or numeric password, is required as a secondary method of personal authentication to be used in addition to readers to access control systems protecting PACS high security areas, such as controlled substance storage, primary computer and communications rooms, research or clinical laboratories that store, use or develop biohazardous materials. “Scramble Pad” type PIN readers are recommended when PIN systems are installed.

viii Biometric Systems – Biometric security systems use a personal measurement, such as fingerprints, hand geometry, facial geometry or iris scans, as authentication. Biometric devices can be used in lieu of PIN systems in PACS high protected spaces, but only as a secondary form of authentication. Biometric measurements may also be used in addition to a PIN in high security applications.

ix Compliance with Federal Standards – New installations or retrofitted access control systems will be compliant with the technology described in FIPS 201, Personal Identity Verification of Federal Employees and Contractors and the document “PACS Implementation Guidance, Version 2.2 (July 30, 2004),” published by the Physical Access Interagency Interoperability Working Group of the GSA Government Smart Card Interagency Advisory Board. In accordance with those policies, systems will meet the International Organization for Standardization & International Electrotechnical Commission (ISO/IEC) 144443 a, Parts 1-4 standard for contactless (proximity) card systems, or the ISO/IEC 7816 Standard for contact-type cards. Facilities may continue to use existing PACS that operate on older technology (Magnetic Stripe, 2nd Generation bar code, etc.) as an interim measure until replacement systems are acquired and installed as part of normal equipment lifecycles.

(c) Disseminate PACS Guidance for Migration Plans for PIV compliance to include:

i VA Staff Guidelines for PIV use within PACS access control environment.

ii Require agencies to use PIV credentials (where applicable in accordance with Federal requirements) as the standard means of identification and authentication to Federal information systems, federally controlled facilities and secured areas. Requires agencies to implement PIV use in accordance with The Risk Management Process for Federal Facilities: An

Interagency Security Committee Standard (or current version) and NIST SP 800-116-1 (NIST SP 800-116) - Guidelines for the Use of PIV Credentials in Facility Access (or current version).

iii Facilitate cross-Government identity federation and interoperability by accepting the PIV credentials issued by other agencies to grant access to agency information systems, facilities and secured areas as defined in the OMB M-19-17, FICAM Policy.

iv VA Resident Guidelines for PIV (or related) use within PACS access control environments.

v Provide guidance and assistance to security and law enforcement staff.

(3) Logical Access - The policies and responsibilities outlined in VA Directive and Handbook 6500 govern logical access policies including Account and/or Password Management. All VA information technology systems shall be developed, operated and maintained to comply with the security control requirements for IA, AU and AC that are specified in VA Cybersecurity Program Guidance, (VA Directive and Handbook 6500), issued by OIT.

(a) In alignment with Executive Order 14058 customer facing digital products such as VA.gov and VA mobile applications shall enable GSA provided services Login.gov accounts for seamless integration.

(b) In alignment with OMB M-22-09, VA resources and applications shall enable phishing-resistant MFA (to the maximum extent possible) that protects VA staff from sophisticated online attacks. Users who have requested any short-term PIV exemption, more than two times in a 5-week period will refer to the VA Memo, Multiple Exemption Management Policy (reference nn).

(c) In alignment with OMB M-22-09, VA phishing-resistant MFA will be incorporated at the application layer of the Open System Interconnection (OSI) model.

(d) In alignment with OMB M-22-09, VA resources and applications shall use Attribute Based Access Control (ABAC) and Role Based Access Control (RBAC) to allow or deny access by enforcing checks based on the user’s identity, the attributes of the resources being accessed and the environment at access-time.

(e) In alignment with VHA Directive 1907.08, Health Care Information Security Policy and Requirements, users accessing Protected Health Information must complete and annually recertify, Health Insurance Portability and Accountability (HIPAA) training.

(4) ZTA (Identity Pillar) - FICAM architecture requires provisioning to be a key component of ZTA. The policy engine (PE) cannot determine if attempted connections are authorized to connect to a resource if PE has insufficient information to identify associated subjects and resources. Strong subject provision and authentication policies must be in place before moving to a more zero trust–aligned deployment. Enterprises need a clear set of subject attributes and policies that a PE can use to evaluate access requests. The OMB M-19-17 on improving identity management for the Federal Government provides guidance. The policy aims to develop "…a common vision for identity as an enabler of mission delivery, trust and safety of the Nation (reference j)." The memo calls on all Federal agencies to form an ICAM office (if one is not present) to govern efforts related to identity issuance and management. Many of these management policies should use the recommendations in NIST SP 800-63 (reference b). As ZTA heavily depends on precise identity management, any ZTA effort will need to integrate the agency's ICAM policy (reference l). An enterprise implementing a ZTA would be expected to have ICAM and asset management systems in place. This includes using phishing-resistant MFA for access to some or all enterprise resources (maximum extent possible). Additionally, to address Executive Order 14028, the ZTA data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where and how are critical for appropriately allowing or denying access to resources based on the combination of sever. In alignment with OMB M-22-09 (and using NIST SP 800-207 guidelines):

(a) Use enterprise-managed identities for VA staff to access the applications they use in their work.

(b) Employ and utilize the centralized identity management systems for VA users that can be integrated into applications and common platforms.

(c) Enforce MFA at application layer instead of the network layer.

(d) Employ phishing-resistant MFA for VA staff, partners and contractors.

(e) Provide phishing-resistant MFA as an option for external users/public users.

(f) Password policies must not require the use of special characters or regular rotation (consistent with practices outlined in NIST SP 800-63B).

(g) Employ authorization such that the access to the resource considers at least one device level signal alongside identity information about the authenticated user.

(h) Employ phishing-resistant authenticators that do not yet support PIV or Derived PIV credentials (such as FIDO2 and Web Authentication-based authenticators).

(5) SSO - The policies and responsibilities set forth in VA Directive 6500, VA Cybersecurity Program and VA Handbook 6500 regarding identification and authentication apply to SSO.

(6) Provisioning:

(a) Provisioning must be conducted by authorized personnel in accordance with the processes defined within Information System Standard Operating Procedures.

(b) Provisioning may include automatic mechanisms.

(c) User accounts must undergo periodic reviews in accordance with designated control frequency. Reference the Security Controls Explorer for the Organizational-Defined Parameter. The direct Supervisor (employees and other user types) or the VA employee(s) designated by VA Handbook 6500 and VA Handbook 6500.6 (contractors) is responsible for reviewing the accounts.

(d) User access must be revoked when it is no longer required and/or appropriate to maintain.

(e) All contractors that require access to VA facilities or systems must comply with HSPD-12 and FIPS 201.

(7) Delegated Authority:

(a) Delegators may specify the time duration for delegate access to their system’s information via a unique account for the delegate. If a duration is not specified, the duration will be set to one year.

(b) Delegators shall designate all or specific types of information (e.g., secure messaging, Labs, Personal Health Information, Medical Information, Prescription Refills/Medications and Account Activity Logging) to be accessible to those delegated access rights.

(c) Delegators shall have access to a log of all account access for a minimum of 7 years; including records of who accessed the account, any actions taken during access, such as edits or additions to information and the date accessed (following VA Handbook 6300.1 Records Management Procedures).

(d) Delegators shall have access to a list of each delegate's access rights.

(e) Delegators shall be informed, in terms that are understandable and in common language, of the implications of granting a delegate access. This may include but is not limited to privacy issues and financial issues (e.g., medication refill, lab results).

(f) Delegators must re-affirm their delegation selections annually.

(g) Delegators shall be shown identity elements (e.g., first name, last name, DOB, address, phone number) belonging to the delegate to confirm the identity of the delegate prior to granting access. Exposure to PII for the Delegator or Delegate shall be in accordance with VA Directive 6502, VA Enterprise Privacy Program.

(h) Delegators shall be required to review and confirm the access being granted prior to the delegate gaining access.

(i) Delegates who have been granted the ability to grant and revoke rights by the Delegator, may do so to persons of their choosing in accordance with the VA policies.

(j) Delegates must have access to the system for which they are delegated authority and must have received a credential appropriate to the Assurance Level required for access to that system.

(k) Delegates shall be able to view the specific access rights granted to them.

(l) Delegate status may be changed or deactivated at any time by the Delegator or by VA in accordance with the VA policies.

(m) Delegates may decline their access rights at any time. The Delegator shall be notified when this action occurs.

(n) All delegators and delegates shall have access to educational materials on how to use the system or application and how to safeguard the privacy of information prior to being granted access.

(o) Systems/Applications shall allow delegators to grant access to several delegates as determined by that system/application requirements. Limitations on this number shall be the responsibility of the system/application capability to assign.

(p) If the Delegator account is deactivated for any reason the delegate shall receive a notification that the Delegator's account has been deactivated and the date the account was deactivated. The delegate will no longer have access to the deactivated account.

(q) If a delegate has been provided access to multiple delegator accounts, the Delegate shall only be able to access one delegator's account at a time.

(r) The delegate's actions shall be logged in an auditable manner and distinguishable from those of the Delegator.

(8) AC - Security controls applicable to the access control to VA information systems/applications by organizational/non-organizational users of ICAM Services as required in VA Handbook 6500.

(9) AU - Security controls applicable to the audit and accountability of audit records on VA information systems/applications relating to organizational/non-organizational users of ICAM Services as required in VA Handbook 6500.

(10) IA – Security controls applicable to the identification and authentication to VA information systems/applications by organizational/non-organizational users of ICAM Services as required in VA Handbook 6500.

(11) Personnel Security (PS) - Security controls applicable to the personnel security of organizational/non-organizational users of ICAM Services as required in VA Handbook 6500.

(12) RoB - Security controls requiring annual security and privacy training and acceptance of the VA RoB before access to VA information systems/applications by organizational/non-organizational users of ICAM Services is granted as required in VA Handbook 6500.

5. REFERENCES.

a. OMB M-11-11, Continued Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors; February 2011.

b. NIST SP 800-63-3, Digital Identity Guidelines; updated October 2023.

c. The FICAM Architecture and Implementation Guidance and the FICAM Playbooks, developed by the Federal CIO Council; June 2023.

d. Requirements for Accepting Externally-Issued Identity Credentials, OMB Memo; October 2011.

e. VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program VA Directive 6500, VA Cybersecurity Program.

f. VA Directive and Handbook 0710, Personnel Security and Suitability Program; June 2010 and May 2016.

g. 0730/4 Appendix B, Security and Law Enforcement; March 2013.

h. CFM Physical Security Design Manual for VA Life-Safety Protected Facilities U.S. Department of Veterans Affairs; January 2024.

i. NIST SP 800-116-1, Guidelines for the Use of PIV Credentials in Facility Access; June 2018.

j. OMB M-19-17, Enabling Mission Delivery Through Improved Identity, Credential and Access Management; May 2019.

k. OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles; January 2022.

l. NIST SP 800-207, Zero Trust Architecture; August 2020.

m. The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency; updated 2021.

n. 15 U.S.C. §§ 7001-7006, Electronic Records and Signatures in Global and National Commerce Act (“E-SIGN”); June 2000.

o. 44 U.S.C. §§ 3551-3558, Federal Information Security Modernization Act (FISMA) of 2014.

p. P.L.105-277, Div. C, Title XVII, codified at 44 U.S.C. § 3504 note, The Government Paperwork Elimination Act (GPEA); October 1998.

q. 45 C.F.R. Parts 160 and subparts A and C of Part 164, Health Insurance Portability and Accountability Act (HIPAA), Security Rule; August 2009.

r. Committee on National Security Systems (CNSS) Instruction No. 4009; April 2010.

s. FIPS 199, Standards for Security Categorization of Federal Information and

Information Systems; February 2004.

t. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems; March 2006.

u. FIPS 201-3, Personal Identity Verification of Federal Employees and Contractors; January 2022

v. NIST SP 800-30-1, Guide for Conducting Risk Assessments; September 2012.

w. NIST SP 800-37-2, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach; December 2018.

x. NIST SP 800-53-5, Security and Privacy Controls for Information Systems and Organizations; September 2020.

y. OMB Memorandum 00-15, OMB Guidance on Implementing the Electronic Signatures; September 2000.

z. VA Directive 6500, VA Cybersecurity Program; February 2021.

aa. VA Directive and Handbook 0730; Security and Law Enforcement, December 2012 and August 2000.

bb. VA Directive and Handbook 0735, Homeland Security Presidential Directive 12 Program; October 2015 and March 2014.

cc. VHA Directive 1907.09, Identity Authentication for Health Care Services; June 2019.

dd. CFM Physical Security Design Manual, Chapter 10.2 PACS installation and standards guidelines 0730/4 Appendix B, Physical Security Requirements and Options; January 2024.

ee. M-274, Handbook for Employers USCIS; July 2023.

ff. VA Directive 6502, VA Enterprise Privacy Program; May 2008.

gg. Presidential Executive Order 14028, Improving the Nation’s Cybersecurity; May 2021.

hh. Presidential Executive Order 13988, Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation; January 2021.

ii. OMB M-22-16, Administration Cybersecurity Priorities for the FY 2024 Budget; July 2022.

jj. The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard; November 2016.

kk. Identity Lifecycle Management Playbook, Federal Chief Information Security Officer Council IAM Subcommittee version 1.2; December 2022.

ll. VA Memo, PIV Logical Access Policy Clarification (VIEWS 00155984); July 2019.

mm. VA Memo, Requirements for Two Factor Authentication for VA Network Access for Individuals with Dual Identities (VAIQ 7735690); December 2016.

nn. VA Memo, Multiple Exemption Management Policy (VIEWS 03979222); January 2021.

oo. VA Memo, Responsibilities of Business and System Owners (VIEWS 04250381); January 2021.

pp. VHA Directive 1907.08, Health Care Information Security Policy and Requirements, 105 - Health Informatics; April 2019.

qq. NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing Requirements; June 2017.

rr. NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management; June 2017.

ss. NIST SP 800-63C, Digital Identity Guidelines: Federation and Assertions; June 2017.

6. DEFINITIONS.

a. **Affiliate:** Individuals who require logical access to VA information systems and/or physical access to VA facilities to perform their jobs and who do not fall under the category of Federal employee or contractor. Examples include but are not limited to: Veteran Service Organizations (VSO) representatives, Joint Commission Reviewers, childcare staff, credit union staff, Union Officials and union support staff. SOURCE: VA Directive 0735

b. **Application:** A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system. SOURCE: FIPS 201

c. **Assurance:** The degree of confidence 1) in the vetting process used to establish the identity of an individual to whom a credential is issued and 2) that the individual who uses the credential is the individual to whom the credential was issued. SOURCE: NIST SP 800-63-3

d. **Authentication:** Verifying the identity of a user, process or device, often as a prerequisite to allowing access to a system's resources. SOURCE: NIST SP 800-63-3

e. **Authenticator:** Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous editions of SP 800-63, this was referred to as a token. SOURCE: NIST SP 800-63-3

f. **Authorization:** Access privileges granted to a user, program or process or the act of granting those privileges. SOURCE: CNSS Instruction No. 4009

g. **Business Owner:** Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance and/or final disposition of an information system. SOURCE: NIST SP 800-216

h. **Challenge Questions:** Questions used to authenticate an identity against VA-known data (i.e., full name, address, military service dates, home address, etc.) when no acceptable primary or secondary identification documents are available, or when requests are received by telephone. SOURCE: CNSSI 4009-2015

i. **Claimant:** A subject whose identity is to be verified using one or more authentication protocols. SOURCE: NIST SP 800-63-3

j. **Claimed Identity:** Any identity that has not been vetted through the identity proofing process. SOURCE: NIST SP 800-63-3

k. **Credential:** Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. SOURCE: FIPS 201-3

l. **Delegated Authority:** For the purposes of VA Handbook 6510, Identity and Access Management, a Delegator grants a Delegate access as needed to act on the Delegator's behalf. The Delegator and Delegate do not share credentials for the purpose of accessing any necessary services.

m. **Data Integrity:** The property that data has not been altered by an unauthorized entity. SOURCE: NIST SP 800-63-3

n. **Digital Identity Risk Assessment:** The process to determine system IAL, AAL and if applicable, FAL. This process examines system transactions, potential for misuse of transaction information, overall risk to individuals, VA operations and assets and potential impacts to involved organizations to determine the individual assurance levels for each VA system. SOURCE: NIST SP 800-63-3

o. **Electronic Credential:** An object that authoritatively binds an identity to an authenticator possessed and controlled by a person. SOURCE: CNSSI 4009-2015

p. **Electronic Signature:** The process of applying any mark in electronic form with the intent to sign a data object. SOURCE: CNSS Instruction 4009

q. **Hardware-Based Authenticator:** A dedicated physical device (such as a token, PIV card, etc.) held by an authorized user, in addition to a basic password, to grant access to computer resources. SOURCE: NIST SP 800-63B

r. **Identification:** The process of discovering the true identity of a person defined by known or recognized characteristics such as birthplace, age and residence of a person. SOURCE: VA Directive 0735

s. **Identity:** A unique representation of a subject (person, device, NPE, or automated technology) engaged with at least one Federal subject or protected resource and may be referred to in two contexts:

(1) Federal enterprise identity – An employee, a contractor, an enterprise user, a device or technology that is managed by a federal agency.

(2) Public identity – A subject that a federal agency interacts with but does not directly manage. SOURCE: OMB M-19-17

t. **Identity Lifecycle Management** - a core identity service to protect federal data. As with our human identities, our digital identities follow a similar

process from creation to retirement. Users complete vetting/identity proofing, have accounts created on multiple systems, get promoted and eventually leave an organization. Identity Lifecycle Management encompasses the activities of creating, identity proofing/vetting, provisioning, aggregating, maintaining and deactivating digital identities on an agency's enterprise ICAM system. SOURCE: Identity Lifecycle Management Playbook

u. **Identity Proofing:** The process of analyzing identity source documents provided by an applicant to determine if they are authentic, to contact sources of the documents to verify that they were issued to the applicant and to perform background checks of the applicant to determine if the claim of identity is correct. SOURCE: VA Directive 0735

v. **Identity Proofing Official:** A VA employee or contractor charged with the creation of PIV card credentials. SOURCE: VA Handbook 0735

w. **In-Person Proofing:** Identity proofing that occurs in the presence of a VA appointed representative. SOURCE: VA Handbook 0735.

x. **Information System Owner:** Official responsible for the overall procurement, development, integration, modification or operation and maintenance of an information system. SOURCE: NIST SP 800-137

y. **Intent:** The understanding and acceptance of the purpose of the electronic signature that is non-reputable. SOURCE: NIST SP 800-63-3

z. **Integrity:** Guarding against improper information, modification or destruction and include ensuring information non-repudiation and authenticity. SOURCE: 44 USC Sec 3542

aa. **Life-Safety Protected Facilities:** VA facilities which are required to protect the life safety of the patients, staff and visitors in case of an emergency; although indispensable to the mission of VA, are not required to remain operational in a natural or manmade extreme event or a national emergency. SOURCE: Physical Security Design Manual for VA Life-Safety Protected Facilities

bb. **Multifactor Authentication:** An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. SOURCE: NIST Computer Security Resource Center Glossary

cc. **Non-Person Entity**: An entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications and information artifacts. SOURCE: NIST SP 800-207

dd. **Non-Repudiation:** Protection against an individual falsely denying having

performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information and receiving a message. SOURCE: NIST SP 800-53-5

ee. **Physical Access Control System:** PACS are information systems and they include, for example, servers, databases, workstations and network appliances in either shared or isolated networks. NIST 800-116-l (or any successive version) contains guidance on the use of PIV credentials in physical access control system (PACS).

ff. **Provisioning:** Creating user access accounts and assigning privileges or entitlements within the scope of a defined process or interaction; provide users with access rights to applications and other resources that may be available in an environment, may include the creation, modification, deletion, suspension or restoration of a defined set of privileges. SOURCE: FICAM Roadmap

gg. **Remote Proofing:** Identity proofing that occurs outside the physical presence of a VA appointed representative. SOURCE: NIST 800-63A

hh. **Risk Assessment:** The process of identifying, estimating and prioritizing risks to organizational operations (including mission, functions, image or reputation), organizational assets, individuals and other organizations, resulting from the operation of a system. It is part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. SOURCE: NIST SP 800-63-3

ii. **Software-based Authenticator:** authentication tokens that are not physically tangible but exist as software on common devices (for example computers or phones). SOURCE: NIST SP 800-63B

jj. **Special Purpose Systems:** At VA, systems that provide a business function that is not specifically an IT function but are connected to the VA network and require the cybersecurity of the systems to be managed. These systems can include energy management systems, HVAC, facility fire alarm systems, building/facility access and security camera systems.

kk. **Transaction:** The transmission of information between two parties relating to the conduct of business, commercial or governmental activities. SOURCE: NIST 800-63-3

ll. **Verify:** Confirmation by examination and provision of identity source documentation that a claimed identity is a valid identity. SOURCE: FIPS 201-3 Under Identity Verification

mm. **Vetting:** Process of examination and evaluation, including background

check activities; results in establishing verified credentials and attributes. SOURCE: FICAM Roadmap

nn. **Zero Trust:** The term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. SOURCE: NIST SP 800-207

oo. **Zero Trust Architecture:** The implementation of zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). SOURCE: NIST SP 800-207

(1) APPENDIX A – ACRONYMS.

Acronym	Definition
CFM	Office of Construction and Facilities Management
CIO	Chief Information Officer
CO	Contracting Officer
CRR	Office of Compliance, Risk and Remediation
CSP	Credential Service Provider
DIRA	Digital Identity Risk Assessment
DOB	Date of Birth
eMASS	Enterprise Mission Assurance Support Service
FICAM	Federal Identity, Credential and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GSA	General Services Administration
HCIdM	Health Care Identity Management
HIPAA	Health Insurance Portability and Accountability Act
HRA	Human Resources and Administration
HSPD-12	Homeland Security Presidential Directive – 12
ICAM	Identity, Credential and Access Management
IGA	Identity Governance Administration
ILM	Identity Lifecycle Management
ISO	Information System Owner
ISSO	Information System Security Officer
MFA	Multifactor Authentication
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OSP	Office of Operations, Security and Preparedness

PACS	Physical Access Control System
PE	Policy Engine
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKI	Public Key Infrastructure
PMO	Program Management Office
RP	Relying Party
SP	Special Publication
SPS	Special Purpose System
SSN	Social Security Number
SSO	Single Sign-On
TRM	Technical Reference Model
VA	Veterans Affairs
ZT	Zero Trust
ZTA	Zero Trust Architecture

(2) APPENDIX B – VA TERMS & DEFINITIONS.

Term Name	Term Definition
Identity Proofing Official	The official responsible for verifying the claimed identity of an applicant by authenticating the identity source documents provided by the applicant (Source: Industry Standard).
Identity Proofing Applicant	An individual who is seeking verification of their claimed identity by authenticating the identity source documents provided by the applicant (Source: VA Handbook 0735).
Information System Security Officer	An individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program (Source: VA Handbook 6500).
Local Chief of VA Police	An individual charged with leading a local VA facility's physical security in the case of an incident reported with suspected criminal intent; this person is the contact for VA ISSO and/or Police Officer (Source: VA Handbook 0730).
System DIRA Authority	An individual granted the official authority to ensure digital identity risk assessments are conducted properly to validate proper AAL, IAL and FAL (if applicable) for credentials and applications (Source: Industry Standard).
Information System Owner	An individual responsible for the overall procurement, development, integration, modification or operation and maintenance of an information system (Source: VA Handbook 6500).
Facility Physical Security Specialist/Assistant Administrators	An individual responsible for upholding and securing the four pillars of physical security related to electronic systems – physical access control systems (card readers), surveillance cameras, duress systems (to allow facility staff to contact security as needed) and assisting with monitoring the facility (Source: VA Handbook 0730).
Electronic Signature Services Credential User	An individual whose signature has been verified as an official electronic signature (Source: Industry Standard).
Credential User	A user of a system that verifies an identity with an object or data structure that authoritatively binds an identity to a token processed and controlled by a subscriber (Source: Industry Standard).
Delegate	An individual who has been assigned access to permit the performance of actions on a specific object or group of objects via their personal authenticators (Source: Industry Standard).
Delegator	An individual with the ability to assign limited authority to a user (delegate) permitting the performance of actions on a specific object or group of objects. The delegator grants access to the user via means other than their personal authenticators (Source: Industry Standard).

(3) APPENDIX C – TELEPHONE IDENTITY PROOFING PROCESS.

1. Overview.

This SOP documents the processes and requirements for the verification of identities through telephone interactions with Veterans, their representatives and all other customers. VA staff must verify the identity of any individual requesting changes to, or release of, any PII. To access any information or make changes to Veteran PII by telephone, the VA staff must ask the Veteran, or person on behalf of the Veteran, the Veteran's full name or preferred name once provided. The staff must ask two additional questions from Table 1: Additional Questions for Verification. Figure 1: Telephone Identity Proofing Process Example shows an example of a general telephone process. (Reference Document: *Department of Veterans Affairs Telephone Identity Proofing Standard Operating Procedure, dated March 14, 2012*).

2. Standard Operating Procedures.

a. A customer places a call to a VA service.

b. VA staff answers the phone and performs an initial identification of the customer through a full name inquiry or preferred name once provided.

(1) If a preferred name is on file, VA Staff will ensure using the customer's preferred name for identity proofing purposes.

c. The VA staff will inform the customer that they should be in a safe environment to limit eavesdropping.

d. VA staff requests a description of the issue the customer is reporting.

e. VA staff transfers the call, as necessary, to the appropriate support group.

f. VA staff requests verification of the customer's full name or preferred name once on file.

g. VA staff asks the customer two additional questions based on the questions found in Table 1, Additional Questions for Verification.

h. If the identity is confirmed, VA staff assists the customer in resolving the issue.

i. If the identity is not confirmed, the call may be terminated, or other appropriate actions taken, as determined by call center policies.

(4) APPENDIX D – ADDRESS CONFIRMATION DOCUMENTS CRITERIA.

1. Additional Questions for Verification:

    a. DOB, including year;

    b. Branch of service and service dates;

    c. Full Social Security number (SSN) NOTE: Although VA has indicated it will not call a Veteran and ask for an SSN, it is allowable to ask for an SSN when the Veteran (or someone on the Veteran's behalf) initiates the call;

    d. Home address (including zip code);

    e. Military Service number;

    f. Mother's maiden name;

    g. Next of kin;

    h. VA Claim Number/Unique Identifier;

    i. Current account number for direct deposit;

    j. Current benefit check amount;

    k. Spouse's name; and

    l. Place of birth, city and state.

2. Acceptable Documents to Verify Mailing Addresses. The following documents are designated as acceptable for identifying the current mailing address. The applicant's name must be the addressee on the document and the document must be dated within the last 30 days.

    a. Phone bill from local phone service provider;

    b. Electric bill from a local electrical service provider;

    c. Fossil fuel (oil, gas, propane) bill from a local service provider;

    d. Credit card statement;

    e. Checking or savings account statement;

    f. Local personal property tax bill;

    g. Mortgage or rent payment voucher; or

h. Veterans Benefits Administration (VBA) corporate data reflecting the correct mailing address as verified by the applicant.

Figure 1

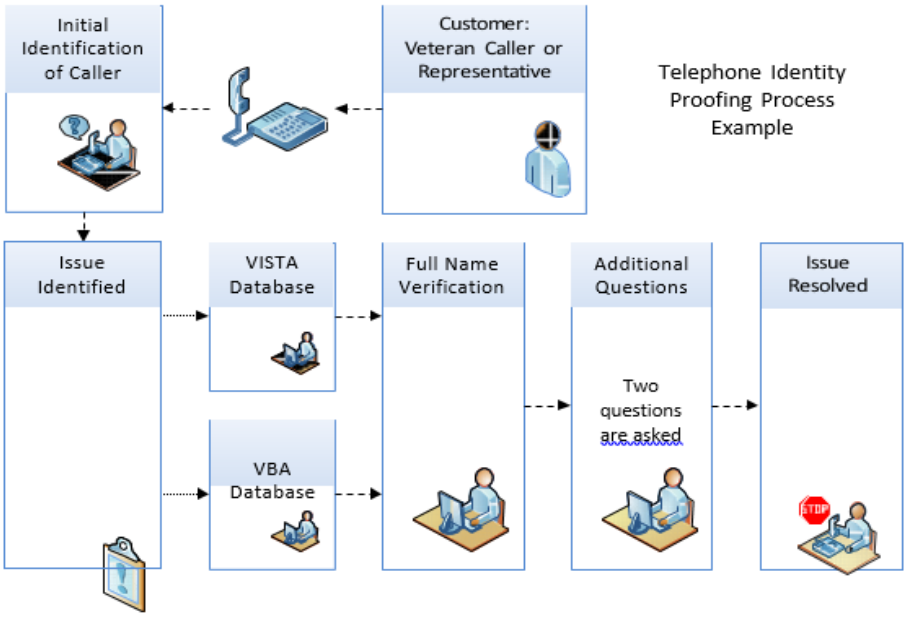

Figure 1 - Telephone Identity Proofing Process Example

(5) APPENDIX E – ASSURANCE LEVEL GUIDE.

Assurance Level	Requirements
IAL1	There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a CSP asserts to an RP).
IAL2	Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
IAL3	Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
AAL1	AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
AAL2	AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.
AAL3	AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication

	protocol(s). Approved cryptographic techniques are required.
FAL1	Allows for the subscriber to enable the RP to receive a bearer assertion. The assertion is signed by the IdP using approved cryptography.
FAL2	Adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.
FAL3	Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the Identity Provider (IdP) and encrypted to the RP using approved cryptography.

(6) APPENDIX F – AUTHENTICATOR ASSURANCE LEVEL EXAMPLES.

1. AAL1 authentication SHALL occur by the use of any of the following authenticator types:

    a. Memorized Secret;

    b. Look-Up Secret;

    c. Out-of-Band Devices;

    d. Single-Factor One-Time Password (OTP) Device;

    e. Multi-Factor OTP Device;

    f. Single-Factor Cryptographic Software;

    g. Single-Factor Cryptographic Device;

    h. Multi-Factor Cryptographic Software; or

    i. Multi-Factor Cryptographic Device.

2. AAL2 - When a multi-factor authenticator is used, any of the following MAY be used:

    a. Multi-Factor OTP Device;

    b. Multi-Factor Cryptographic Software;

    c. Multi-Factor Cryptographic Device; or

    d. When a combination of two single-factor authenticators is used, it SHALL include a Memorized Secret authenticator and one possession-based (i.e., “something you have”) authenticator from the following list:

        (1) Look-Up Secret;

        (2) Out-of-Band Device;

        (3) Single-Factor OTP Device;

        (4) Single-Factor Cryptographic Software; or

        (5) Single-Factor Cryptographic Device.

3. AAL3 authentication SHALL occur by the use of one of a combination of authenticators. Possible combinations are:

    a. Multi-Factor Cryptographic Device;

b. Single-Factor Cryptographic Device used in conjunction with Memorized Secret;

c. Multi-Factor OTP device (software or hardware) used in conjunction with a Single-Factor Cryptographic Device;

d. Multi-Factor OTP Device (hardware only) used in conjunction with a Single-Factor Cryptographic Software;

e. Single-Factor OTP Device (hardware only) used in conjunction with a Multi-Factor Cryptographic Software Authenticator; or

f. Single-Factor OTP Device (hardware only) used in conjunction with a Single-Factor Cryptographic Software Authenticator and a Memorized Secret.

(7) APPENDIX G – IDENTITY PROOFING LEVELS

In-Person

IAL2	
Evidence Collection	The CSP SHALL collect the following from the applicant: (1) One piece of SUPERIOR or STRONG evidence **if** the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; **OR** (2) Two pieces of STRONG evidence; **OR** (3) One piece of STRONG evidence plus two pieces of FAIR evidence Identity Evidence Quality Requirements can be found in NIST SP 800-63a Section 5.2.1.
Evidence Validation	The CSP SHALL validate each piece of evidence with a process that can achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG. Validating Identity Evidence can be found in NIST SP 800-63a Section 5.2.2.
Evidence Verification	The CSP SHALL verify identity evidence as follows: 1. At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG. 2. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification. Identity Verification Methods can be found in NIST SP 800-63a Section 5.3.1.
IAL3	
Evidence	The CSP SHALL collect the following from the applicant:

Collection	1. Two pieces of SUPERIOR evidence; **OR** 2. One piece of SUPERIOR evidence and one piece of STRONG evidence **if** the issuing source of the STRONG evidence, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; **OR** 3. Two pieces of STRONG evidence plus one piece of FAIR evidence. Identity Evidence Quality Requirements can be found in NIST SP 800-63a Section 5.2.1.
Evidence Validation	The CSP SHALL validate identity evidence as follows: Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG. Validating Identity Evidence can be found in NIST SP 800-63a Section 5.2.2.
Evidence Verification	The CSP SHALL verify identity evidence as follows: 1. At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of SUPERIOR. 2. KBV SHALL NOT be used for in-person (physical or supervised remote) identity verification. Identity Verification Methods can be found in NIST SP 800-63a Section 5.3.1.

(8) APPENDIX H – RISK METHODOLOGY.

Impact Categories (IC)	**IAL1**	**IAL 2**	**IAL 3**
IC #1 Damage to Reputation	Low 1-15	Moderate 16-31 or 32-48	High 49-81
IC #2 Financial Loss / Liability	Low 1-15	Moderate 16-31 or 32-48	High 49-81
IC #3 Harm to Agency Programs or Public Interest	N/A	Low 1-15 or 16-48	High 49-81
IC #4 Unauthorized Release of Sensitive Information	N/A	Low 1-15 or 16-48	High 49-81
IC #5 Personal Safety	N/A	Low 1-15	Moderate or High 16-48 or 49-81
IC #6 Civil / Criminal Violations	N/A	Low or Moderate 1-15 or 16-48	High 49-81
Probability Level	**Probability Definition**		
Low **(10%=1, 20%=2, 30%=3)**	**The threat-source lacks motivation or capability, or business controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.**		
Moderate **(40%=4, 50%=5, 60%=6)**	**The threat-source is motivated and capable, but business controls are in place that may impede successful exercise of the vulnerability.**		
High **(70%=7, 80%=8, 90%=9)**	**The threat-source is highly motivated and sufficiently capable and business controls to prevent the vulnerability from being exercised are ineffective.**		

(9) APPENDIX I – DIGITAL IDENTITY ACCEPTANCE STATEMENT.

1. In accordance with NIST SP 800-63 the following are the instructions and template to be used in the creation of a Digital Identity Acceptance Statement.

2. Agencies SHOULD include this information in existing artifacts required to achieve a security authorization and accreditation (SA&A). The statement SHALL include, at a minimum:

   a. Assessed xAL;

   b. Implemented xAL;

   c. Rationale, if implemented xAL differs from assessed xAL;

   d. Comparability demonstration of compensating controls when the complete set of applicable 800-63 requirements are not implemented; and

   e. If not accepting federated identities, rationale.

(10) APPENDIX J – I-9 APPROVED IDENTITY SOURCE DOCUMENTS.

LIST A Documents that Establish Both Identity and Employment Authorization	OR	LIST B Documents that Establish Identity	AND	LIST C Documents that Establish Employment Authorization
1. U.S. Passport or U.S. Passport Card		**1.** Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address		**1.** A Social Security Account Number card, unless the card includes one of the following restrictions: **(1)** NOT VALID FOR EMPLOYMENT **(2)** VALID FOR WORK ONLY WITH INS AUTHORIZATION **(3)** VALID FOR WORK ONLY WITH DHS AUTHORIZATION
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)		**2.** ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address		**2.** Certification of report of birth issued by the Department of State (Forms DS-1350, FS-545, FS-240)
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa		**3.** School ID card with a photograph		**3.** Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
4. Employment Authorization Document that contains a photograph (Form I-766)		**4.** Voter's registration card		**4.** Native American tribal document
5. For an individual temporarily authorized to work for a specific employer because of his or her status or parole: **a.** Foreign passport; and **b.** Form I-94 or Form I-94A that has the following: **(1)** The same name as the passport; and **(2)** An endorsement of the individual's status or parole as long as that period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form.		**5.** U.S. Military card or draft record		**5.** U.S. Citizen ID Card (Form I-197)
		6. Military dependent's ID card		**6.** Identification Card for Use of Resident Citizen in the United States (Form I-179)
		7. U.S. Coast Guard Merchant Mariner Card		**7.** Employment authorization document issued by the Department of Homeland Security For examples, see **Section 7** and **Section 13** of the M-274 on **uscis.gov/i-9-central**. The Form I-766, Employment Authorization Document, is a List A, **Item Number 4.** document, not a List C document.
		8. Native American tribal document		
		9. Driver's license issued by a Canadian government authority		
		For persons under age 18 who are unable to present a document listed above:		
		10. School record or report card		
		11. Clinic, doctor, or hospital record		
		12. Day-care or nursery school record		
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI				