Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6510
Transmittal Sheet
January 15, 2016

VA IDENTITY AND ACCESS MANAGEMENT

1. REASON FOR ISSUE: This Directive defines the policy and responsibilities to manage identity and access management for the Department of Veterans Affairs (VA) enterprise.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive sets forth VA policy and responsibilities for enterprise identity and access management.

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

4. RELATED HANDBOOK: VA Handbook 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 VETERANS AFFAIRS:

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

Distribution: Electronic Only

This page is intentionally left blank.

VA IDENTITY AND ACCESS MANAGEMENT

1. PURPOSE:

This Directive defines the policies for enterprise identity and access management (IAM) for the Department of Veterans Affairs (VA).

a. The policies identified in this Directive apply to all VA administrations, staff offices, and all VA staff who support IAM functionality, Veterans, affiliates, and any users who require logical access to VA information services including resources both internally and externally managed and offered through VA.

b. The policies established in this Directive address assurance levels, electronic authentication risk assessments, identity proofing, identity credential management, electronic signature, and access management.

c. The policies established in this Directive are written to meet or exceed the federal standards listed in the References section.

2. POLICY:

a. Assurance Levels and Electronic Authentication Risk Assessments

(1) VA shall have an electronic authentication risk assessment process, in accord with the Office of Management and Budget (OMB) Memorandum 04-04, *E-Authentication Guidance for Federal Agencies,* that must be completed for all department applications in order to determine the appropriate level of assurance based on the risk inherent to the application and the required confidence in user identities to conduct transactions in the application. The electronic authentication risk assessment process examines the transactions; the potential for misuse of transaction information; overall risk to individuals, VA operations and assets; and potential impacts to involved organizations. The risks identified shall be used to define the appropriate assurance level for each role and transaction within the application.

(2) VA's electronic authentication risk assessment process shall comply with the National Institute for Standard and Technology (NIST) Special Publication 800-63-2*, Electronic Authentication Guideline*, which defines graduated levels of assurance for requesting, registering, sponsoring, identity proofing, vetting, adjudicating, and issuing electronic credentials.

(3) The Office of Information Security (OIS) will monitor and manage the electronic authentication risk assessment process and its alignment to OMB and NIST standards. OIS will provide guidance and work with other program offices to achieve compliance with these standards.

(4) VA shall comply with the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, which outlines a common framework for identity, credential, and access management within the Federal Government, including supporting implementation guidance for program managers, leadership, and stakeholders.

b. **Identity Proofing**

(1) All VA staff who support IAM functionality, Veterans, and any users who request access to VA information resources shall adhere to VA's identity proofing process matching the level of assurance required by performing the electronic authentication risk assessment process prior to the issuance of VA electronic credentials. 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*.

(2) The identity proofing process and identity proofing requirements are based on the level of assurance defined in the electronic authentication risk assessment process, in accordance with NIST guidelines. The process verifies all claimed identities prior to the issuance of VA electronic credentials, the initial grant of access, or provisioning of access rights.

(3) VA shall provide remote identity proofing as an alternative to in-person identity proofing for issuing credentials in accordance with NIST guidance and VA policies.

(4) VA will accept identity proofing data from VA internal services as well as VA-approved third parties. Third party identity proofing processes must meet federal standards and adhere to VA policies prior to approval for use.

c. **Electronic Credentials**

(1) VA shall manage electronic credentials to ensure they reflect confidence in verified user identities. The electronic credentials are used to access VA resources that require authentication or authorization; are only issued by authorized personnel; are issued in a manner that ensures the individual receiving the electronic credential is the verified individual; and includes lifecycle management of the electronic credentials.

(2) VA may accept third-party identity credentials for purposes of access to VA information resources. Identity credentials accepted by VA shall be compliant with FICAM and meet at least one of the following criteria:

(a) Issued by the federal government;

(b) Cross-certified by the Federal Bridge; or

(c) Issued by a third-party identity credential provider in accordance with NIST guidelines and Federal Chief Information Officers (CIO) Council procedures as required by OMB.

(3) All VA-issued credentials must meet federal standards and adhere to VA policies.

(4) VA provides governance for the correlation between electronic credentials issued to verified and trusted identities and identity records contained in internal systems to ensure that the right person has access to the right information.

(5) Access privileges shall be associated to a vetted identity and reviewed periodically throughout the lifecycle of the identity.

(6) VA, where appropriate, captures, uses, and accepts biometric data to enable biometric logon, biometric unlock of authentication tokens, and enable non-repudiation.

(a) Biometrics is an acceptable identity methodology under NIST SP 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, April, 2013, to authenticate individuals for logical or physical access.

(b) Biometrics can be used for authentication for Level of Assurance (LOA) 2 through 4.

d. **Use of Electronic Credentials as Electronic Signatures**

(1) VA accepts the use of electronic signatures as equivalent to traditional handwritten signatures, also referred to as wet signatures. Such acceptance shall not limit users from conducting transactions in a non-electronic form.

(2) VA shall use digital signatures, which are considered a form of electronic signatures that attaches encrypted data derived from the electronic credential to the electronic document. The encrypted data constituting the digital signature may be used as an electronic signature, as part of a process to authenticate a person or device, or to verify the integrity of the record.

(3) The identity of the individual executing a digital or electronic signature shall be validated to the appropriate level of assurance prior its (1) capture, or (2) application to a document or transaction. Validation, capture, and execution shall occur during the same session.

(4) Use of a digital or electronic signature as legally binding in addition to authentication of the signer or verifying the integrity of the record requires a positive decision or action by the individual indicating to the system or an observer their intent to execute the signature and that it be legally binding.

(5) Digital and electronic signatures are captured using methods familiar to the user and shall not require the user to remember special codes for the purpose of electronic signature alone.

(6) Applications utilizing electronic signature shall generate an auditable record of the end user's signature that is maintained for the life of the document without possibility of alteration or corruption and shall include submission of signature as the event, the signed document, the identity of the signee, and the credential used to sign the document. An auditable record includes events captured by the system in the audit trail that may include items such as verification of credential provided at moment of signature, date/time of signature, and distinguished name.

(7) Applications utilizing electronic signatures require data integrity mechanisms that do not allow changes, errors, or corruption in data upon signature of the document.

(8) A user generated personal identification number (PIN) will be used to unlock the signing credential for credentials LOA 3 or higher.

e. **Access Management**

(1) VA shall grant access to information and information systems commensurate with the risk inherent in access and the level of assurance of the identity credential used to access the information and information systems.

(2) VA implements standard methods for controlling access to information, information systems, and to both secure and publicly available physical resources.

3. RESPONSIBILITIES

a. **Assistant Secretary for Information and Technology, who serves as VA CIO,** or designee will:

(1) Manage and develop enterprise level IAM technology for the Department, ensuring that proper equipment is purchased and used, and contracts are established to support the work when needed;

(2) Review and approve all assurance determinations from the electronic authentication risk assessments;

(3) Ensure interoperability with approved electronic credentials issued by external electronic credential providers, as appropriate;

(4) Ensure the issuance of electronic credentials associated with an identity for access to services, IT resources, and physical resources;

(5) Establish Office of Information and Technology (OIT) policies that clearly state IT processes, roles, and responsibilities in conformance with identity, credential, and access management services requirements; and

(6) Ensure compliance with the responsibilities set forth in paragraph 3.e. of this Directive.

b. **Deputy Assistant Secretary (DAS) for Information Security,** or designee will:

(1) Act as the business sponsor for IAM;

(2) Establish Enterprise IAM Business Office;

(3) Oversee and coordinate VA-wide IAM activities;

(4) Establish VA-wide IAM policy;

(5) Provide stewardship for the IAM strategic vision and roadmap;

(6) Collaborate with FICAM, National Strategy for Trusted Identities in Cyberspace, and other key stakeholders;

(7) Develop and maintain VA's Transition Plan for Alignment with the FICAM Segment Architecture;

(8) Coordinate and oversee IAM steering committees, governance boards, and integrated project teams, as necessary;

(9) Define, prioritize, and ensure implementation of Enterprise IAM Business Requirements;

(10) Set standards and evaluate performance of activities implementing IAM requirements;

(11) Coordinate VA-wide IAM communications, including reports to committee members; and

(12) Advocate for the implementation of enterprise-wide IAM requirements, as necessary.

c. **Assistant Secretary for Operations, Security, and Preparedness** will:

(1) Ensures all enterprise Physical Access Control System (PACS) are integrated with VA architecture and systems; and

(2) Ensure compliance with the responsibilities set forth in paragraph 3.e. of this Directive.

d. **Executive Director, Office of Acquisition, Logistics, and Construction** will:

(1) Ensure support of acquisitions activities necessary to support the IAM Program; and

(2) Ensure compliance with the responsibilities set forth in paragraph 3.e. of this Directive.

e. **Under Secretaries, Assistant Secretaries, Deputy Assistant Secretaries, and Other Key Officials** will:

(1) Ensure compliance with the policies, procedures, and guidance issued by the OIT and established in this Directive and any associated policies;

(2) Ensure the accuracy, validity, and completeness of all input into all information systems used to support VA IAM;

(3) As appropriate, establish organizational policies, including policies which delineate processes, roles and responsibilities for VA consistent with the requirements in this Directive;

(4) Participate in steering committees, governance boards, and integrated project teams, as requested by the DAS for Information Security; and

(5) Coordinate the development of processes and systems to implement FICAM with the DAS for Information Security.

f. **Office of Inspector General** will:

(1) Conduct audits of IAM processes and systems, as necessary;

(2) Conduct investigations of complaints and referrals of violations, as deemed appropriate; and

(3) Conduct other oversight activities as authorized by the Inspector General Act of 1978, as amended, 5 U.S.C. App. 3.

g. **Office of General Counsel** will provide review of and advice on legal issues related to IAM policies and procedures.

4. 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. Uniform Electronic Transactions Act ("UETA"), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999, adopted by 47 states as of November 2010

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

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

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

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

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

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

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

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

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

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

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

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

r. *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

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

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

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

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

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

5. 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 201-1

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 800-63-2

d. **Authentication:** The process of establishing confidence in the identity of users or information systems. SOURCE: NIST SP 800-63-2

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

f. **Authorized**: For the purpose of electronic authorization, the level of assurance of the electronic method, the sensitivity of the document, and the authorization level of the signer are commensurate with the risk of forgery of the document and the ability of the signer to repudiate that they in fact signed the document.

g. **Claimant:** A party whose identity is to be verified using an authentication protocol. SOURCE: NIST SP 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. **Digital Signature:** Digital signatures are an electronic signature based on cryptographic methods used to verify the identity of the signer and integrity of the data.

k. **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.

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

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

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 U.S.C. § 3552

s. **Non-Repudiation:** Protection against an individual falsely denying having performed a particular action. Provides the capability to create evidence as to whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. SOURCE: NIST SP 800-53-4

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. **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 SP 800-63-2

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

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

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