DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

VA Needs to Improve Governance of Identity, Credential, and Access Management Processes

REVIEW | REPORT #22-00210-191 | AUGUST 3, 2022

MISSION

The mission of the Office of Inspector General is to serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

FOR MORE
VA OIG REPORTS
CLICK HERE

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

Identity, credential, and access management (ICAM) is a set of tools, policies, and systems that an agency uses to ensure the right individual has access to the right resource, at the right time, for the right reason in support of federal business objectives.[1] Agencies use ICAM to unify information technology services and improve physical access control, information security, and decision-making.

In February 2021, the VA Office of Inspector General (OIG) received a hotline complaint concerning VA's governance of its ICAM program. Specifically, the complainant alleged that since 2016, the Office of the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness (HRA/OSP) and the Office of Information and Technology (OIT) have disagreed regarding roles and responsibilities for the ICAM program and VA Directive 6510.[2] The lack of cooperation between these entities has contributed to VA not being able to effectively comply with Office of Management and Budget (OMB) ICAM policy.[3] Based on this allegation, the OIG conducted this review to determine whether VA is effectively governing its ICAM program as required by OMB.

OMB ICAM policy has four requirements that federal agencies must follow:[4]

1. Establish an agencywide ICAM office, team, or other governance structure to effectively enforce ICAM efforts. In addition, the chief operating officers or the agency equivalents must ensure regular coordination among agency leaders to implement, manage, and maintain the ICAM policies, processes, and technologies.
2. Define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap.
3. Outline performance expectations for security and privacy risk management.
4. Incorporate digital identity risk management into existing federal processes as outlined in the National Institute of Standards and Technology (NIST) guidelines.[5]

[1] Federal Identity, Credential, and Access Management Playbooks, *Federal ICAM Architecture Introduction*, accessed March 11, 2021, https://playbooks.idmanagement.gov/arch/#what-is-icam.

[2] VA Directive 6510, *VA Identity and Access Management*, January 15, 2016.

[3] OMB M-19-17, Memorandum for Heads of Executive Department and Agencies, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," May 21, 2019.

[4] OMB M-19-17.

[5] NIST, *Digital Identity Guidelines*, NIST Special Publication 800-63-3, June 2017.

What the Review Found

The OIG found that VA's ICAM program did not meet three of the four OMB governance requirements; therefore, VA did not effectively manage and coordinate its ICAM efforts.[6] Specifically, VA did not

- assign roles and responsibilities to effectively manage and coordinate ICAM efforts,
- implement a single comprehensive ICAM policy or meet goals established in its technology solutions roadmap for fiscal years (FY) 2020 and 2021, or
- implement updated NIST digital identity risk management requirements.

These issues occurred primarily because leaders of the different offices performing VA's ICAM functions have not agreed on how the program should be governed, creating an obstacle to implementing OMB's requirements. Without proper ICAM governance, VA is at risk of both restricting information from users who need it to perform their job functions and leaving information vulnerable to improper use. VA also risks being unable to mitigate the OIG's Federal Information Security Modernization Act (FISMA) audit findings of deficiencies in ICAM processes.

VA Did Not Effectively Manage and Coordinate ICAM Efforts

The OIG found the roles and responsibilities assigned to VA offices do not lead to effective management and coordination of ICAM efforts since they have not been revised to comply with the latest OMB policy issued in May 2019. OMB requires VA to designate an integrated office, team, or structure to effectively govern and enforce ICAM efforts.[7] The OIG found that, through memos issued in 2011, 2012, and 2014, VA designated an integrated office, team, or governance structure for ICAM. In 2011, a former assistant secretary for OIT issued a memo designating the deputy assistant secretary for information security as the business sponsor for identity and access management. This included assigning responsibility for coordinating enterprise-wide identity access management activities and developing VA's transition plan for alignment with federal ICAM segment architecture. In 2012, VA designated OSP to lead VA's identity management program, and in 2014, OSP was designated to lead the personnel security and suitability programs.[8] In 2016, the business sponsor responsibilities for VA identity access management were informally transferred from OIT's Office of Information Security to OSP. However, this transfer was not approved by VA senior leaders, creating confusion and disagreement between

[6] OMB M-19-17.

[7] OMB M-19-17.

[8] VA Secretary memo, "Elimination of the Position of Assistant Secretary for Operations, Security, and Preparedness (OSP) and Realignment of OSP Functions," September 14, 2018. In September 2018, OSP was combined with HRA to form HRA/OSP.

VA offices over roles and responsibilities for managing ICAM efforts. VA has not reassessed ICAM governance since the OMB memo was issued in 2019.

The OIG also found VA's ICAM policies are outdated and do not meet the OMB requirement that agencies define and maintain a single comprehensive policy, process, and technology solution roadmap.[9] All three directives and their accompanying handbooks outlining VA's ICAM policies had not been updated in accordance with VA's enterprise directives management procedures, which require that all permanent directives and handbooks be recertified within five years of issuance to ensure consistency with other enterprise directives and handbooks.[10] Specifically, VA Directive 6510 and its accompanying handbook were not updated because, for reasons detailed below, neither HRA/OSP nor OIT accepted ownership of the policy.[11] According to the Office of ICAM executive director and the HRA/OSP chief security officer, HRA/OSP has been in the process of updating VA directives 0735 and 0710 and their accompanying handbooks but was delayed due to changes in VA's credentialing process and updated federal guidance for personnel vetting.[12] According to the executive director, they expect to publish the updates for both directives and handbooks by the end of summer 2022.

VA developed an ICAM technology solutions roadmap meeting OMB requirements but did not meet the goals it established for FY 2020 to FY 2021. This occurred because of a lack of coordination between HRA/OSP and OIT on completing the goals. According to the Office of ICAM executive director, the roadmap goals relate to OIT job functions, and his staff did not have the technical expertise to complete them. OIT's former deputy assistant secretary, who is also the chief information security officer, said he knew of no coordination efforts between HRA/OSP and OIT to ensure the roadmap goals were being addressed and achieved.

VA Directive 6510 and its accompanying handbook require VA to comply with NIST's electronic authentication guidelines.[13] OMB requires agencies to implement NIST's digital identity guidelines, which supersede the electronic authentication guidelines and any successive versions.[14] However, VA did not incorporate digital identity risk management into its policy as

[9] VA Directive 6510and VA Handbook 6510, *VA Identity and Access Management*, January 15, 2016; VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, October 2015, and VA Handbook 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, March 2014; and VA Directive 0710, *Personnel Security and Suitability Program*, June 4, 2010, and VA Handbook 0710, *Personnel Security and Suitability Program,* May 2, 2016.

[10] VA Handbook 0999, *Enterprise Directives Management (EDM) Procedures*, August 1, 2019.

[11] VA Directive 6510; VA Handbook 6510.

[12] VA Directive 0735; VA Handbook 0735; VA Directive 0710; VA Handbook 0710.

[13] NIST, *Electronic Authentication Guideline*, NIST Special Publication 800-63-2, August 2013. Withdrawn and superseded by NIST Special Publication 800-63-3.

[14] OMB M-19-17.

outlined in NIST guidelines because HRA/OSP and OIT failed to take responsibility for updating the directive and handbook.

Disagreements over Roles and Responsibilities Prevented Effective Management

Federal guidance recommends agencies create a governing body to oversee ICAM projects and workstreams and align those services and management with the agency's mission.[15] HRA/OSP created an ICAM Executive Steering Committee and the original committee charter, dated January 2015, provided that unresolved issues would be elevated to a more senior decision authority. The committee is important because it governs VA ICAM business processes, projects, investments, initiatives, and activities. The review team evaluated minutes and supporting information from the committee's meetings from May 2019, after OMB's policy took effect, through October 2021, and found no indication that the committee acted to address issues affecting ICAM management or suggested elevating them to a higher decision authority.

Meanwhile, disagreements have interfered with the effective operation of VA's ICAM policies. According to the Office of ICAM executive director, who has been in place since August 2018, his staff does not possess the information technology and cybersecurity technical skill sets and IT systems experience needed to most effectively contribute as a partner with OIT in the management and oversight of VA's ICAM program. HRA/OSP's chief security officer, who has been in place since July 2020, stated their focus should be on personnel security, credentialing, and policy oversight. Both believe OIT should manage identity and access. However, OIT believes that ICAM ownership belongs to HRA/OSP. According to an Office of Information Security document titled "Resolving Confusion Over Responsibilities Within VA for Identity, Credential, and Access Management (ICAM)," provided by the Office of ICAM executive director, one of the roles informally transferred from OIT to OSP in 2016 as part of the identity and access management business sponsor role was ownership of the directive and handbook. As a result, there has been confusion and disagreements between HRA/OSP and OIT leaders on the specific ICAM roles and responsibilities to be performed by each office.

In February 2021, due to a lack of resources and technical expertise, the HRA/OSP chief security officer directed the Office of ICAM staff to stop updating VA Directive 6510 and its accompanying handbook. According to the chief security officer, transfer of responsibilities from OIT to OSP was never formalized through a directive or other agreement by VA senior leaders. At the time of this review, the directive and handbook assigned OIT as the responsible office for the contents of these policies. However, according to OIT's former deputy assistant secretary and

[15] Federal Identity, Credential, and Access Management Playbooks, *Program Governance and Leadership*, accessed on January 26, 2022, https://playbooks.idmanagement.gov/pm/governance/.

chief information security officer, ownership of the directive and handbook belongs to HRA/OSP and is not OIT's responsibility.

OMB also requires agency chief operating officers to ensure regular coordination to implement, manage, and maintain the agency's ICAM policies, processes, and technologies.[16] In VA, this responsibility falls on the deputy secretary. The OIG found that neither the deputy secretary nor his office has been involved in coordination of VA's ICAM efforts across the VA enterprise since OMB issued its memo in 2019, and thus has not resolved disagreements or clarified policies and roles to meet OMB's requirements.

VA Information Security Is at Risk

Identity governance and administration is the ability to manage and reduce the risk that comes with excessive or unnecessary user access to applications, systems, and data. The OIG has annually demonstrated in its FISMA audits VA's weaknesses in implementing proper monitoring and governance controls in determining whether users have the right access to perform their job functions. Until VA issues a single comprehensive policy, updates its directives and handbooks, and clearly defines roles and responsibilities, it will not comply with OMB requirements.

VA information systems security officers rely on internal guidance such as VA Directive 6510 for assessing security controls related to identity and access management. VA Directive 6510 and its accompanying handbook have not been updated to include the digital identity risk management requirements established by NIST.[17] Consequently, the guidance in VA's Enterprise Mission Assurance Support Service, where VA's risk management framework process is performed and documented, was not updated to include such requirements. As a result, VA relied on an outdated policy when assessing security controls and is not meeting requirements established by NIST.[18]

What the OIG Recommended

The OIG recommended the VA deputy secretary designate roles and responsibilities for all program offices involved in VA's ICAM program. The deputy secretary should also provide and ensure appropriate oversight and coordination between designated program offices to implement a comprehensive ICAM policy. The OIG also recommended that the assistant secretary for information and technology update and publish the VA directive and handbook associated with identity and access management to include current NIST requirements. The OIG further recommended that the assistant secretary for HRA/OSP update and publish VA directives and handbooks associated with the Homeland Security Presidential Directive 12 Program and VA's

[16] OMB M-19-17.

[17] NIST Special Publication 800-63-3.

[18] NIST Special Publication 800-63-3.

personnel security and suitability program, as required by VA's enterprise directives management procedures.[19]

VA Comments and OIG Response

VA's deputy secretary said VA concurs with the OIG's findings and recommendations. In addition, the deputy secretary, the assistant secretary for OIT, and the assistant secretary for HRA/OSP each concurred with the recommendations directed to them. The OIG considers the submitted corrective action plans acceptable and will monitor VA's progress in meeting the intent of the recommendations. The OIG recognizes the corrective action plan for updating and publishing the VA directive and handbook associated with identity and access management is dependent on OIT being designated the responsible policy office. The OIG will close the recommendations when it receives sufficient evidence that appropriate remedial measures have been taken. Appendix D includes the full text of the deputy secretary's comments.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

[19] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. This directive mandates a federal standard for secure and reliable forms of identification.

Contents

Abbreviations

FISMA	Federal Information Security Modernization Act
FY	fiscal year
HRA	Office of Human Resources and Administration
ICAM	identity, credential, and access management
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OSP	Office of Operations, Security, and Preparedness
VASI	VA system inventory

Introduction

Identity, credential, and access management (ICAM) is a set of tools, policies, and systems that an agency uses to ensure the right individual has access to the right resource, at the right time, for the right reason in support of federal business objectives.[20] Agencies use ICAM to unify their information technology services, improve physical access control, and improve information security and decision-making. In February 2021, the VA Office of Inspector General (OIG) received a hotline complaint concerning VA's governance of its ICAM program. Specifically, the complainant alleged that since 2016, there has been a lack of agreement between the Office of the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness (HRA/OSP) and the Office of Information and Technology (OIT) regarding roles and responsibilities for the ICAM program and VA Directive 6510 which has contributed to VA not being able to effectively comply with Office of Management and Budget (OMB) policy.[21] Based on this allegation, the OIG conducted this review to determine whether VA is effectively governing its ICAM program as required by OMB.

Identity, Credential, and Access Management

The Federal Information Security Modernization Act (FISMA) of 2014 provides a broad framework for ensuring the effectiveness of federal information systems and calls for the development and implementation of continuous monitoring oversight mechanisms.[22] The federal ICAM architecture was created in 2009 to provide a common framework for federal agencies. The framework helps agencies plan their ICAM programs and provides a solution roadmap. It focuses on enterprise identity processes, practices, policies, and information security disciplines.[23] The framework also provides collaboration opportunities and guidance on information technology (IT) policy, standards, implementation, and architecture. Figure 1 provides a high-level overview of ICAM and its practice areas and supporting elements.

[20] Federal Identity, Credential, and Access Management Playbooks, *Federal ICAM Architecture Introduction*, accessed March 11, 2021, https://playbooks.idmanagement.gov/arch/#what-is-icam.

[21] OMB M-19-17, Memorandum for Heads of Executive Department and Agencies, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," May 21, 2019.

[22] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 3551.

[23] OMB M-19-17. A federal enterprise identity is the unique representation of an employee, contractor, or enterprise user, which could be a mission or business partner, or even a device or technology managed by a federal agency to achieve its mission and business objectives.

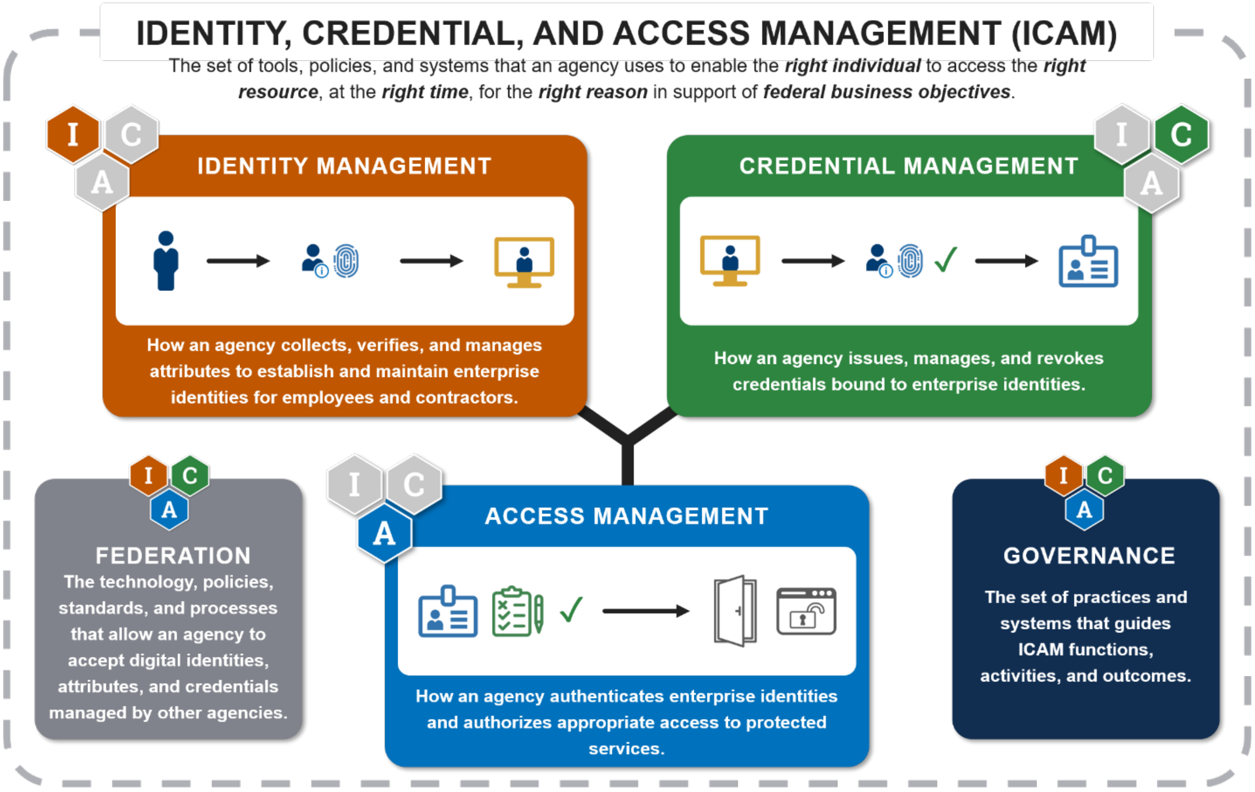
IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)
The set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives.
I C A
IDENTITY MANAGEMENT
How an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors.
CREDENTIAL MANAGEMENT
How an agency issues, manages, and revokes credentials bound to enterprise identities.
FEDERATION
The technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.
ACCESS MANAGEMENT
How an agency authenticates enterprise identities and authorizes appropriate access to protected services.
GOVERNANCE
The set of practices and systems that guides ICAM functions, activities, and outcomes.

Figure 1. *ICAM overview.*
Source: https://playbooks.idmanagement.gov/arch/#what-is-icam.

Office of Management and Budget Policy

OMB sets the federal government's ICAM policy. According to its memo, to ensure secure and efficient operations, agencies of the federal government must be able to identify, credential, monitor, and manage users of federal resources, including information, information systems, facilities, and secured areas.[24] How agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security and delivery of their services, as well as individuals' privacy. The memo establishes ICAM governance requirements as follows:

- Agencies shall establish an agencywide ICAM office, team, or other structure to effectively govern and enforce ICAM efforts. In addition, the chief operating officers or the agency equivalents must ensure regular coordination among agency leaders to implement, manage, and maintain the ICAM policies, processes, and technologies.
- Agencies shall define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap.

[24] OMB M-19-17.

- Agencies shall outline performance expectations for security and privacy risk management.
- Agencies shall incorporate digital identity risk management into existing federal processes as outlined in the National Institute of Standards and Technology (NIST) guidelines.[25]

Digital Identity Risk Management

According to NIST guidelines, digital identity is an individual's online persona, although the exact definition is widely debated internationally. Without context, it is difficult to land on a single definition that satisfies all. Using digital identity as a legal identity makes the issue even more complex. Proving individuals are who they say they are—especially remotely, via a digital service—is fraught with opportunities for an attacker to successfully impersonate someone. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the individual in all contexts. In other words, an individual can access a digital service without revealing his or her real-life identity.

Identity proofing establishes that individuals are who they claim to be. Digital authentication establishes that someone trying to access a digital service is in control of one or more valid authenticators associated with that individual's digital identity. Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individuals over an open network to access digital government services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks. NIST digital identity guidelines provide technical requirements for federal agencies implementing digital identity services.[26]

NIST defines the requirements for identity proofing and authentication of users interacting with government IT systems over open networks. In addition, NIST defines technical requirements for identity proofing, authenticators, management processes, authentication protocols, federation, and related assertions. As a part of digital identity risk management, agencies are required to select identity, authenticator, and federation assurance levels, and assess them separately. The separation of these categories provides greater flexibility, more user convenience, enhanced privacy, and reduced risk. See appendix A for further details.

VA's ICAM Structure

VA's ICAM program is predominantly governed by the Office of the Assistant Secretary for Human Resources and Administration/Operations, Security, and Preparedness (HRA/OSP) with

[25] NIST, *Digital Identity Guidelines*, NIST Special Publication 800-63-3, June 2017.

[26] NIST Special Publication 800-63-3.

assistance from OIT.[27] HRA/OSP is responsible for managing VA's national security portfolio and comprises five program offices to provide for emergency management and resilience; identity, credential, and access management; resource management; security and law enforcement; and a VA chief of police. In addition, HRA/OSP leads the development and oversight of human capital strategies, security, and preparedness policies and capabilities.

VA's Office of ICAM, which is organized under HRA/OSP, is responsible for central coordination and oversight of VA's personnel security and identity management infrastructure and enforcing VA compliance with federal statutes, regulations, and policies. OIT manages VA's cybersecurity and privacy programs and delivers enterprise-wide strategy, policy, governance, and network defense through collaboration with VA business units. See appendix A for VA's policies and procedures on ICAM.

Office of Identity, Credential, and Access Management

The Office of ICAM collaborates with VA's Veterans Experience Office as the executive sponsors for identity management practices and solutions. The Office of ICAM has the following four functional responsibilities:

- Access and identity management
- Credential management
- Personnel security, including fingerprinting, adjudication, and ownership of VA Centralized Adjudication and Background Investigation System
- Personnel security adjudication, including background investigations

Figure 2 illustrates the HRA/OSP organization and where the Office of ICAM fits into the structure.

[27] VA Secretary memo, "Elimination of the Position of Assistant Secretary for Operations, Security, and Preparedness (OSP) and Realignment of OSP Functions," September 14, 2018.

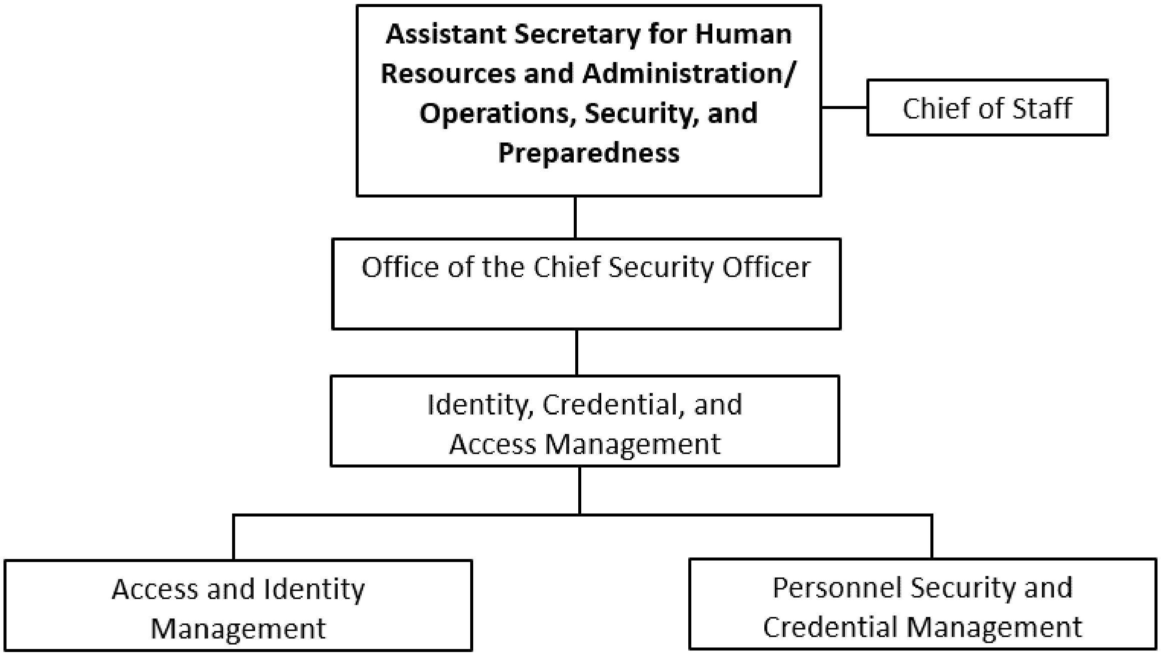
Assistant Secretary for Human Resources and Administration/ Operations, Security, and Preparedness
Chief of Staff
Office of the Chief Security Officer
Identity, Credential, and Access Management
Access and Identity Management
Personnel Security and Credential Management

Figure 2. *HRA/OSP organizational chart.*
Source: VA 2020 functional organization manual.

Office of Information and Technology

OIT manages the technology components of ICAM functions and VA's risk management framework controls through two divisions, (1) the Office of Information Security and (2) Development, Security, and Operations. OIT performs the following functions specific to ICAM:

- Cybersecurity Technology and Metrics Identity and Access Management Security (under the Office of Information Security) ensures VA's ICAM services comply with federal requirements and fulfill cybersecurity controls.
- Development, Security, and Operations performs business operations services such as projects and implementation management activities in support of ICAM.

Figure 3 illustrates the OIT organization.

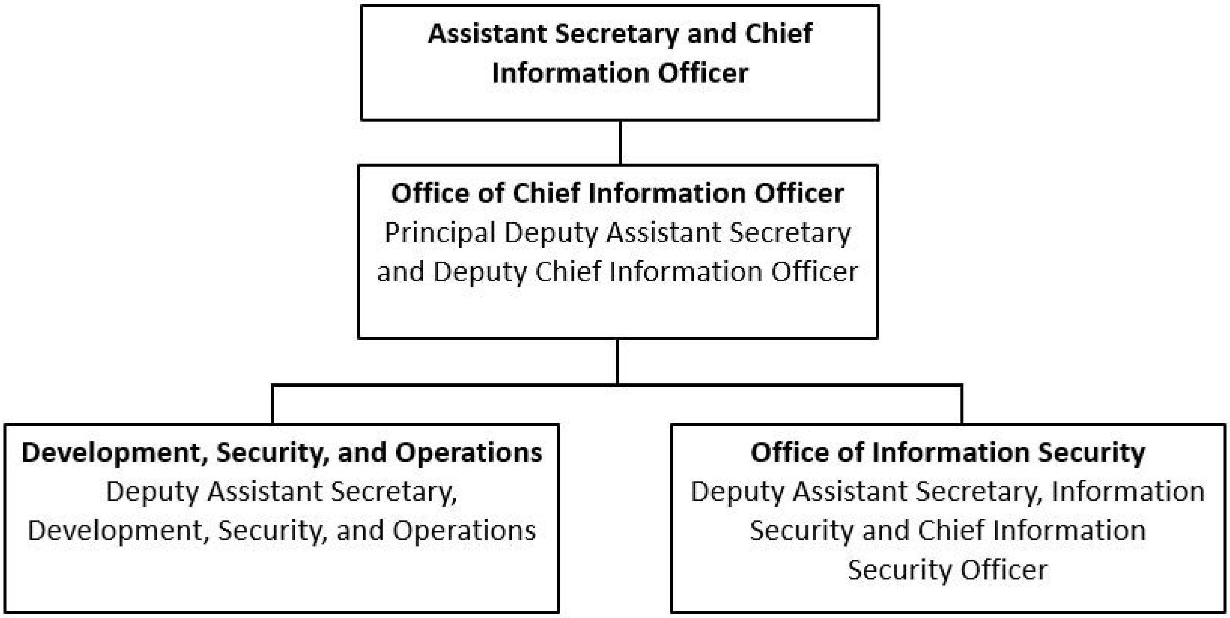
Assistant Secretary and Chief Information Officer
Office of Chief Information Officer
Principal Deputy Assistant Secretary and Deputy Chief Information Officer
Development, Security, and Operations
Deputy Assistant Secretary, Development, Security, and Operations
Office of Information Security
Deputy Assistant Secretary, Information Security and Chief Information Security Officer

Figure 3. *OIT organizational chart.*
Source: VA OIG analysis of "The Organization," VA OIT, accessed February 28, 2022, https://www.oit.va.gov/about/index.cfm.

Results and Recommendations

Finding: VA's Governance of ICAM Does Not Meet OMB Policy

The OIG found VA's ICAM program does not meet three of the four OMB governance requirements.[28] Specifically, VA did not

- assign roles and responsibilities to effectively manage and coordinate ICAM efforts,
- implement a single comprehensive ICAM policy, and meet goals established in its technology solutions roadmap for fiscal years (FY) 2020 and 2021, or
- implement updated NIST digital identity risk management requirements.

These issues occurred primarily because VA's ICAM functions are performed by several offices whose leaders have not agreed on how it should be governed, creating an obstacle to implementing OMB's requirements. Without proper ICAM governance, VA is at risk of restricting information from users who need it to perform their job functions, and leaving information vulnerable to improper use. VA also risks being unable to mitigate FISMA audit findings related to deficiencies in its ICAM processes.

Although VA maintains policies for individual elements of ICAM, including identity and access management, credentialing, and personnel security, these policies do not meet OMB's requirements for a single, comprehensive policy. The identity and access management policy does not incorporate digital identity risk management into existing processes as outlined in the most recent NIST publications, including the selection of assurance levels commensurate with the risk to digital service offerings.[29] Several different offices have responsibility for managing various elements of the ICAM program, and they have not agreed on which office should perform which tasks. For example, HRA/OSP leaders believe they lack the technical expertise to manage identity and access, but OIT leaders believe it should not be their responsibility to manage those functions.

OMB requires chief operating officers to ensure regular coordination to implement, manage, and maintain the agency's ICAM policies, processes, and technologies. VA's deputy secretary is also VA's chief operating officer. The OIG found neither the deputy secretary nor his office, although briefed on ICAM-related topics, was involved in coordination of ICAM efforts across the VA enterprise since OMB issued its policy in 2019. The OIG determined that the deputy secretary did not resolve disagreements or clarify policy and roles on ICAM to meet OMB's requirements.

[28] OMB M-19-17.

[29] NIST Special Publication 800-63-3.

The following determinations formed the basis for the finding and led to the OIG's recommendations:

- VA did not effectively manage and coordinate ICAM efforts to keep policies updated and meet roadmap goals.
- Disagreements over roles and responsibilities prevented effective management of ICAM policy.
- VA information security is at risk.

What the OIG Did

The OIG reviewed OMB requirements for ICAM governance. The review team interviewed managers and employees in HRA/OSP and OIT. Also, the team reviewed documentation to determine whether VA defined ICAM roles and responsibilities; developed ICAM policies; implemented strategic plans and roadmaps; and implemented digital identity risk management requirements established by NIST.[30] Details of the OIG's methodology can be found in appendix B.

VA Did Not Effectively Manage and Coordinate ICAM Efforts

The OIG found the roles and responsibilities assigned to VA offices do not lead to effective management and coordination of ICAM efforts, since they have not been revised to comply with the latest OMB policy issued in May 2019. Specifically, the policy required VA to designate an integrated office, team, or governance structure for effective ICAM efforts.[31] The policy also stated that agency ICAM teams should include personnel from offices of the chief information officer, chief financial officer, human resources, general counsel, chief information security officer, senior agency official for privacy, chief acquisition officer, and senior officials responsible for physical security.[32] Furthermore, the policy suggested ICAM teams include component organizations that manage ICAM programs and capabilities, including those deployed through the continuous diagnostics and mitigation program.[33] VA designated office responsibility for identity access management in 2011, 2012, and 2014. However, an informal transfer of VA identity access management business sponsor roles in 2016 led to confusion and

[30] NIST Special Publication 800-63-3.

[31] OMB M-19-17.

[32] OMB M-19-17.

[33] OMB M-19-17. The continuous diagnostics and mitigation program enhances the overall security and privacy posture of the federal government by providing federal agencies with capabilities to reduce the attack surface of their respective networks, identify cybersecurity risks, and enable agencies to prioritize actions to mitigate or accept risks based on the potential effects for their missions.

disagreement among VA offices over their roles and responsibilities. VA has not reassessed its ICAM governance structure since the OMB policy was issued in 2019.

On March 23, 2011, a former assistant secretary for OIT issued a memo designating the deputy assistant secretary for information security as the business sponsor for identity and access management. This included assigning responsibility for coordinating enterprise-wide identity access management activities and developing VA's transition plan for alignment with federal ICAM segment architecture. On April 12, 2012, the deputy secretary at the time issued a memo assigning OSP as the lead office for VA's identity management program. The assignment specified that OSP would manage the process of ensuring all people who access VA facilities are proofed, trusted, and credentialed at the appropriate level to carry out assignments.

On October 9, 2014, the deputy secretary at the time directed OSP to assume the role as the executive agent to supervise and coordinate VA personnel security and suitability programs. In January 2016, there was an informal agreement to transfer VA identity and access management business sponsor roles from Office of Information Security to OSP, but this agreement was never formally documented or approved by VA senior leaders. On March 1, 2017, the acting assistant secretary for OIT and chief information officer rescinded the March 2011 memo assigning the deputy assistant secretary of Office of Information Security identity access management responsibilities for coordinating enterprise-wide identity access management activities. This was done because of a shift of identity access management responsibilities to OSP, which combined with HRA in September 2018 to form HRA/OSP.[34]

VA ICAM Policies Are Outdated and Do Not Meet Roadmap Goals

VA's ICAM policies, which consist of three directives and their accompanying handbooks, are outdated and do not meet the OMB requirement that agencies define and maintain a single comprehensive ICAM policy and technology solution roadmap.[35] According to VA's enterprise directives management procedures, permanent directives and handbooks are required to be recertified within five years of issuance to ensure the current policy and procedures are consistent with other enterprise directives and handbooks.[36] VA's ICAM policies were all outside that window. VA Directive 6510 and its accompanying handbook were not updated

[34] VA Secretary memo.

[35] VA's ICAM policy encompasses three directives and their accompanying handbooks:

- VA Directive 6510, *VA Identity and Access Management*, January 15, 2016; VA Handbook 6510, *VA Identity and Access Management*, January 15, 2016
- VA Directive 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, October 2015; VA Handbook 0735, *Homeland Security Presidential Directive 12 (HSPD-12) Program*, March 2014
- VA Directive 0710, *Personnel Security and Suitability Program*, June 4, 2010; VA Handbook 0710, *Personnel Security and Suitability Program,* May 2, 2016.

[36] VA Handbook 0999, *Enterprise Directives Management (EDM) Procedures*, August 1, 2019.

because neither HRA/OSP nor OIT accepted ownership of the policies. According to the Office of ICAM executive director and the HRA/OSP chief security officer, HRA/OSP has been in the process of updating the VA directives 0735 and 0710 and their accompanying handbooks but was delayed due to changes in VA's credentialing process and updated federal guidance for personnel vetting. According to the executive director, HRA/OSP expected to publish the updates for both directives and handbooks by the end of summer 2022.

According to the Office of ICAM executive director, he instructed his staff to update both Directive 6510 and its accompanying handbook to satisfy OMB's requirement for a single comprehensive ICAM policy. From June 2017 through December 2020, the Office of ICAM drafted updates to the directive and handbook and coordinated with OIT and other VA offices to incorporate OMB requirements and define various ICAM roles and responsibilities. The executive director further stated that the directive and handbook were near completion, but there was still disagreement with OIT over which office was responsible for the directive and accompanying handbook. According to the Office of ICAM Access and Identity Management division director, the lack of accountability for ICAM has prevented the governance that is needed. The division director also stated that the comprehensive ICAM strategy cannot be developed without the foundational policy provided by Directive 6510 and its accompanying handbook 6510, and after that is done, VA can move forward with publishing them and the subsequent development and implementation of comprehensive ICAM policy.

VA developed an ICAM technology solutions roadmap in accordance with OMB requirements but did not meet the goals it established. The most recent roadmap was issued in June 2020. For FY 2020 and FY 2021, VA established five goals related to identity governance and administration and access management and certification.[37] The goals were to

- update standards and architecture framework to support enhanced identity governance and administration for patients, application users, support staff, and non-person entities,[38]
- develop standardized identity governance policies and processes,
- complete access management discovery phase to prioritize the list of applications for access automation, access request, access certification and role-engineering efforts,
- acquire identity governance and administration solutions and create application prioritization matrix to aid with onboarding, and

[37] FY 2020 was from October 1, 2019, through September 30, 2020; FY 2021 was from October 1, 2020, through September 30, 2021.

[38] NIST Computer Security Resource Center, "Non-person entity," accessed March 29, 2022, https://csrc.nist.gov/glossary/term/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."

- develop access certification requirements to support access certification and recertification capabilities.

These goals were not met because of a lack of coordination between HRA/OSP and OIT on completing them. According to the Office of ICAM executive director, the roadmap goals relate to OIT job functions, and his staff are not IT specialists and do not have the technical expertise to complete the goals. OIT's former deputy assistant secretary and chief information security officer said that to his knowledge, there were no coordination efforts between HRA/OSP and OIT to ensure the roadmap goals were being addressed and achieved.

VA Did Not Implement Updated NIST Digital Identity Risk Management Requirements

VA Directive 6510 and its accompanying handbook require VA to comply with NIST's electronic authentication guidelines.[39] OMB requires agencies to implement NIST's digital identity guidelines, which superseded the electronic authentication guidelines and any successive versions.[40] These guidelines apply to all systems for which digital identity or authentication is required. However, VA did not incorporate digital identity risk management in VA policy as outlined in NIST guidelines. This occurred due to HRA/OSP and OIT's failure to take responsibility for updating the policies.

To evaluate whether VA incorporated digital identity risk management requirements, the review team selected a sample of 50 of 882 IT systems from the VA system inventory (VASI). For more information on VASI, see appendix A. The review team found 45 systems were noncompliant; the remaining five systems were out of the review's scope because they did not have user authentication, they were decommissioned, or they did not have a point of contact.[41] None of the 45 in-scope systems had any evidence showing that the risks of proofing, authentication, and federation errors were separately assessed, or the digital identity acceptance statement was completed.[42] As a result of the sampling, the OIG estimated that at least 93.6 percent of IT systems with user authentication were noncompliant. Based on this percentage, the number of systems in VASI, and the proportion of sampled systems with user authentication, the OIG estimated that the number of noncompliant IT systems in the VASI sampling frame of 882 was

[39] NIST, *Electronic Authentication Guideline*, NIST Special Publication 800-63-2, August 2013. Withdrawn and superseded by NIST Special Publication 800-63-3.

[40] OMB M-19-17.

[41] NIST Special Publication 800-63-3.

[42] NIST Special Publication 800-63-3. The digital identity acceptance statement includes at a minimum (1) the assessed identity, authenticator, and federation assurance levels, (2) the implemented identity, authenticator, and federation assurance levels, (3) rationale, if implemented identity, authenticator, and federation assurance levels differ from what was assessed, (4) comparability demonstration of compensating controls when all applicable NIST special publication requirements are not implemented, and (5) if not accepting federated identities, the rationale.

no less than 728. The sample included 25 systems that were premium criticality, which indicates that a compromise to the system would have grave consequences that could lead to loss of life, serious injury to people, or mission failure as determined by the business line.[43] For details on the sampling methodology, see appendix C.

Disagreements Over Roles and Responsibilities Prevented Effective Management

Federal guidance recommends that agencies create a program governance body, such as an executive steering committee, to oversee ICAM projects and workstreams and align those services and management with the agency's mission.[44] OSP created an ICAM Executive Steering Committee, and the original committee charter, dated January 2015, provided that unresolved issues would be elevated to a senior decision authority. The 2015 committee had members from offices across the VA enterprise, including HRA, OSP, and OIT, which cochaired the committee. The committee is important because it governs VA ICAM business processes, projects, investments, initiatives, and activities. After the committee charter was updated in 2020, the Veterans Experience Office became a cochair, and OIT declined to continue as cochair but remained a voting member of the committee. According to the former VA deputy chief information officer, OIT's role was to put IT capabilities in place to support ICAM functions. Putting OIT in a position of deriving business requirements was not an appropriate role.

The review team evaluated the committee's meeting minutes and supporting information from May 2019, after OMB's policy took effect, through October 2021. The team also evaluated two executive steering committee charters that were approved and signed during the review period, one of which was effective in January 2015 and the other in May 2020. The 2015 charter required the committee to meet no less than monthly, and the 2020 charter required it to meet no less than quarterly. The team determined there was one meeting in August 2019, two meetings in 2020 (May and September), and three meetings in 2021 (June, August, and October). Information from these meetings did not contain any indication that the committee addressed issues identified in this report or suggested elevating them to a higher decision authority.

According to OMB, agency chief operating officers are required to ensure regular coordination among agency leaders to implement, manage, and maintain the agency's ICAM policies, processes, and technologies.[45] In VA, this responsibility falls on the deputy secretary. According to the Office of ICAM executive director, neither the deputy secretary nor his office has been involved in coordination of VA's ICAM efforts across the VA enterprise since OMB issued its

[43] VASI Glossary dated September 29, 2021, obtained from senior architect, Enterprise Architecture, OIT.

[44] Federal Identity, Credential, and Access Management Playbooks, *Program Governance and Leadership*, accessed on March 21, 2022, https://playbooks.idmanagement.gov/pm/governance/.

[45] OMB M-19-17.

memo in 2019.[46] As a result, the OIG determined that the deputy secretary did not resolve disagreements or clarify policies and roles on ICAM to meet OMB's requirements.

The deputy secretary was briefed on ICAM-related topics but not on the dispute over roles and responsibilities, according to HRA and OSP leaders. As a result, he has not been involved in efforts to resolve the disagreements. The review team did not identify evidence that the prior deputy secretary was involved in the coordination of VA's ICAM efforts. The OIG concluded the deputy secretary should work with subordinate managers to assess and clearly define roles and responsibilities for all parties involved in VA's ICAM process.

The OIG also found that disagreements have interfered with the effective operation of VA's ICAM policies. According to the Office of ICAM executive director, who has been in place since August 2018, his staff does not possess the information technology and cybersecurity technical skill sets and IT systems experience needed to most effectively contribute as a partner with OIT in the management and oversight of VA's ICAM program. HRA/OSP's chief security officer, who has been in place since July 2020, stated their focus should be on personnel security, credentialing, and policy oversight. Both believe OIT should manage identity and access. However, OIT believes that ICAM ownership belongs to HRA/OSP. As a result, there have been confusion and disagreements between HRA/OSP and OIT leaders on ICAM roles and responsibilities to be performed by each office.

In February 2021, due to a lack of resources and technical expertise, the HRA/OSP chief security officer directed the Office of ICAM staff to stop efforts to update VA Directive 6510 and its accompanying handbook. According to the chief security officer, transfer of responsibilities from OIT to OSP was never formalized through a directive or other agreement by VA senior leaders, and many of the transferred functions were IT-based functions that OSP did not have the technical expertise to perform or properly manage. At the time of this review, the directive and handbook assign OIT as the responsible office for the contents of these policies. According to an Office of Information Security document titled "Resolving Confusion Over Responsibilities Within VA for Identity, Credential, and Access Management (ICAM)," provided by the Office of ICAM executive director, one of the roles informally transferred from OIT to OSP in 2016 as part of the identity and access management business sponsor role was ownership of the directive and handbook.

According to the OIT former deputy assistant secretary and chief information security officer, ownership of the directive and its accompanying handbook belongs to HRA/OSP and is not OIT's responsibility. The HRA/OSP chief security officer said HRA/OSP and OIT are considering realigning the Office of ICAM Access and Identity Management division under OIT, as part of a coordinated effort. In April 2021, OIT prepared an ICAM Realignment Course of Action Analysis citing a need for agreement on ICAM roles and responsibilities and streamlined

[46] VA's current deputy secretary was sworn in on July 19, 2021.

ICAM requirements. The analysis also recommended that ICAM functions of digital identity and access management be realigned from HRA/OSP to OIT. In November 2021, in response to a request from OIT, the Access and Identity Management division director provided OIT with a transition plan and draft presentation outlining the alignment of the Access and Identity Management office under OIT. She stated that she met with the OIT Chief Technology Officer in February 2022 to provide an overview of the transition plan, but received no response after following up on this meeting.

VA Information Security Is at Risk

Effective identity governance and administration is the ability to manage and reduce the risk that comes with excessive or unnecessary user access to applications, systems, and data. Annual OIG FISMA audits have demonstrated weaknesses in implementing proper monitoring and governance controls in determining whether users have the right access to perform their job functions. In addition, VA users and business operations suffer from inefficient processes and are unable to gain timely access to the applications they need to perform their job functions. To mitigate these gaps, VA intended to implement an enterprise identity governance agency solution. However, VA has not met the FY 2020 and FY 2021 goals established for its identity governance agency solution. Until VA issues a single comprehensive policy, updates its directives and handbooks, and clearly defines roles and responsibilities, it will not comply with OMB requirements.

The identity governance and administration goals in the ICAM roadmap are intended to mitigate gaps related to access management identified in the annual FISMA audit reports. By not meeting those goals, VA cannot mitigate deficiencies found during these audits related to identity management and access controls. These issues include numerous instances of unnecessary system privileges, excessive and unauthorized user accounts, accounts without formal access authorizations, and active accounts for terminated personnel. Additionally, user access requests were not consistently reviewed to eliminate conflicting roles and enforce segregation of duties principles. The FISMA audit reports have identified inconsistent monitoring of access for individuals with excessive privileges within certain major applications. This occurred because VA has not implemented effective reviews to monitor for instances of unauthorized system access or excessive permissions. Periodic reviews are critical to restrict legitimate users to specific systems and to prevent unauthorized access by both internal and external users.[47] VA will continue with the same repeat deficiencies if its leaders do not act to mitigate the gaps identified in the FISMA audit reports.

[47] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021.

Further, according to the Office of Information Security Risk Management Framework Authorization Process Design and Integration supervisor, and the Development, Security, and Operations district information security director, VA information systems security officers rely on internal guidance such as VA Directive 6510 for assessing security controls related to identity and access management. According to OIT's Development, Security, and Operations district information security director, they provide support services to ensure that security controls are implemented for the risk management framework process.[48] Because VA Directive 6510 and its accompanying handbook have not been updated, they do not include the digital identity risk management requirements established by NIST. Consequently, the guidance in VA's Enterprise Mission Assurance Support Service was not updated to include such requirements. As a result, VA relied on an outdated policy when assessing security controls and is not meeting requirements established by NIST.[49] By not implementing current digital identity risk management requirements, VA risks leaving its systems vulnerable to compromise by impostors who may gain access to protected information.

Conclusion

VA's governance of its ICAM efforts does not meet OMB standards for comprehensive and effective management. VA's ICAM policies are outdated, and the agency is not meeting its own roadmap goals. This is because there are no processes for ensuring coordination among the various offices, leading to disagreements over ownership of ICAM efforts and delays in updating policies to match evolving standards. Further, there is no process in place to ensure the deputy secretary is informed of concerns or effectively coordinates ICAM efforts, as required by OMB. Without proper governance, VA risks access and security issues, including users not having the appropriate access to perform their job functions and impostors gaining access to protected information. Improper governance also makes it harder for VA to mitigate issues identified during annual FISMA audits.

[48] Committee on National Security Systems, *Committee on National Security Systems Glossary*, April 6, 2015. The risk management framework is a structured approach used to oversee and manage risk for an enterprise. The risk management framework process is performed and documented in VA's Enterprise Mission Assurance Support Service, a government-owned, web-based application with a broad range of services for comprehensive cybersecurity management.

[49] NIST Special Publication 800-63-3.

Recommendations 1–4

The OIG made two recommendations to the VA deputy secretary:

1. Designate roles and responsibilities for all program offices involved in VA's identity, credential, and access management program.
2. Provide appropriate oversight and ensure coordination between designated program offices to implement a comprehensive identity, credential, and access management policy.

The OIG made the following recommendation to the assistant secretary for information and technology:

3. Update and publish a VA directive and handbook associated with identity and access management that includes current National Institute of Standards and Technology requirements.

The OIG made the following recommendation to the assistant secretary for human resources and administration/operations security and preparedness:

4. Update and publish VA directives and handbooks associated with the Homeland Security Presidential Directive 12 Program and VA's personnel security and suitability program as required by VA's enterprise directives management procedures.

VA Management Comments

VA's deputy secretary concurred with all the report's findings and recommendations and submitted responsive action plans. Appendix D provides the full text of the deputy secretary's comments.

In response to recommendation 1, the deputy secretary will issue a memo that designates the roles and responsibilities for all program offices involved in VA's ICAM program. The target completion date is August 31, 2022.

For recommendation 2, the deputy secretary will ensure that appropriate oversight and coordination are in place between designated program offices to implement a comprehensive ICAM policy. To accomplish this, VA will designate a lead program office. VA's target completion date is September 30, 2022.

In response to recommendation 3, the deputy secretary reported the assistant secretary for OIT concurred, dependent on implementation of recommendations 1 and 2. Should OIT be designated as the responsible policy office, it will update and publish VA Directive and Handbook 6510. OIT's target date is nine to 18 months after the deputy secretary designates roles and responsibilities for all program offices involved in VA's ICAM program.

For recommendation 4, the deputy secretary reported the assistant secretary for HRA/OSP concurred and has placed VA Directives 0710 and 0735 and associated handbooks into VA's formal review and coordination process. The deputy secretary reported the implementation plan is in the final steps with an anticipated completion date of September 30, 2022.

OIG Response

The OIG considers the corrective action plans acceptable and will monitor VA's progress in meeting the intent of the recommendations. The OIG recognizes the corrective action plan for recommendation 3 is dependent on OIT being designated the responsible policy office. The OIG will close the recommendations when it receives sufficient evidence that appropriate measures have been taken.

Appendix A: Background

Digital Identity Guidelines

NIST guidelines provide technical requirements for federal agencies implementing digital identity services.[50] The guidelines cover identity proofing and authentication of users including employees, contractors, and private individuals interacting with government IT systems over open networks. The guidelines also define technical requirements in each area of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions and apply to all digital services requiring authentication or identity proofing, regardless of the constituency—citizens, business partners, or government entities.[51] Figure A.1 provides an overview of the digital identity model.

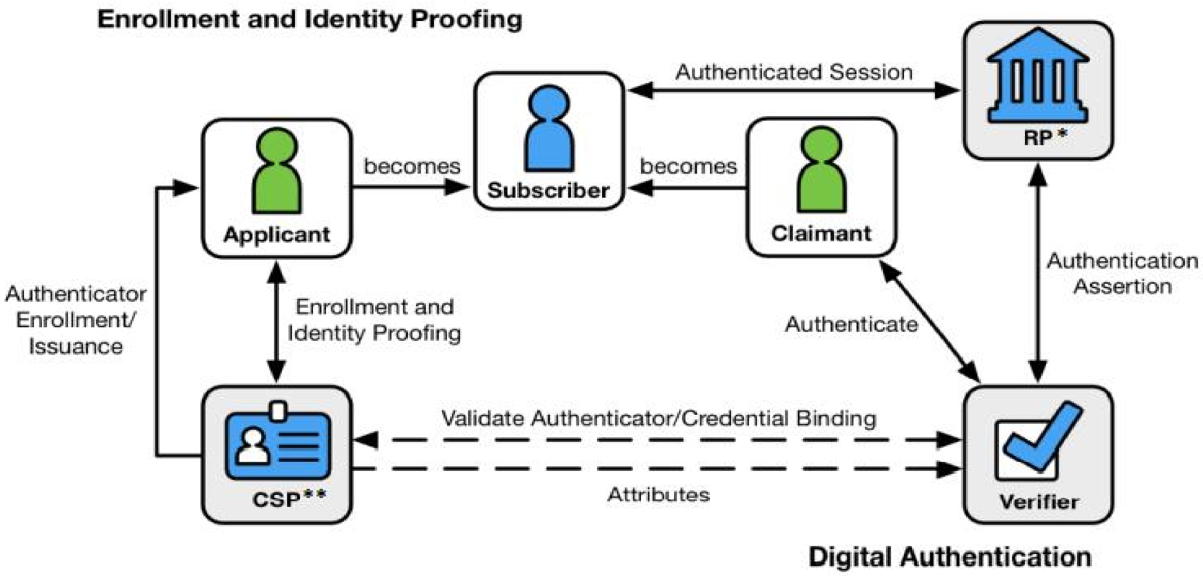

Figure A.1. *Digital identity model.*
Source: NIST Special Publication 800-63-3.
**Relying party is an entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.*
***Credential service provider is a trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers.*

[50] NIST Special Publication 800-63-3. Digital identity is the unique representation of a subject engaged in an online transaction and always unique in the context of a digital service, but does not necessarily uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known.

[51] NIST Special Publication 800-63-3. Identity proofing is the process in which a credential service provider collects, validates, and verifies information about a person. Authentication is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.

Federal agencies also use NIST guidelines as part of the risk assessment and implementation of their digital services and to mitigate an authentication error's negative impacts by separating the individual elements of identity assurance into discrete component parts. For nonfederated systems, agencies select two components, identity assurance and authenticator assurance levels.[52] For federated systems, agencies select a third component, federation assurance level.[53] The guidelines "retire the concept of a level of assurance as a single ordinal that drives implementation-specific requirements" by instead "combining appropriate business and privacy risk management side-by-side with mission need." Consequently, agencies are required to select identity assurance level, authenticator assurance level, and federation assurance level as distinct options. "The separation of these categories provides agencies flexibility in choosing identity solutions and increases the ability to include privacy-enhancing techniques as fundamental elements of identity systems at any assurance level." Table A.1 provides details of the three assurance levels for identity, authenticator, and federation.

Table A.1. Identity, Authenticator, and Federation Assurance Levels

Level	Type of assurance
	Identity
1	There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a credential service provider asserts to a relying party).
2	Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. Identity assurance level two introduces the need for either remote or physically present identity proofing. Attributes can be asserted by credential service providers to relying parties in support of pseudonymous identity with verified attributes.[54]
3	Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the credential service provider. As with identity assurance level two, attributes can be asserted by credential service providers to relying parties in support of pseudonymous identity with verified attributes.

[52] NIST Special Publication 800-63-3. Federation is a process that allows the conveyance of identity and authentication information across a set of networked systems. Identity assurance level is a category that conveys the degree of confidence that the applicant's claimed identity is their real identity. Authenticator assurance level is a category describing the strength of the authentication process.

[53] NIST Special Publication 800-63-3. Federation assurance is a category describing the assertion protocol used by the federation to communicate authentication and attribute information (if applicable) to a relying party.

[54] NIST Special Publication 800-63-3. Pseudonymous identifier is a meaningless but unique number that does not allow the relying party to infer anything regarding the subscriber, but which does permit the relying party to associate multiple interactions with the subscriber's claimed identity. A subscriber is a party who has received a credential or authenticator from a credential service provider.

Level	Type of assurance
Authenticator	
1	Authenticator assurance level one provides some assurance that the claimant controls an authenticator bound to the subscriber's account. Authenticator assurance level one requires either single-factor or multifactor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
2	Authenticator assurance level two provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at authenticator assurance level two and above.[55]
3	Authenticator assurance level three provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at level three is based on proof of possession of a key through a cryptographic protocol. Level three authentication shall use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both these requirements. To authenticate at level three, claimants shall prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.
Federation	
1	Allows for the subscriber to enable the relying party to receive a bearer assertion. The assertion is signed by the identity providers using approved cryptography.
2	Adds the requirement that the assertion be encrypted using approved cryptography such that the relying party is the only party that can decrypt it.
3	Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the identity providers and encrypted to the relying party using approved cryptography.

Source: NIST Special Publication 800-63-3.

VA Systems Inventory

VASI is the authoritative data source for VA IT systems.[56] VASI also provides a VA-wide inventory of systems and systems-related information that reflects the current state of VA's information environment. VASI links systems information to other information about VA's business and IT environment, enabling analysis and decision support across a wide variety of topics. For an IT capability to be registered as a system in VASI, it must exhibit one or more of the following characteristics:

[55] NIST Special Publication 800-63-3. Cryptographic authenticator is an authenticator where the secret is a cryptographic key. A cryptographic key is a value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

[56] VA Directive 6404, *VA System Inventory (VASI)*, February 23, 2016.

- Automates or supports the automation of a VA business process that enables a business capability aligned to the business reference model
- Is funded by VA or any other government entity in support of VA, either by investment or fee-for-use
- Is hosted in a shared computing environment (e.g., data center, government or commercial cloud facility, medical center)
- Uses personal identity verification, password, or other multifactor authentication methods to access the system's data, services, and other capabilities
- Sends or receives data or interfaces with data to veterans, users, another VA product, or a product outside of VA

VA Policies and Procedures on ICAM

VA Directive 6510 defines the policies for enterprise identity and access management for VA.[57] VA Handbook 6510 defines roles, responsibilities, and procedures to implement VA Directive 6510, and the VA-wide identity and access management program. This program provides access to VA information, resources, and services to improve timeliness and promote ease of access for all VA users.[58]

VA Directive 0710 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 IT systems.[59] VA Handbook 0710 establishes and implements policy and procedures, provides guidelines, delegates authority, and assigns responsibilities regarding personnel security, suitability, and fitness for personnel within VA.[60]

VA Directive 0735 establishes department-wide requirements and responsibilities for VA's Homeland Security Presidential Directive 12 program.[61] The directive defines department-wide policies, roles, and responsibilities for aligning personal identity verification, logical access control systems, and physical access control systems with the identity verification and access

[57] VA Directive 6510.

[58] VA Handbook 6510.

[59] VA Directive 0710.

[60] VA Handbook 0710.

[61] VA Directive 0735; Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004. This directive mandates a federal standard for secure and reliable forms of identification.

management capabilities within VA. VA Handbook 0735 provides guidance regarding use, administration, and governance of VA identity credentials.[62]

Prior VA OIG FISMA Audits

For years, the OIG has found deficiencies with identity management and access controls during its annual FISMA audits. In an April 2021 audit report, OIG identified significant information security control deficiencies in several areas including password management, access management, audit logging and monitoring, and personnel screening and investigations.[63] All the findings, except for personnel screening and investigations, were repeated findings from prior years. The OIG recommended the assistant secretary for information and technology implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices. The OIG also recommended the assistant secretary implement periodic reviews to minimize access by system users with incompatible roles, permissions exceeding required functional responsibilities, and unauthorized accounts, in addition to enabling system audit logs on all critical systems and platforms and conducting centralized reviews of security violations across the enterprise. These are repeat recommendations from prior years.

The OIG further recommended the Office of Personnel Security strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors and applicable investigation data are accurately tracked within the authoritative system of record. Finally, the OIG recommended the Office of Personnel Security formalize the position descriptions and methodology used within the human resource business process to ensure that employees with similar positions are required to have the same level of background investigation.

[62] VA Handbook 0735.

[63] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021.

Appendix B: Scope and Methodology

Scope

The OIG performed this review from October 2021 through May 2022 to determine if VA effectively implemented ICAM governance requirements established in OMB policy.

Methodology

To gain an understanding of overall ICAM governance requirements and implementation by VA, the review team examined OMB's ICAM policy, NIST special publications, the federal ICAM playbooks, and VA handbooks and directives. The team also requested and reviewed information and documentation from HRA/OSP and OIT related to VA's implementation, coordination, and management of VA's ICAM program. The team interviewed HRA/OSP and OIT employees involved in VA's ICAM processes.

To evaluate the extent to which VA incorporated digital identity risk management per NIST's digital identity guidelines, the review team evaluated a statistical sample of VA information systems to determine if requirements were met for those systems. The team interviewed VA employees to determine VA's information system repository of record, and the extent systems contained in that repository were subject to NIST requirements. The team then met with members of OIG's data and statistical analysis teams, secured access to the repository to extract a universe of systems, selected a sample, and worked with OIT staff and system owners to test the sample for compliance with the requirements.

Internal Controls

The review team assessed the internal controls of VA's ICAM program significant to the review objective. This included an assessment of the five internal control components: control environment, risk assessment, control activities, information and communication, and monitoring.[64] In addition, the team reviewed the principles of internal controls as associated with the objective. The team identified the following four components and nine principles as significant to the objective.[65]

- Component 1: Control Environment
    - Principle 2: Exercises oversight responsibility

[64] Government Accountability Office (GAO), *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014.

[65] Since the review was limited to the internal control components and underlying principles identified, it may not have disclosed all internal control deficiencies that may have existed at the time of this review.

    - Principle 3: Establishes structure, authority, and responsibility
    - Principle 4: Demonstrates commitment to competence
- Component 2: Risk Assessment
    - Principle 7: Identifies and analyzes risk
    - Principle 9: Identifies and analyzes significant change
- Component 3: Control Activities
    - Principle 10: Selects and develops control activities
    - Principle 11: Selects and develops general controls over technology
    - Principle 12: Deploys through policies and procedures
- Component 4: Information & Communication
    - Principle 14: Communicates internally

The team identified deficiencies in the above internal control components and principles during its review. The deficiencies are discussed in the report findings and addressed in the OIG's recommendations.

Fraud Assessment

The review team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant within the context of the review objectives, could occur during this review. The team exercised due diligence in staying alert to any fraud indicators and did not identify any instances of fraud or potential fraud during this review.

Data Reliability

The OIG obtained electronic spreadsheets of all active VA systems that were directly downloaded from VA Enterprise Architecture Repository's VASI data and traced the information of selected sample systems to Enterprise Mission Assurance Support Service system summary reports. The OIG believes the data from the electronic spreadsheets were reliable for their intended purposes and used to support conclusions in the audit report.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.* The evidence obtained provided a reasonable basis for the OIG's findings and conclusions based on the review objective.

Appendix C: Statistical Sampling Methodology

Approach

To determine whether VA properly implemented digital identity risk management, the review team evaluated a sample of VA IT systems as of October 28, 2021. The team used statistical sampling to quantify the extent of records where OIT properly documented evidence of digital identity risk management implementation for each system.

Population

The target population consisted of active systems with user authentication in VASI as of October 28, 2021. However, for sampling purposes, the review team assembled a sampling frame consisting of all 882 active VA systems in VASI as of October 28, 2021.

Sampling Design

The sampling frame was stratified into two groups. One group was systems identified as "premium criticality," and the second group consisted of non-premium criticality systems.[66] The team requested a statistical sample of 50 systems as seen in table C.1.

Table C.1. Statistical Strata for IT System Digital Identity Risk Management Review

Strata	Strata description	Sample size	Sampling frame size
1	Premium criticality	25	209
2	Non-premium criticality	25	673
	Total	**50**	**882**

Source: VA OIG statistician's stratified population. Data obtained from VASI.

Weights

Samples were weighted to represent the population from which they were drawn, and the weights were used in the estimate calculations. For example, the team calculated the estimated percentage that was noncompliant by first summing the sampling weights for all sample records that were noncompliant, then dividing that value by the sum of the weights for all sample records.

[66] VASI Glossary dated September 29, 2021, obtained from a senior architect, Enterprise Architecture, OIT. Premium criticality indicates that a compromise to the system would have grave consequences leading to loss of life, serious injury to people, or mission failure as determined by the business line.

Projections and Margins of Error

The projection is an estimate of the population value based on the sample. The associated margin of error and confidence interval show the precision of the estimate. If the OIG repeated this audit with multiple sets of samples, the confidence intervals would differ for each sample but would include the true population value 90 percent of the time. The OIG statistician calculated estimates, margins of error, and confidence intervals that account for the complexity of the sample design.

The sample size was determined after reviewing the expected precision of the projections based on the sample size, potential error rate, and logistical concerns of the sample review. While precision improves with larger samples, the rate of improvement decreases significantly as more records are added to the sample review. Figure C.1 shows the effect of progressively larger sample sizes on the margin of error.

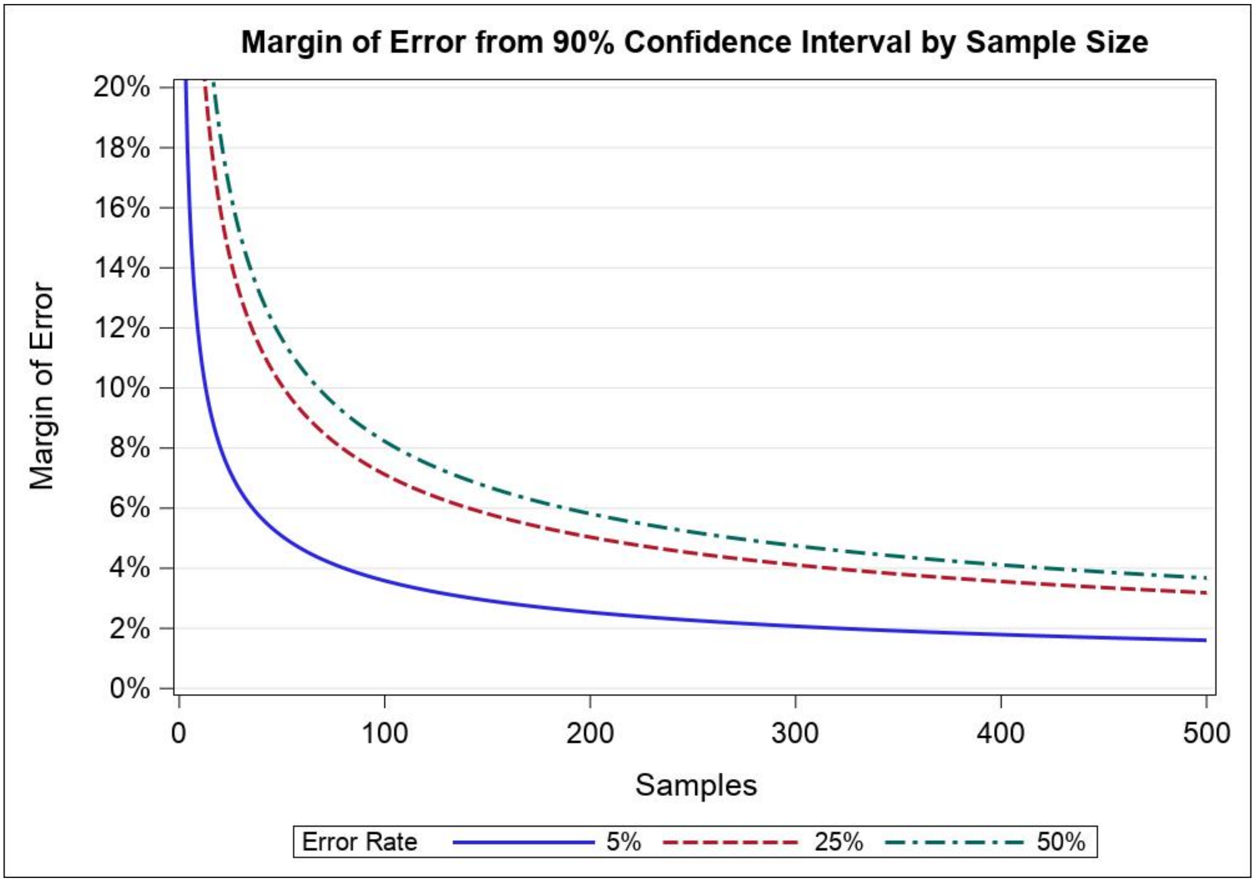

Figure C.1. *Effect of sample size on margin of error.*

Source: VA OIG statistician's analysis.

Projections

Two sets of statistical projections were calculated. Table C.2 shows the estimated number of noncompliant systems, absolutely and as a percentage of the total number of systems in the sampling frame. Table C.3 shows the estimated number of noncompliant, in-scope systems (where a system was out of scope if it did not have user authentication, it was decommissioned, or did not have a point of contact) as a percentage of all in-scope systems.

Table C.2. Statistical Projections Summary for All Active Systems

Projection	Estimate	Margin of error	Two-sided 90 percent confidence lower limit	Two-sided 90 percent confidence upper limit	One-sided 90 percent confidence lower limit	(Noncompliant sample count)/ (sample size)
Noncompliant systems	803	72	707	850	728	45/50
Percent noncompliant	91.1%	8.1%	80.1%	96.4%	82.5%	45/50

Source: VA OIG analysis of statistically sampled results over the sample populations. Data used for analysis and projections were obtained from VASI.

Note: Projections in table C.2 denote the number and percentage of noncompliant systems out of all 882 active systems on October 28, 2021. Clopper-Pearson confidence intervals are reported to conservatively bound these values. The margin of error is calculated as half the difference between the two-sided 90 percent confidence interval's upper and lower bounds.

Table C.3. Statistical Projections Summary for Active Systems with User Authentication

Projection	Estimate	Margin of error	Two-sided 90 percent confidence lower limit	Two-sided 90 percent confidence upper limit	One-sided 90 percent confidence lower limit	(Noncompliant sample count)/ (sample size)
Percent noncompliant	100.0%	8.2%	91.8%	100.0%	93.6%	45/45

Source: VA OIG analysis of statistically sampled results over the sample populations. Data used for analysis and projections were obtained from VASI.

Note: The projections in table C.3 denote the number of noncompliant active, in-scope systems as a percentage of all active, in-scope systems on October 28, 2021. Clopper-Pearson confidence intervals are reported to conservatively bound these values. The margin of error is calculated as the difference between the point estimate and the one-sided 90 percent confidence interval lower bound.

Appendix D: Management Comments

Department of Veterans Affairs Memorandum

Date: July 7, 2022

From: Deputy Secretary of Veterans Affairs (001)

Subj: Draft Report: VA Needs to Improve Governance of Identity, Credential and Access Management Processes—Project Number 2022-00210-AE-0012

To: Assistant Inspector General for Audits and Evaluations (52)

1. Thank you for the opportunity to review and comment on the Office of Inspector General, Office of Audits and Evaluation, report entitled VA Needs to Improve Governance of Identity, Credential and Access Management Processes. We concur on the report and provide the attached response and comments for completing the open recommendations.

The OIG removed point of contact information prior to publication.

(Original signed by)

Donald R. Remy

Attachment

Attachment

Department of Veterans Affairs (VA)
Comments to Office of Inspector General (OIG) Draft Report:
VA Needs to Improve Governance of Identity, Credential and
Access Management Process (Project Number 2022-00210-AE-0012)

OIG made two recommendations to VA's Deputy Secretary:

OIG Recommendation 1: Designate roles and responsibilities for all program offices involved in VA's identity, credential and access management program.

VA Response: Concur. VA's Deputy Secretary will issue a memo that designates the roles and responsibilities for all program offices involved in VA's identity, credential and access management program.

Target completion date is August 31, 2022.

OIG Recommendation 2: Provide appropriate oversight and ensure coordination between designated program offices to implement a comprehensive identity, credential and access management policy.

VA Response: Concur. VA's Deputy Secretary will ensure that appropriate oversight and coordination is in place between designated program offices to implement a comprehensive identity, credential and access management policy. This will be accomplished by designating a lead program office and requiring regular status updates through the Department's current governance process, with the first status report briefing to be scheduled for the 4th quarter of fiscal year 2022.

Target completion date is September 30, 2022.

OIG made one recommendation to the Assistant Secretary for Information and Technology:

OIG Recommendation 3: Update and publish a VA directive and handbook associated with identity and access management that includes current National Institute of Standards and Technology requirements.

VA Response: Concur. The Office of Information and Technology (OIT) concurs, dependent on implementation of recommendations 1 and 2 and the outcome of the designation of roles and responsibilities for all program offices involved in the identity, credential and access management program. Should the Deputy Secretary designate OIT as the responsible policy office for VA Directive and Handbook 6510 (VA Identity and Access Management), OIT's plan of action is to establish a working group or tiger team incorporating all stakeholders to update and publish VA Directive and Handbook 6510, to include incorporating digital identity risk management as outlined in National Institute of Standards and Technology guidance.

Target completion date is 9-18 months after the Deputy Secretary designates roles and responsibilities for all program offices involved in VA's identity, credential and access management program.

OIG made one recommendation to the Assistant Secretary for Human Resources and Administration/Operations, Security and Preparedness:

OIG Recommendation 4: Update and publish VA directives and handbooks associated with the Homeland Security Presidential Directive 12 Program and VA's personnel security and suitability program as required by VA's Enterprise Directives Management Procedures.

VA Response: Concur. The Office of Human Resources and Administration/Operations, Security and Preparedness has placed VA directives and handbooks associated with the Homeland Security Presidential Directive 12 Program (VA Directive 0735), and VA's Personnel Security and Suitability Program (VA Directive 0710) into the Department's formal review and coordination process with all offices, using VA's Integrated Enterprise Workflow Solution correspondence management database. The implementation plan is in the final steps as feedback and comments from VA offices are being resolved and adjudicated.

The target completion date to finalize the updated directive and handbooks 0710 and 0735 is September 30, 2022.

Department of Veterans Affairs
July 2022

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461–4720.
Review Team	Al Tate, Director Justice Baek Dominick Caldwell John Cefai Javon Johnson Herman Woo
Other Contributors	Kendal Ferguson Charles Hoskinson Jason Reyes Clifford Stoddard

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.va.gov/oig.