Department of Veteran Affairs
Washington, DC 20420

VA HANDBOOK 6510
Transmittal Sheet
January 15, 2016

VA IDENTITY AND ACCESS MANAGEMENT

1. REASON FOR ISSUE: This Handbook defines roles, responsibilities, and procedures to implement VA Directive 6510, *VA Identity and Access Management,* for the Department of Veterans Affairs (VA).

2. SUMMARY OF CONTENT/MAJOR CHANGES: This Handbook sets forth roles, responsibilities, and procedures for VA Identity and Access Management.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (OIT) (005), Office of Information Security (005R), Office of Cyber Security (005R2) is responsible for the contents of this Handbook.

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

5. RESCISSIONS: None.

CERTIFIED BY:

/s/
LaVerne H. Council
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS

/s/
LaVerne H. Council
Assistant Secretary for
Information and Technology

Distribution: Electronic Only

This page left intentionally blank.

VA IDENTITY AND ACCESS MANAGEMENT

Contents

This page left intentionally blank.

1. INTRODUCTION

a. Background

(1) The Department of Veterans Affairs (VA) has implemented an Identity and Access Management (IAM) Program that provides access to VA information, resources, and services to improve timeliness and promote ease of access for all VA users. VA has established the IAM Business Program Management Office to manage the business of aligning IAM Services to federal mandates and guidance. VA accepts and institutes the policies and guidelines in accordance with the following documents.

(a) The *E-Authentication Guidance for Federal Agencies (M-04-04) memorandum*, issued by the Office of Management and Budget (OMB) on December 16, 2003, requires agencies to (i) review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance (LOA), and (ii) establishes and describes four levels of identity assurance for electronic transactions requiring authentication.

(b) The *Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors* memorandum, issued by OMB on February 3, 2011, provides an outline plan of action for agencies that will expedite the Executive Branch’s full use of the personal identification verification (PIV) credentials for access to federal facilities and information systems.

(c) The *Electronic Authentication Guideline Special Publication (SP) 800-63-2, December 2011*, issued by the National Institute of Standards and Technology (NIST), provides recommended technical guidelines to agencies for the implementation of electronic authentication.

(d) The *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, developed by the Federal Chief Information Office (CIO) Council, is provided as a resource for agency implementers of identity, credential, and access management programs.

(e) The *Requirements for Accepting Externally-Issued Identity Credentials* memorandum, issued by OMB on October 6, 2011, require agencies to follow OMB policy and accept only externally issued credentials that are issued in accordance with NIST guidelines and Federal CIO Council processes.

(f) The VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, provides the risk-based process for selecting system security controls, including the operational requirements for VA information technology systems per VA Directive 6500, Managing Information Security Risk: VA Information Security Program.

(g) The VA Directive and Handbook 0710, *Personnel Security and Suitability Program*, describes the purpose, responsibilities, requirements, and procedures of VA’s Personnel Security and Suitability Program, applicable to VA applicants, appointees, employees, contractors, and affiliates who have access to departmental operations, facilities, information, or information technology systems.

b. Purpose. This Handbook defines roles, responsibilities, and procedures for the VA-wide IAM Program.

c. Scope. This Handbook addresses the roles, responsibilities, and procedures associated with administration, governance, and use of the following IAM Services:

(1) Electronic Authentication Risk Assessment;

(2) Enterprise Identity Proofing;

(3) Electronic Credential Management;

(4) Electronic Signatures; and

(5) Access Management

d. Applicability

(1) This Handbook applies to all VA administrations, staff offices, all VA staff who support IAM functionality, Veterans, affiliates, and any users who require logical access to VA information systems including resources both internally and externally managed and offered through VA.

(2) The identity proofing process for 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, *Homeland Security Presidential Directive 12 (HSPD-12) Program*.

(3) The security and privacy controls in VA Handbook 6500, represents VA’s information technology (IT) security requirements as it applies to VA information systems/applications utilizing IAM Services. The VA National Rules of Behavior (ROB) in Appendix D of VA Handbook 6500, provides the specific responsibilities and expected behavior for organizational/non-organizational users of IAM Services.

(4) Federal Information Processing Standards (FIPS-201) *Personal Identity Verification* requirements are addressed in VA Handbook 0710 and require that at a minimum National Agency Check with Inquiries (NACI) be initiated prior to the issuance of a Personal Identity Verification (PIV) compliant card.

e. The Office of Information and Technology (OIT) will develop and disseminate additional directives, handbooks, memoranda, notices, and best practices to implement these procedures or to institute additional requirements for enterprise identity, credential, and access management activities.

2. ROLES AND RESPONSIBILITIES

a. Identity Proofing Officials are responsible for providing vetting services for applicants requesting identity proofing including:

(1) Reviewing identity source documentation;

(2) Comparing, as necessary, identity source documentation to ensure data matches;

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

(4) Recording identity source documentation data; and

(5) Notifying the local Information Security Officer (ISO) when there is reasonable suspicion that fraudulent identity documentation is presented by an applicant as proof of identity.

b. Applicants for Identity Proofing are any users requesting a credential for VA IAM Services. These individuals are responsible for:

(1) Initiating request for access to information;

(2) Providing demographic data; and

(3) Providing identity source documentation.

c. Information Security Officers (ISOs) are responsible for ensuring that the appropriate operational security posture is maintained for an information system or program**,** <u>including</u>:

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

(2) Assisting information system owner with performing the electronic authentication risk assessment process;

(3) Reviewing the electronic authentication risk assessment and verifying the assurance determinations for each system/application role transactions;

(4) Conducting responsibilities of the Electronic Authentication Risk Assessment Authority or ensuring the responsibilities are carried out if assigned to another party; and

(5) Ensuring Information Systems comply with all security requirements in VA Handbook 6500.

d. Local Privacy Officer is responsible for coordinating with Regional Counsel, Office of Inspector General (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. Electronic Authentication Risk Assessment Authority is responsible for providing official authority to ensure risk assessments to determine proper LOA credentials for applications are conducted, including:

(1) Receiving Electronic Authentication Risk Self-Assessment(s) from Information System Owner (or designated assessor);

(2) Evaluating assurance levels determination from self-assessment;

(3) Approving or Rejecting assurance level determinations; and

(4) Approving assurance level determinations that have been acknowledged by the information system owner.

f. Information System Owner (i.e., Project Manager, Business Project Manager) is responsible for:

(1) Submitting required information to request use of electronic signature services;

(2) Signing and abiding by the Memorandum of Understanding (MOU) between the application and the electronic signature service;

(3) Ensuring all applications using electronic signature services meet electronic signature service requirements;

(4) Ensuring adequate self-guided training or reference documentation is available to electronic signature users;

(5) Performing credential assurance self-assessment for each system/application role transaction;

(6) Reviewing and approving recommended assurance determinations for credential assurance authority approval;

(7) Reviewing and approving/rejecting requests for use of the electronic signature service(s), where applicable; and

(8) Complying with all security requirements in VA Handbook 6500.

g. Electronic Signature Service User is responsible for:

(1) Enrolling and applying for electronic signature credentials in order 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 and procedures;

(3) Addressing the consequences that result from the disclosure of the electronic signature service credential within his/her control;

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

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

h. **Electronic Signature Service Credential Issuer** is responsible for:

(1) Issuing and maintaining the electronic signature service credentials including the associated password, passphrase, or personal identification number (PIN); and

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

i. **Credential User** is responsible for:

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

(2) Reporting the loss or false use of an electronic credential;

(3) Surrendering electronic credentials upon termination of association with VA or upon the direction of the issuing authority (applies to LOA 4 credentials and LOA3 physical tokens);

(4) Completing annual security and privacy training as required, sign VA Rules of Behavior, and comply with VA Handbook 6500; and.

(5) Completing a background investigation as required in VA Directive and Handbook 0710 and VA Handbook 6500.

j. **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; and

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

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

(1) Authorizing level of access and defining the validity period for access by each delegate; and

(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.

3. LEVELS OF ASSURANCE AND ELECTRONIC AUTHENTICATION RISK ASSESSMENTS

a. In order to gain access to identity, credential or access services, applications must undergo an electronic authentication risk assessment to receive an LOA determination. The assurance determination guides the choice of technologies and the details of their implementation and considers whether those technologies provide adequate assurance to support the residual assurance risk associated with the ability to conduct transactions with VA systems. LOA determinations shall be evaluated every time additional access or transactions are changed within the application.

b. VA follows the NIST *SP 800-63-2,* defines graduated levels of assurance that govern the requirements users must meet to assure their identity and conduct transactions with VA systems. Each assurance level, starting at low and ending at very high, introduces controls that provide additional security to mitigate the risks of a user gaining unauthorized access and conducting unauthorized transactions.

(1) Low. No confidence in identity. There is no assurance required and all claimed identities are accepted. There are no security controls in place to assure the identity of the claimant at this level and no authentication is necessary.

(2) Medium. Moderate confidence in identity. Limited assurance of identity is required. On balance, provides evidence allowing confidence in non-repudiation and inability to dispute of actions performed. Includes single-factor authentication.

(3) High. High confidence in identity. Significant assurance of identity is required. Provides evidence for a high confidence level of non-repudiation and inability to dispute of actions performed. Includes using two-factor authentication.

(4) Very High. Very high confidence in identity. Appropriate where very high confidence in the asserted identity's accuracy is required. Provides evidence for a very-high level of non-repudiation and inability to dispute of actions. Includes using two-factor authentication with a hard token and a biometric.

c. Electronic authentication risk assessments leverage the basic framework for existing security risk categorization, as defined in VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: 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, as defined in NIST SP 800-30, *Risk Management Guide for Information Technology Systems.*

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

(2) A self-assessment is conducted by the information system owners and lines of business to assign scores for the impact and probability for each of 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:

(a) Damage to reputation. Consider inconveniences, distress, or damages that occur to the standing or reputation of any involved party.

1. Low. At worst, limited, short-term inconvenience, distress or embarrassment to any party.

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

3. 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).

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

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

2. Moderate. At worst, a serious unrecoverable financial loss to any party, or a serious agency liability.

3. High. Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

(c) Harm to agency 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 3.c.(2)(a) above).

1. Low. At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectiveness, or (ii) minor damage to organizational assets or public interests.

2. Moderate. At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness; or (ii) significant damage to organizational assets or public interests.

3. High. A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

(d) Unauthorized release of sensitive information. Consider the effect(s) which result from an unauthorized release of VA sensitive information. In assessing degree of impact, it is important to consider both 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.

1. Low. At worst, a limited release of VA sensitive information to unauthorized parties resulting in a loss of confidentiality with a low-impact as defined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.

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

3. High. A release of VA sensitive information to unauthorized parties resulting in loss of confidentiality with a high-impact as defined in FIPS 199.

(e) Personal safety. Any ability to modify health information poses risks to personal safety. Most other transactions would not have an impact on personal safety and would be rated “not applicable” or “N/A.”

1. Low. At worst, minor injury not requiring medical treatment.

2. Moderate. At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.

3. High. A risk of serious injury or death.

(f) Civil/Criminal violations. Determine if VA be subjected to civil or criminal violations.

1. Low. At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.

2. Moderate. At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.

3. High. A risk of civil or criminal violations that are of special importance to enforcement programs.

d. 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.

(1) Information system owners may choose to accept a single assurance determination for all transactions performed by a single set of users; or

(2) Information system owners may choose to accept multiple assurance determinations for each transaction performed by a single set of users.

(3) 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. The risk methodology is provided in Appendix H.

(4) The final assurance determination shall be approved by the information system owner and an assurance determination recommendation is provided to the electronic authentication risk assessment approving authority for acceptance.

4. ENTERPRISE IDENTITY PROOFING

a. Identity Proofing Controls

(1) Chain of trust provides the following benefits:

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

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

(c) Allows acceptance of identity proofing results from third parties or other parties within VA.

(2) In order to ensure that access to personally identifiable information (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 a Level 2 credential or above for access to PII.

b. In-person Identity Proofing Process and Requirements

(1) In-person identity proofing can only be used for issuance of credentials at Level 2, 3, and 4. In-person identity proofing at Level 1 does not exist because all identities, including pseudonymous identities, are accepted.

(2) 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.

(3) In order to be in-person proofed:

(a) The applicant must present the required forms of identification (see Appendix C of this Handbook) to the identity proofing official. 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 presented and verified if verification cannot be obtained from existing records.

(b) 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 of this Handbook for proofing requirements for each LOA.

(c) 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.

(d) 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.

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

(f) 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 E of this Handbook for acceptable documents). If an address is not on record, the applicant may provide an address, validated against acceptable identity source documents (see Appendix C of this Handbook) if available. Additional contact information such as home phone, mobile phone, or email address may also be recorded.

(g) 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.

(h) If the applicant is unable to 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 asking the applicant to respond to a series of verifiable challenge questions. An example is provided in the VHA Directive 2012-036, *Identity Authentication for Health Care Services*.

c. Remote Identity Proofing Process and Requirements

(1) Remote identity proofing can only be used for issuance of credentials at Level 2 and Level 3. Remote identity proofing at Level 1 does not exist because all identities, including pseudonymous identities, are accepted. Level 4 does not permit remote identity proofing.

(2) 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).[1]

(3) To access any information or make changes to Veteran PII information by telephone, the VA employee **must** ask the Veteran, or person on behalf of the Veteran, the Veteran’s full name. The employee must ask 2 additional questions from Table 1 in Appendix D. Figure 1 in Appendix D shows an example of a general telephone identity proofing process.

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

(5) In order to be remotely identity proofed through automated identity proofing services:

[1] Department of Veterans Affairs Telephone Identity Proofing Memo, dated March 14, 2012

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

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

(c) The applicant must present information from required forms of identification (see Appendix C of this Handbook) 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 Appendix C of this Handbook.

(d) 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.

(e) If the applicant record lists a mailing address, an effort will be made to validate the address in 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.

(f) 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.

(g) 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.

5. ELECTRONIC CREDENTIAL MANAGEMENT

a. Applicability. Credential issuance and credentials accepted for use with IAM Services will be required to comply with the following statements.

b. Electronic Credential Management Controls will:

(1) Support multiple credentials for a given identity.

(2) Support credentials at every LOA for a given identity.

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

(4) Support creation of pseudonym identities and tokens to support legal investigations.

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

(6) Have the capability to consume credentials at Assurance Levels 4, 3, and 2 that are created and issued externally to VA.

(7) Have the capability to consume identity data from credentials at Assurance Levels 4, 3, and 2 that have been created and issued external to VA.

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

c. Credential Categories

(1) Hard Token

(2) Soft Token

d. Credential Assurance Levels. Credentials at each assurance level are aligned with Appendix F of this Handbook.

e. Credential Lifecycle

(1) 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).

(2) Usage

(a) All credential users are notified at the time of issuance of their responsibilities for possession of their electronic credential.

(b) Forging, falsifying, or allowing misuse of an electronic credential in order to gain unauthorized access to VA physical or logical resources is punishable up to the full extent of the law.

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

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

(a) The user no longer has a legitimate need for the capability;

(b) The user requests revocation of the capability; or

(c) VA authorities deem it necessary to revoke or disable the capability.

(5) Termination. Hard token electronic credentials must be destroyed when they are expired, replaced, defective, or otherwise no longer active. Soft electronic credentials associated with a terminated hard token must be revoked in these instances.

(6) 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.

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

(8) Lost/Stolen

(a) Lost or stolen electronic credentials should be reported to the issuing office as soon as practicable, or within 24 hours after discovery of the loss/theft.

(b) 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 as a result of this action.

6. ELECTRONIC SIGNATURES

a. Applicability: This section provides policy on the use of electronic signatures for IAM Services Signature Service.

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

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

b. Electronic Signature Service Capabilities will include:

(1) Ability to apply an electronic signature for documents, email, and other artifacts that are unique to the person making the signature.

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

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

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

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

c. Electronic Signature Service requirements:

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

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

(3) The electronic signature service shall accept credentials approved by the IAM Integrated Project Team.

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

(5) Level 2 or higher credential shall be a prerequisite to obtaining and using key certificate pair for signing documents digitally.

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

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

d. Electronic Signature Service Approval Process

(1) Information system owners shall submit a request for 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 require signature, and a list of relevant PII that is captured in the transaction. Information system owners shall be required to complete an electronic assurance risk assessment and include the LOA determination in the service request.

(2) The electronic signature service request shall be reviewed by the electronic signature service owner and an LOA shall be assigned based on the results of the assurance determination process. If an LOA of Very High (4) 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.

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

e. MOU

(1) Owners of participating VA consuming applications shall sign an MOU with the IAM electronic signature service documenting specific roles and responsibilities of the application and the electronic signature service including the following:

(a) Authentication of the user at a LOA determined to be commensurate with the signing transaction through an electronic authentication risk assessment;

(b) Presentation of demographic data in an approved form data structure; and

(c) A user interface for the signing event.

(2) The electronic signature service will provide:

(a) Electronic signature certificates;

(b) A unique identifier appropriate for the signing transaction;

(c) A user generated PIN used to unlock the signing credential for credentials LOA 3 or higher; and

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

7. ACCESS MANAGEMENT

a. Single Sign-On (SSO). The policies and responsibilities set forth in VA Directive 6500, *Managing Information Security Risk: VA Information Security Program,* and VA Handbook 6500 in regards to identification and authentication are applicable to SSO.

b. Physical Access. The policies and responsibilities set forth in VA Directive and Handbook 0730, *Security and Law Enforcement,* and VA Handbook 6500 govern common and secure physical access policies.

c. Logical Access. The policies and responsibilities set forth in VA Directive and Handbook 6500 govern logical access policies.

d. Provisioning

(1) Provisioning must be conducted by authorized personnel.

(2) Provisioning may include automatic mechanisms.

(3) User accounts must be reviewed at least annually and is ultimately the Information System Owners responsibility to ensure this is completed.

e. Delegated Authority

(1) Delegators may specify the time duration for delegate access to their information. If a time duration is not specified, the duration will be set to one year.

(2) 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 who have been delegated access rights.

(3) 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.

(4) Delegators shall have access to a list of each delegate’s access rights.

(5) Delegators shall be informed, in terms that are understandable and in common language, of 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).

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

(7) Delegators shall be shown identity elements (e.g., first name, last name, DoB, address, phone number) belonging to the delegate in order to confirm the identity of the delegate prior to granting access.

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

(9) Delegates who have been granted the ability to grant and revoke rights by the delegator, may do so to persons of their choosing.

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

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

(12) Delegate status may be changed or deactivated at any time by the delegator or by VA.

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

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

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

(16) 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.

(17) In the event that 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.

(18) The actions of delegates shall be logged in an auditable manner and shall be distinguishable from those of the delegator.

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

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

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

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

8. REFERENCES

a. 15 U.S.C. §§ 7001-7006, *Electronic Records and Signatures in Global and National Commerce Act* ("E-SIGN")

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

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

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

e. Committee on National Security Systems (CNSS) *Instruction No. 4009*, April 26, 2010

f. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guide*, December 2, 2011

g. *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*, February, 2004

h. *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*, March, 2006

i. *FIPS 201-2, Personal Identity Verification of Federal Employees and Contractors,* August, 2013

j. *Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004

k. *NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach,* February, 2010

l. *NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations*, April, 2013

m. *NIST SP 800-63-2, Electronic Authentication Guideline*, August, 2013

n. *OMB Memorandum 00-15, OMB Guidance on Implementing the Electronic Signatures,* September 25, 2000

o. *OMB M-04-04, E-Authentication Guidance for Federal Agencies*, December 16, 2003

p. *OMB M-06-16, Protection of Sensitive Agency Information*, June 23, 2006

q. *OMB M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011

r. *OMB Memorandum, Requirements for Accepting Externally-Issued Identity Credentials*, October 6, 2011

s. *VA Directive 6500, Managing Information Security Risk: VA Information Security Program*

t. *VA Directive and Handbook 0730, Security and Law Enforcement*

u. *VA Directive and Handbook 0735, Homeland Security Presidential Directive 12 Program*

v. *VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*

w. *VHA Directive 2012-036, Identity Authentication for Health Care Services, December 26, 2012*

APPENDIX A: 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 201-2

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 SP800-63-2

d. **Authentication:** The process of establishing confidence in the identity of users or information systems. SOURCE: NIST SP800-63-2

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

f. **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.

g. **Claimant:** A party whose identity is to be verified using an authentication protocol. SOURCE: NIST 800-63-2

h. **Claimed Identity:** Any identity that has not been vetted through the identity proofing process.

i. **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 201-2

j. **Electronic Authentication Risk Assessment:** The process of identifying risks to security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.

k. **Electronic Credential:** An object that authoritatively binds an identity to a token possessed and controlled by a person.

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

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

n. **Identity:** A set of attributes that uniquely describe a person within a given context. The set of physical and behavioral characteristics by which an individual is uniquely recognizable. SOURCE: VA Directive 0735

o. **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

p. **In-Person Proofing:** Identity proofing that occurs in the presence of a VA appointed representative.

q. **Intent:** The understanding and acceptance of the purpose of the electronic signature that is non-repudiable.

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

s. **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

t. **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 maybe available in an environment, may include the creation, modification, deletion, suspension, or restoration of a defined set of privileges. SOURCE: FICAM Roadmap

u. **Remote Proofing:** Identity proofing that occurs outside the physical presence of a VA appointed representative.

v. **Risk Assessment:** The process of identifying risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. SOURCE: NIST SP800-63-2

w. **Token:** Something, either physical or digital, that the Claimant possesses and controls that serves to represent or authenticate an identity, e.g., username and password combination, ID card, or a PKI certificate. SOURCE: NIST SP800-63-2

x. **Transaction:** The transmission of information between two parties relating to the conduct of business, commercial, or governmental activities.

y. **Verify:** Confirmation by examination and provision of identity source documentation that a claimed identity is a valid identity.

z. **Vetting:** Process of examination and evaluation, including background check activities; results in establishing verified credentials and attributes. SOURCE: FICAM Roadmap

APPENDIX B: ACRONYMS

Acronym	Definition
CIO	Chief Information Officer
CSP	Credentials Service Provider
DoB	Date of Birth
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HSPD-12	Homeland Security Presidential Directive - 12
IAM	Identity and Access Management
ISO	Information Security Officer
LOA	Level of Assurance
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SP	Special Publication
SSN	Social Security Number
SSO	Single Sign-On
VA	Veterans Affairs

APPENDIX C: LIST OF ACCEPTABLE DOCUMENTS

The following documents are designated as acceptable for the purpose of identity proofing in accordance with NIST 800-63-2 and Appendix G of this Handbook. All documents and artifacts presented must be unexpired.

COLUMN A **PRIMARY** **Government Issued Photo ID**	**COLUMN B** **SECONDARY** **Non-Picture ID and/or Acceptable Picture ID not issued by Federal or State Government**
• U.S. Passport or U.S. Passport Card • Permanent Resident Card or Alien Registration Receipt Card (Form I-551) • Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa • Employment Authorization Document that contains a photograph (Form I-766) • Foreign passport with Form I-94 or Form I-94A that has the same name as the passport • Driver's license or ID card issued Federally, by a State, or an outlying possession of the United States Government; the card must contain a photograph and information such as name, date of birth, gender, height, eye color, and address (includes PIVs) • U.S. Military ID card (both active and retired acceptable) or draft record issued by National Archives and Registration Administration or Selective Service System • U.S. Military dependent's ID card • Non-U.S. Driver's license or foreign government issued ID card, includes passports; the card must contain a photograph and information such as name, date of birth, gender, height, eye color, and address (In-person identity proofing ONLY) o (When accepting foreign-issued identification for identity proofing at LOA2, challenge questions shall be used to ensure applicants identity)	• U.S. Social Security Card issued by the Social Security Administration • U.S. Original or certified Birth Certificate • Certification of Birth Abroad Issued by the Department of State (Form FS-545) • Certification of Report of Birth issued by the Department of State (Form DS-1350) • U.S. Certificate of Naturalization (Form N-550 or N-570); must contain a photograph or information such as name, date of birth, gender, height, and eye color • U.S. State or territory issued Voter's Registration Card • Native American Tribal Document • U.S. Citizen ID Card (Form I-197) • Identification Card for Use of Resident Citizen in the United States (Form I-179) • Employment Authorization document issued by the Department of Homeland Security • School ID with photograph • U.S. Coast Guard Merchant Mariner Card

*NOTE: U.S. includes state, county, municipal authority or outlying possession of the United States.

APPENDIX D: TELEPHONE IDENTITY PROOFING PROCESS

(Reference Document: *Department of Veterans Affairs Telephone Identity Proofing Standard Operating Procedure, dated March 14, 2012*)

Overview

This standard operating procedure documents the processes and requirements for 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 personally identifiable information (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. 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.

Standard Operating Procedures

1. A customer places a call to a VA service.
2. VA staff answers the phone and performs an initial identification of the customer through a full name inquiry.
3. The VA staff will inform the customer that they should be in a safe environment to limit eavesdropping.
4. VA staff requests a description of the issue the customer is reporting.
5. VA staff transfers the call, as necessary, to the appropriate support group.
6. VA staff requests verification of the customer's full name.
7. VA staff asks the customer two additional questions based on the questions found in Table 1, Additional Questions for Verification.
8. If the identity is confirmed, VA staff assists the customer in resolving the issue.
9. If the identity is not confirmed, the call may be terminated, or other appropriate actions taken, as determined by call center policies.

Table 1 - Additional Questions for Verification

Additional Questions for Verification	
Date of birth (DoB), including year	Branch of service and service dates
Full Social Security number (SSN) *NOTE: Although VA has indicated it will not call a Veteran and ask for a SSN, it is allowable to ask for a SSN when the Veteran (or someone on the Veteran's behalf) initiates the call.*	Home address (including zip code)
Military Service number	Mother's maiden name
Next of kin	Spouse's name
VA Claim Number/Unique Identifier	Place of birth, city and state
Current benefit check amount	Current account number for direct deposit

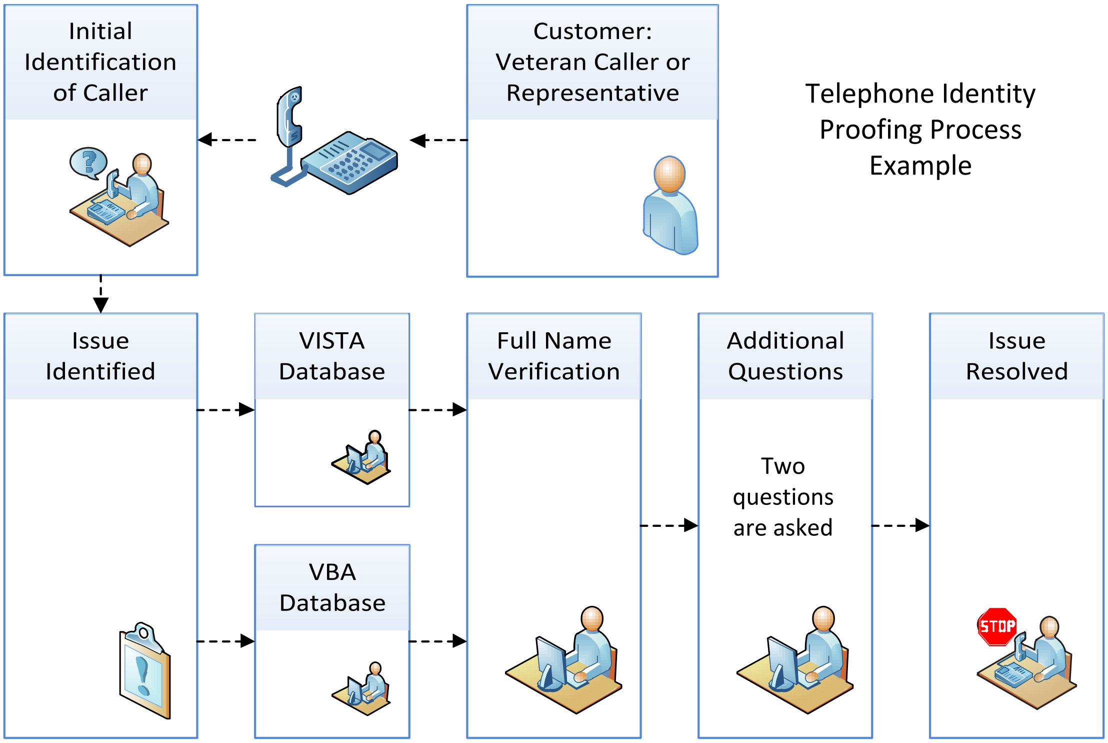

Figure 1 - Telephone Identity Proofing Process Example

APPENDIX E: ADDRESS CONFIRMATION DOCUMENT CRITERIA

The following documents are designated as acceptable for identifying the current mailing address. The applicants name must be the addressee on the document, and the document must be dated within the last 30 days.

Acceptable Documents to Verify Mailing Addresses
1. Phone bill from local phone service provider
2. Electric bill from a local electrical service provider
3. Fossil fuel (oil, gas, propane) bill from a local service provider
4. Credit card statement
5. Checking or savings account statement
6. Local personal property tax bill
7. Mortgage or rent payment voucher
8. Veterans Benefits Administration (VBA) corporate data reflecting correct mailing address as verified by applicant

APPENDIX F: ASSURANCE LEVEL GUIDE

Assurance Level	Description	Restrictions	Attributes	Physical Signature	Electronic Signature Mechanism
Low (1)	There is no identity proofing requirement at this level. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4.	Plaintext passwords or secrets are not transmitted across a network at Level 1.	Essentially no security controls Easiest to dispute	Verbal signature (for example, acceptance of responsibility for sitting in the airplane exit row)	Electronic signature without proof of authentication (x in the box).
Medium (2)	Identity proofing requirements are introduced, requiring presentation of identifying materials or information before a credential is issued for authentication. For single factor authentication, Memorized Secret Tokens, Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out of Band Tokens, and Single Factor One Time Password Devices are allowed at Level 2. Level 2 also allows any of the token methods of Levels 3 or 4.	Long-term shared authentication secrets, if used, are never revealed to any party except the Claimant and Verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent Verifiers by the CSP. In addition to Level 1 requirements, assertions must be resistant to disclosure, redirection, capture and substitution attacks. Approved cryptographic techniques are required for all assertion protocols used at Level 2 and above.	Moderate integrity Limited non-repudiation Somewhat hard to dispute	Handwritten signature /Signature recorded electronically. For example signing a clinical note in a closed environment, signing 1010 EZ.	Electronic signature with one-factor authentication Application notarization for signature validation/binding.

Assurance Level	Description	Restrictions	Attributes	Physical Signature	Electronic Signature Mechanism
High (3)	Provides multi-factor remote network authentication. Identity proofing procedures require verification of identifying materials and information. It is based on proof of possession of a key or a one-time password through a cryptographic protocol. Authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.	Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the CSP, however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations.	High integrity, authentication, and non-repudiation Hardest to dispute	Handwritten signature with in-person proofing, witnesses and/or notarization meeting legal standards.	Two-factor authentication Digital Signature Identity proofing based upon formal processes Strong signature validation/binding Application notarization

Assurance Level	Description	Restrictions	Attributes	Physical Signature	Electronic Signature Mechanism
Very High (4)	Highest practical remote network authentication assurance. Authentication is based on proof of possession of a key through a cryptographic protocol. Only “hard” cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process.	The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.	Very high integrity, authentication , and non-repudiation Hardest to dispute	Handwritten signature with in-person proofing, witnesses and/or notarization meeting legal standards.	Two-factor authentication with hard token Digital Signature In-person proofing based upon formal processes Strong signature validation/binding Application notarization

ASSURANCE LEVEL EXAMPLES

Level of Assurance	**Interface Type**	**Impact to VA**	**Example Capabilities**	**Description**
1	Government to Consumer; General Public Access	Low	User Acceptance, Licensing Agreement	Usage agreement for viewing/using online material; identity verification typically not required for access/usage
2	VA to Vendors; VA Corporate/ Internal Data	Medium	Password/ Token verified session with electronic verification of intent	When a user accesses his/her individual content or material and agrees to a modification to his/her record; Requires single-factor authentication through presentation of identifying materials or information before a credential issued for authentication (i.e., passwords, secret tokens, etc.)
3	Government to Government/ Commercial	High	Full PKI digital signature utilizing approve credentials (i.e., Common Access Card (CAC), PIV)	PII is stored or accessed by the application; Two-factor authentication required (i.e., password + biometrics, password + token) is required.
4		Very High		PII is stored or accessed; Minimum secured two-factor authentication required. Secure authentication is based on proof of possession of a key token through a multi-factor cryptographic protocol.

APPENDIX G: IDENTITY PROOFING LEVELS

In-person

Level 2	
Basis for issuing credentials	Possession of an unexpired current primary Government photo-ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or Passport)
Identity Proofing Official actions	Inspects photo-ID, compares picture to applicant, records ID number, address and DoB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or; b) If ID does not confirm address of record, issues credentials in a manner that confirms address of record.
Level 3	
Basis for issuing credentials	Possession of an unexpired current primary Government photo-ID that contains applicant's picture and either address of record or nationality (e.g., driver's license or passport)
Identity Proofing Official actions	Inspects photo-ID and verifies via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compares picture to applicant, record ID number, address and DoB. If ID is valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issues credentials in a manner that confirms address of record.
Level 4	
Basis for issuing credentials	In-person appearance and verification of two independent ID documents or accounts, meeting the requirements for Level 3 (in-person and remote), one of which must be unexpired current primary Government photo-ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport), and a new recording of a biometric of the applicant at the time of application.
Identity Proofing Official actions	a) *Primary Photo ID:* Inspects photo-ID and verifies via the issuing government agency, compares picture to applicant, records ID number, address and DoB. b) *Secondary Government ID or financial account* 1) Inspects photo-ID and if valid, compares picture to applicant, records ID number, address and DoB, or; 2) Verifies financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. c) *Record Current Biometric:* Records a current biometric (e.g., photograph or fingerprints) to ensure that applicant cannot repudiate application. d) *Confirm Address* Issues credentials in a manner that confirms address of record.

Remote

Level 2	
Basis for issuing credentials	Possession of an unexpired Government photo-ID (e.g., a driver's license or Passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of **either** number.
Identity Proofing Official actions	• Inspects both ID number and account number supplied by applicant (e.g., for correct number of digits). Verifies information provided by applicant including ID number OR account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • Address confirmation and notification: a) Sends notice to an address of record confirmed in the records check; or, b) Issues credentials in a manner that confirms the address of record supplied by the applicant; or c) Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications at number associated with the applicant in records. Any secret sent over an unprotected channel shall be reset upon first use.
Level 3	
Basis for issuing credentials	Possession of an unexpired Government photo-ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of **both** numbers.
Identity Proofing Officials actions	• Verifies information provided by applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. • Address confirmation: a) Issues credentials in a manner that confirms the address of record supplied by the applicant; or b) Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice or using equivalent alternative means to establish non-repudiation.
Level 4	
Basis for issuing credentials	Not Applicable
Identity Proofing Official actions	Not Applicable

APPENDIX H: RISK METHODOLOGY

Impact Categories (IC)	IAL1*	IAL 2*	IAL 3*	IAL 4*
IC #1 Damage to Reputation	Low 1-15	Moderate 16-31	Moderate 32-48	High 49-81
IC #2 Financial Loss / Liability	Low 1-15	Moderate 16-31	Moderate 32-48	High 49-81
IC #3 Harm to Agency Programs or Public Interest	N/A	Low 1-15	Moderate 16-48	High 49-81
IC #4 Unauthorized Release of Sensitive Information	N/A	Low 1-15	Moderate 16-48	High 49-81
IC #5 Personal Safety	N/A	N/A	Low 1-15	Moderate or High 16-48 or 49-81
IC #6 Civil / Criminal Violations	N/A	Low 1-15	Moderate 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.**