Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6510
Transmittal Sheet
September 3, 2024

VA IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT

1. **REASON FOR ISSUE:** The Department of Veterans Affairs (VA) Directive 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 the responsible office to Office of Information Technology (OIT) ICAM Program Management Office (PMO) – Office of Information Security (OIS).

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

   c. Revise VA policies to meet or exceed the Federal standards listed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 - Digital Identity Guidelines suite including NIST SP 800-63A – Enrollment and Identity Proofing Guidelines, NIST SP 800-63B - Authentication and Lifecycle Management and NIST SP 800-63C – Federation and Assertions (hereby referred to as NIST SP 800-63 and appropriate corresponding letter).

   d. Revise VA policies and provide guidance to incorporate OMB M-19-17 - Enabling Missions Delivery through Improved Identity, Credential and Access Management (hereby referred to as OMB M-19-17).

   e. Revise VA policies and provide guidance to incorporate Executive Order 14028 – Improving the Nation’s Cybersecurity as related to ICAM.

   f. Revise VA policies and provides guidance to incorporate Executive Order 14058 – Transforming Federal Customer Experience and Service Delivery as related to ICAM.

   g. 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) as related to ICAM.

   h. Revise 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) as related to ICAM.

i. Revise VA policies and provides guidance to incorporate Executive Order 13988 - Preventing and Combating Discrimination on the Basis of Gender Identity and Sexual Orientation as related to ICAM.

j. Revise VA policies and provides guidance to incorporate OMB M-22-16 – Administration Cybersecurity Priorities for FY 2024 Budget (hereby referred to as OMB M-22-16) as related to ICAM.

k. Define VA requirements to develop and maintain a single comprehensive ICAM policy, process and technology solution roadmap, consistent with VA authorities and operational mission needs that encompass the VA's entire enterprise, aligned with the Government-wide FICAM Architecture requirements and incorporate applicable Federal policies, standards, playbooks and guidelines and include roles and responsibilities for all users.

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

m. Update roles and responsibilities for various offices for enterprise ICAM functions.

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

4. **RELATED HANDBOOK:** Handbook 6510, VA Identity, Credential and Access Management.

5. **RESCISSION:** VA Directive 6510, VA Identity and Access Management, dated January 15, 2016.

CERTIFIED BY:

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

BY 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.**This directive defines the policies for enterprise ICAM for the Department of Veterans Affairs (VA). The purpose of ICAM is to ensure secure and efficient operations to enable the VA to identify, credential, monitor and manage person and non-person entities (NPE) that access VA and Federal resources, including information, information systems, facilities and secured areas across the enterprise. The ICAM policies identified in this directive:

a. Apply to all VA Administrations, Staff Offices, all VA staff who support ICAM functionality, Contractors, Veterans, affiliates and any users who require physical access to VA facilities and/or logical access to VA information services. VA Information systems include resources both internally and externally managed and offered through VA.

b. Build on the 'Protect Function—Identity Management, Authentication and Access Controls' based upon the NIST Cybersecurity Framework (reference dd) and established in VA Directive 6500—VA Cybersecurity Program (reference j) to provide FICAM guidance to address assurance levels, electronic authentication risk assessments, identity proofing, identity credential management, electronic signature and access management. Build on NIST SP 800-53-5 Security and Privacy Controls for Information Systems and Organizations (hereby referred to as NIST SP 800-53) (reference l) to protect identity, execute least privilege principles and ensure that access is monitored and controlled properly as detailed in VA Handbook 6500 Risk Management Framework for VA Information Systems VA Information Security Program (reference k).

c. Are written to complement the following VA memos, directives and handbooks to provide a comprehensive framework for ICAM:

(1) The Office of Information Security manages a policy portal known as the VA Information Security Knowledge Service (KS). This policy portal covers the Risk Management Framework and in particular, the security controls used by VA and their implementation guidance.

(2) VA Directive and Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program (reference m). This Directive/Handbook establishes Department-wide requirements, policies, roles and responsibilities for the creation, operation and maintenance of an HSPD-12 Program necessary to ensure Department compliance with Homeland Security Presidential Directive 12 (HSPD-12) (reference f).

(3) VA Directive and Handbook 0710 Personnel Security and Suitability Program (reference o). This Directive/Handbook describes 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.

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

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

(6) VA Memo, Requirement for Two Factor Authentication for VA Network Access for Individuals with Dual Identities (VA Intranet Quorum [VAIQ] 7735690) (reference aa). 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).

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

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

2. POLICY.

a. All users shall comply with the FICAM policy (OMB M-19-17) and the FICAM Architecture guidance (reference d), which outlines a common framework for identity, credential and access management within the Federal Government, including supporting implementation guidance for program managers, Information System Owners (ISO), leadership and stakeholders.

b. VA shall comply with the OMB M-22-09 and utilize the NIST SP 800-207 to implement best practices and procedures regarding Zero Trust Architecture (ZTA).

c. VA shall implement NIST SP 800-63, to set the foundation for identity management and its usage to access physical and digital resources. This publication must be used in combination with the remaining suite of publications (NIST SP 800-63A, B and C) that relate to identity management issued by NIST, the Office of Personnel Management (OPM) and the Department of Homeland Security (DHS) to form a comprehensive approach to identity proofing that safeguards privacy and security.

d. VA shall incorporate Digital Identity Risk Management into existing VA processes as outlined in NIST SP 800-63, including selecting assurance levels commensurate with the risk to their digital service offerings.

e. VA shall comply with Federal Government-wide credentialing standards including Federal Information Processing Standards 201-3 (FIPS 201) or its successors for making all decisions related to issuing, suspending, or revoking eligibility of individuals for a HSPD-12 PIV credential to support physical or logical access to VA and federally controlled facilities and/or information systems (reference n).

f. VA shall establish authoritative systems/solutions/services for VA ICAM functions and promote flexible, scalable and interchangeable solutions that work across different agencies per OMB M-19-17 (reference i).

(1) Assurance Levels and System Digital Identity Risk Assessments (DIRA)

(a) VA shall utilize a system DIRA process to determine system assurance levels, in accordance with NIST SP 800-63. For each VA system, VA ISOs shall implement a DIRA to determine the appropriate Identity Assurance Level (IAL), Authenticator Assurance Level (AAL) and Federation Assurance Level (FAL) for their system. IAL refers to the identity proofing process. AAL refers to the authentication process. FAL refers to the assertion protocol the federation uses to communicate authentication and attribute information (if applicable). More details related to ISOs and system DIRAs can be located in the VA Directive and Handbook 6500.

(b) The system DIRA 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 system.

(c) These categories provide flexibility in choosing identity solutions and increase the ability to include privacy-enhancing techniques as fundamental elements of identity systems at any assurance level.

i VA ISOs must complete a DIRA for IAL and AAL on their systems.

ii VA ISOs must complete a DIRA for federated systems to determine the FAL (reference j). FAL refers to the strength of an assertion in a federated environment used to communicate authentication and attribute information to a relying party (RP).

iii VA shall evaluate each of the assurance levels separately.

iv VA's system DIRA process shall comply with the NIST SP 800-63.

v VA will monitor and manage the system DIRA process and its alignment to the latest OMB and NIST guidelines.

vi VA will provide guidance to various program offices to comply with standards stated in this Directive.

(2) Identity Proofing and Management.

(a) Users requesting access to VA information systems shall agree to adhere to ICAM identity assurance standards (reference h) before issuing electronic credentials.

(b) The identity proofing process shall comply with the VA Directive and Handbook 6500.

(c) For internal users, the identity proofing process shall also comply with VA Directive and Handbook 0735 HSPD-12 Program and VA Directive and Handbook 0710 Personnel Security and Suitability Program.

(d) The identity proofing process and requirements are based on the assurance levels defined in the system DIRA process. The process verifies all claimed identities before issuing VA electronic credentials, the initial grant of access, or provisioning of access rights.

(e) VA shall utilize remote identity proofing as an alternative to in-person identity proofing for external users, where feasible, for issuing credentials in accordance with the latest version of NIST guidelines and VA ICAM policies, VA Directive and Handbook 6500 security control policies and Federal policies.

(f) VA shall adopt a unique identifier for digital identities and logical access in accordance with NIST SP 800-63A and tailored to VA's needs by VA Memo, Person Identity Authoritative Data Source Selection (VAIQ 7836410).

(g) VA shall leverage existing credentials and identity federations that align with NIST and FICAM requirements and satisfy VA's accepted risk level to replace the issuance of new user credentials for external Federal Agency users. VA shall accept these approved identity and authentication assertions in accordance with VA Directive and

Handbook 6500, VA Directive and Handbook 0710 and Information Security KS security control requirements.

(h) VA shall limit the collection of personally identifiable information (PII) for establishing identity to what is legally authorized and necessary. Once collected, PII shall be protected and encrypted in states of rest, transit and use as required by the VA Enterprise Privacy Program guidance in VA Directive 6502.

(i) VA shall establish processes to allow individuals to bind, update, use and disassociate non-Government furnished authenticators to their digital identity.

(j) VA shall manage the digital identity lifecycle of VA devices, NPEs and automated technologies, in addition to all other VA digital identities.

(k) VA authoritative sources for attributes utilized in identity proofing events shall establish privacy-enhanced data validation Application Programming Interfaces (API) for public and private sector access based on consumer content.

(l) VA shall use Federal or commercial shared services to deliver identity assurance and authentication services to the public in alignment with ICAM guidelines.

(m) VA shall, in compliance with Executive Order 13988, ensure every person be treated with respect and dignity and should be able to live without fear, no matter who they are or whom they love. Identity Proofing must be accomplished in accordance with Federal healthcare laws (attributes to have been verified in person or remotely using the procedures given in NIST SP 800-63A) and this requires the legal recorded name and associated documents to be used for proofing. Once Identity Proofing has been completed, personal and systematic transactions should ensure the use of the customer’s preferred names.

(3) Electronic Credentials.

(a) VA shall manage electronic credentials to ensure they are bound to 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 include lifecycle management of the electronic credentials.

(b) VA shall use PIV credentials as the primary means of identification and authentication for access to VA systems and facilities.

(c) VA shall use Derived Credentials for VA employees, contractors and other enterprise users (where applicable in accordance with OPM requirements) and to enable the acceptance of Derived Credentials by applications and devices (reference n). Derived PIV Credentials are not applicable to PIV-I credentials and may only be derived from valid PIV credentials.

(d) VA shall implement processes to manage access control, including revoking access privileges and revoking or destroying credentials when no longer authorized. This is necessary to prevent unauthorized access to information systems when the employee or contractor separates from the VA, or the credential has been lost (reference n).

(e) VA shall ensure the use of the PIV credential for physical access to VA facilities and secured areas is implemented in accordance with DHS published The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard and NIST SP 800-116 Guidelines for the Use of PIV Credentials in Facility Access.

(f) VA shall establish capabilities aligned to FICAM Architecture and DHS Continuous Diagnostics and Mitigation (CDM) requirements that enable the continuous vetting and evaluation of the suitability of personnel subject to HSPD-12.

(g) The VA shall establish and update a Master User Record (MUR) according to the DHS CDM Memorandum of Agreement to provide data to the Agency and Federal CDM Dashboards.

(h) VA must accept third-party identity credentials issued by other Federal agencies and external, commercial Credential Service Providers for purposes of accessing VA resources when appropriate. Identity credentials accepted by VA shall align with published Federal mandates and FICAM to meet at least one of the following criteria:

i Issued by the Federal Government;

ii Cross-certified by the Federal Bridge; or

iii Issued by a third-party identity credential provider in accordance with the latest version of NIST guidelines and Federal Chief Information Officers Council procedures as required by OMB.

(i) All VA-issued digital credentials must meet Federal standards (including phishing-resistant multifactor authentication [MFA] per OMB M-22-09) and adhere to latest the VA policies (please refer to VA Directive and Handbook 0735 HSPD-12 Program).

(j) In support of privilege management, the VA shall implement a Privileged Access Management (PAM) program 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.

(k) Enterprise access privileges shall be associated with a vetted identity and reviewed periodically throughout the lifecycle of the identity. The frequency of these reviews will be based on the risk associated with the access privileges.

(l) VA, where appropriate, captures, uses and accepts biometric data to enable biometric logon, biometric unlock of Authenticators and non-repudiation (reference m and reference n).

(4) Use of Electronic Credentials as Electronic Signatures.

(a) VA accepts electronic signatures as equivalent to traditional handwritten signatures, also called wet signatures (reference i). Such acceptance shall not limit users from conducting transactions in a non-electronic form.

(b) VA shall implement an electronic credential signature capability. The capability is considered a form of electronic signature that attaches encrypted data from the credential to the document electronically. 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.

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

(d) Use of a digital or electronic signature as legally binding requires 1) authentication of the signer 2) verifying the integrity of the record 3) a positive decision or action by the individual indicating to the system or an observer their intent to execute the signature as legally binding.

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

(f) 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 the 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 verification of credentials provided at the moment of signature, date/time of signature and user's name.

(g) Applications utilizing electronic signatures require data integrity mechanisms that notate changes, errors or corruption in data upon signature of the document.

(h) A user generated personal identification number (PIN) will be used to unlock the signing credential for authenticators with an AAL of 2 or higher (reference h).

(5) Access Management.

(a) VA shall grant persons and NPEs access to the information and information systems commensurate with the risk inherent in the access and the assurance level of the user's identity or credential used to access the information and information systems.

(b) VA shall implement standard methods for managing access to information, information systems and to available VA physical resources. Those individuals requiring access to Protected Health Information (PHI) are required to complete Health Insurance Portability and Accountability Act training in accordance with Veteran Health Administration (VHA) Directive 1907.08, Health Care Information Security Policy and Requirements.

(c) VA shall use PIV credentials, where applicable, for physical access to facilities in accordance with NIST SP 800-116-1, Guidelines for the Use of PIV Credentials in Facility Access (hereby referred to as NIST SP 800-116).

(d) VA shall implement access control processes to authorize and revoke access (logical and physical) privileges in a timely manner as defined per the OIT standards in VA 6500 Handbook, VA 6500 Directive and Information Security KS (reference k, l and m).

(e) VA shall require all users with physical or logical access to VA facilities or systems to comply with HSPD-12 and FIPS 201 (reference f).

(f) VA shall leverage policies mentioned in this Directive in collaboration with VA Directive and Handbook 6500 (reference j and k) (e.g., for Account and/or Password Management). 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 Cybersecurity Program Guidance (VA Directive, Handbook 6500 and KS) issued by OIT.

(6) Zero Trust Architecture (ZTA).

(a) VA shall, in accordance with Executive Order 14028, work toward the implementation of an enterprise-wide ZTA. VA's implementation of ZTA shall also coincide with the migration to cloud technology. The cloud initiatives shall comply with ZTA guidelines.

(b) VA shall implement a Zero Trust (ZT) strategy emphasizing stronger enterprise identity and access management controls, including phishing-resistant MFA. Without secure, enterprise-managed identity systems, adversaries can take over user accounts and gain a foothold in an agency to steal data or launch attacks (per OMB M-22-09 [reference u]).

(c) In accordance OMB M-22-09, VA shall ensure data is encrypted at rest, in transit and in use, where feasible, as determined by VA Directive and Handbook 6500 security controls.

(d) VA shall leverage the NIST SP 800-207 document (reference s) to ensure the implementation of VA's ZTA embodies ZT principles completely and with all best practices in mind.

3. RESPONSIBILITIES.

a. **Office of Information Technology Principal Deputy Assistant Secretary for Information and Technology or designee** shall:

(1) Serve as ICAM business owner;

(2) Serve as the business sponsor liaison for ICAM-related activities at VA;

(3) Serve as ISO for VA ICAM technologies and solutions;

(4) Ensure the utilization of the VA defined unique ID (Integration Control Number [ICN] for association and Security Identifier [SecID] for logical access as referenced in VAIQ 7836410);

(5) Collaborate with Veterans Experience Office to collect, define and oversee the process for documenting and providing business requirements for external ICAM activities at VA to OIT;

(6) Collaborate and follow guidelines provided by external entities such as General Service Administration (GSA), OMB, DHS, CISA, NIST and other key stakeholders;

(7) Establish an agency-wide ICAM office, team or other governance structure to maintain and guide ICAM processes;

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

(9) Define and maintain a single comprehensive ICAM policy and process, consistent with agency authorities and operational mission needs;

(10) Develop and maintain the VA’s ICAM technology solution roadmap, consistent with VA authorities and operational mission needs. The technology solution roadmap should encompass the VA’s entire enterprise and align with the Government-wide FICAM Architecture, ZTA and CDM requirements;

(11) Provide stewardship for the ICAM strategic plan;

(12) Define, prioritize and ensure implementation of VA enterprise-wide ICAM Business Requirements in collaboration with business stakeholders that defines the ICAM requirements for Veterans and VA users;

(13) Manage, operate and maintain enterprise-level IAM services and technology for VA, including the USAccess PIV credentialing system which is a shared service operated by GSA;

(14) Define the ICAM architecture for VA;

(15) Collaborate with Office of Acquisition, Logistics and Construction (OALC) to procure digital certificates for identification and authentication of Federal enterprise identities utilizing Best in Class and Tier 2 contract vehicles, or federally provided shared services;

(16) Coordinate VA-wide ICAM communications;

(17) Review, approve and manage all assurance determinations from system DIRAs;

(18) Establish ZTA and implement ZT practices as related to ICAM for VA enterprise-wide;

(19) Establish interoperability with approved electronic credentials issued by electronic credential providers, where permitted;

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

(21) Require MFA for logical access to internal VA network and information systems by VA users;

(22) Coordinate with the Office of Human Resources and Administration/ Operations, Security, and Preparedness (HRA/OSP) in the development of policy as it relates to implementing the technical solutions to conduct the VA's HSPD-12, PACS and Personnel Security mission;

(23) Provide technical support when an office requests assistance in the installation of a PACS connected to the VA network as an OIT special purpose system deployment;

(24) Assist VA programs and offices with their PACS when requested for coordination of OIT efforts to provide the infrastructure connectivity that complies with HSPD-12 technical and interoperability standards;

(25) Establish OIT policies for standard operating procedures and implementation guidance that aligns with the ICAM policies as defined in this Directive to clearly state IT processes, roles and responsibilities to maintain ICAM services;

(26) Develop policy as it relates to implementing the technical solutions to carry out the VA ICAM mission;

(27) Develop and maintain ICAM related security and privacy controls on the Information Security KS, as VA's centralized repository to provide cybersecurity and privacy policies, procedures and guidance; and

(28) Ensure compliance with the responsibilities set forth in section 3.g. of this Directive.

b. **Under Secretaries, Assistant Secretaries, Chief Acquisition Officer, Chief Financial Officer and Other Key Officials** shall:

(1) Support efforts to adhere to ICAM requirements across their respective offices and foster accountability at all levels of the organization;

(2) Comply with and enforce the policies, procedures and guidance established in this Directive and any associated policies;

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

(4) Require MFA for logical access to internal VA network and information systems by VA users;

(5) Ensure contracts comply with the Federal Acquisitions Regulations (FAR), VA Acquisitions Regulations (VAAR) and VA Acquisition Manual (VAAM) as it relates to HSPD-12 and FIPS 201 for affected contractor personnel based on OPM requirements. The VA employee(s), as indicated by VA Handbook 0710 (reference o) and VA Handbook 6500.6 (reference l), will

be responsible for managing contractor access, PIV compliance per VA Handbook 0735, the stewardship of IT assets provided as government-furnished equipment (GFE), in accordance with VA Handbook 7002 Logistics Management Policy and elevated privilege tokens in accordance with VA and Federal standards;

(6) Require Contracting Officers (CO) to include clauses in contracts, as appropriate, that address PIV requirements for contractor personnel per the FAR and VAAR;

(7) Coordinate with OIT to achieve and maintain compliance with ICAM-related policies and requirements; and

(8) Ensure review of legal advice as set forth in section 3.g. of this directive.

c. **Assistant Secretary, Office of Enterprise Integration** shall:

(1) Assist in reforming operations to reflect leading practices leveraging technology and process changes and drive successful outcomes for enterprise initiatives at VA;

(2) Conducts forward-thinking strategic planning to address long-range issues; and ensures integration of business requirements aligns with the planning and execution activities of the Department's programs and initiatives at VA;

(3) Support efforts to adhere to ICAM requirements across their respective offices and foster accountability at all levels of the organization;

(4) Comply with the policies, procedures and guidance established in this Directive and any associated policies;

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

(6) Participate in steering committees, governance boards and integrated project teams, as requested by OIT;

(7) Coordinate with OIT to achieve and maintain compliance with ICAM-related policies and requirements; and

(8) Ensure review of legal advice as set forth in section 3.g. of this directive.

d. **Chief, Operations, Security and Preparedness, HRA/OSP** shall:

(1) Serve as the business owner for VA's PACS program;

(2) Coordinate with stakeholders to discuss business requirements, key decisions, risks and issues through meetings and forums (e.g., Identity and Access Management [IAM] Working Integrated Product Team [WIPT] meetings [reference s]);

(3) Ensure VA's PACS program effectively compliments VA's logical access tools and practices, contributing to the effectiveness of VA's overall ICAM program;

(4) Support the identification of enterprise PACS requirements to integrate with VA architecture and systems;

(5) Assist facility physical security specialists with PACS policies and guidance;

(6) Coordinate with OIT in the development of policy as it relates to implementing the technical solutions to conduct the HRA/OSP VA's HSPD-12 (VA Handbook and Directive 0735), PACS and Personnel Security mission; and

(7) Ensure review of legal advice as set forth in section 3.g. of this directive.

e. **Chief, Veterans Experience Officer** shall:

(1) Coordinate ICAM solutions based on Veteran-focused designs and industry best practices while aligning VA services with the Secretary's priorities;

(2) Deliver easy and effective Veteran experiences through all communications channels and technology mechanisms;

(3) Collaborate with OIT to collect, define and oversee the process for documenting and providing business requirements for ICAM activities for the Veterans;

(4) Comply with the policies, procedures and guidance established in this directive and any associated VA directives, handbooks and policies;

(5) Support efforts to adhere to ICAM requirements across their respective offices and foster accountability at all levels of the organization;

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

(7) Coordinate and participate in steering committees, governance boards and integrated project teams, as requested by ICAM PMO and OIT;

(8) Coordinate with OIT to achieve and maintain compliance with ICAM-related policies and requirements; and

(9) Ensure review of legal advice as set forth in section 3.g. of this directive.

f. **The Inspector General** shall:

(1) Conduct audits of ICAM processes and systems;

(2) Conduct investigations of complaints and referrals of violations; and

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

g. **The General Counsel** shall provide review of and advice on legal issues related to ICAM policies and procedures.

4. REFERENCES.

a. 44 U.S.C. §§ 3551-3558, Federal Information Security Modernization Act (FISMA); December 2014.

b. 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.

c. Committee on National Security Systems (CNSS) Instruction No. 4009; March 2022.

d. GSA Federal Identity, Credential and Access Management (FICAM) Architecture; January 2021.

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

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

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

h. NIST SP 800-63-3, Digital Identity Guidelines; June 2017.

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

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

k. VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program; February 2021.

l. VA Handbook 6500.6, Contract Security; March 2010.

m. Information Security Knowledge Service, VA SharePoint site; January 2021.

n. VA Directive and Handbook 0735, Homeland Security Presidential Directive 12 Program; March 2014.

o. VA Directive and Handbook 0710, Personnel Security and Suitability Program; May 2016.

p. VA Directive and Handbook 0730, Security and Law Enforcement; August 2000.

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

r. Department of Homeland Security, The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard; updated 2021.

s. IAM WIPT Charter, VA ICAM PMO SharePoint; August 2023.

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

u. Presidential Cybersecurity Executive Order 14028, Improving the Nation's Cybersecurity; May 2021.

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

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

x. Presidential Executive Order 14058, Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government; December 2021.

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

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

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

bb. VA Memo, VA Person Identity Authoritative Data Source Selection (VAIQ 7836410); February 2018.

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

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

ee. NIST Cybersecurity Framework v2.0, Framework for Improving Critical Infrastructure Cybersecurity; February 2024.

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

gg. VA Directive 7002, Logistics Management Policy; January 2020.

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

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

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

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 201-3

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 NIST SP 800-63, this was referred to as a token. SOURCE: NIST SP 800-63-3

f. **Authenticator Assurance Level:** A category describing the strength of the authentication process. SOURCE: NIST SP 1800-17b

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

h. **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. SOURCE: NIST SP 800-53-5

i. **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

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

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

l. **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

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

n. **Derived PIV Credential:** The Derived PIV Credential is a Derived PIV Authentication certificate, which is an X. 509 public key certificate that has been issued in accordance with the requirements of this document and the X. 509 Certificate Policy for the U.S. Federal PKI Common Policy Framework; (SOURCE: NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials. SOURCE: VA Directive 0735

o. **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

p. **Digital Signature:** An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection and non-repudiation, but not confidentiality protection. SOURCE NIST SP 800-63-3

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

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

s. **Federation Assurance Level:** A category describing the assertion protocol used by the federation to communicate authentication and attribute information (if applicable) to a relying party. SOURCE: NIST SP 1800-17b

t. **Federal Identity, Credential and Access Management:** the government-wide approach to implementing the tools, policies and systems that an agency uses to manage, monitor and secure access to protected resources. SOURCE: GSA Government IT Initiatives

u. **Identity:** A unique representation of a subject (person, device, non-person entity, 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

v. **Identity Assurance Level:** A category that conveys the degree of confidence that the applicant's claimed identity is their real identity. SOURCE: NIST SP 1800-17b

w. **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

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

y. **Information System 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 800-161-1

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

aa. **Integrity:** Guarding against improper information, modification or destruction and include ensuring information non-repudiation and authenticity. SOURCE: 44 U.S.C. § 3552

bb. **Logical Access:** An individual's ability to access one or more computer system resources such as a workstation, network, application, or database. SOURCE: NIST SP 800-53-5

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

dd. **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

ee. **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 800-53-5

ff. **Physical Access Control System:** An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules. SOURCE: NIST SP 800-53-5

gg. **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 and FICAM Playbooks

hh. **Remote Proofing:** Identity proofing that occurs outside the physical presence of a VA appointed representative. SOURCE: VA Handbook 6500

ii. **Special Purpose System:** A network-connected, nonmedical systems that do not have the standard VA baseline configuration. These systems play a vital role in supporting VA facilities organizational mission. Special purpose systems are involved in maintaining and supporting the infrastructure, safety and/or security systems and environmental controls at VA facilities. Source: VA Notice 20-09 - Interim Policy on Complying with the Federal Information Technology Acquisition Reform Act (FITARA)

jj. **Trusted:** A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly and impartially, along with assurance that the entity and its identifier are genuine. SOURCE: NIST SP 800-152

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

ll. **Verify:** The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed. SOURCE: FIPS 201-3

mm. **Vet:** The process of examination and evaluation, including background check activities; results in establishing verified credentials and attributes. SOURCE: FICAM Roadmap and FICAM Playbooks

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

6. VA TERMS & DEFINITIONS.

VA Terms	VA Definitions
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 (ISSO)	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 (ISO)	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 the monitoring of 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).