US DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

VA Should Strengthen Enterprise Cloud Security and Privacy Controls

Audit	22-03525-195	September 27, 2023

BE A

VOICE FOR VETERANS

REPORT WRONGDOING

va.gov/oig/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

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.

Visit our website to view more publications.
va.gov/oig

Executive Summary

VA is committed to delivering information technology systems that ensure convenient and secure access and improve delivery of the benefits, health care, and myriad services it provides.[1] This includes improving cybersecurity, privacy protections, and resiliency; ensuring information and data are secure and easy to share; and reducing system downtime. According to its enterprise roadmap, VA is undergoing unprecedented information technology modernization and digital transformation to enable improved customer service and interoperability with external partners by optimizing the cloud.[2]

The cloud refers to technology solutions provided by outside vendors that offer access to fully featured applications, software development and deployment environments, and computing infrastructure assets such as network-accessible data storage and processing.[3] VA essentially rents access to the cloud. Its system development must follow the National Institute of Standards and Technology (NIST) risk management framework. The framework is a comprehensive, flexible, repeatable, and measurable seven-step process designed to protect the confidentiality, integrity, and availability of information.[4] The security and privacy controls outlined in the framework can protect organizations, individuals, and information systems from persistent threats and privacy risks arising from the processing of personally identifiable and other protected information in varied operational, environmental, and technical scenarios.

The Veterans Affairs Enterprise Cloud (VAEC) is built on contracts with two major vendors that provide cloud services, referred to in this report as vendor A and vendor B. The Enterprise Cloud Solutions Office (ECSO) within the Office of Information and Technology (OIT) developed and operates the VAEC on the rented vendors' infrastructure. According to VA, the VAEC enables the delivery of services to veterans in a fast, cost-effective, and efficient manner. The VAEC hosts more than 200 systems that employees, veterans, and contractors use to support the delivery of health care, compensation benefits, and home loan guarantees for veterans. It also helps expand cloud-based telework, telehealth, and storage capabilities across VA.

Once a cloud system is established, users purchase "cloud service provider credits" to gain access to the services. To access the VAEC, the department purchases cloud service provider credits from two additional vendors, referred to in this report as service credit vendors. VA also purchases software licenses, software maintenance, and technical support from service credit

[1] VA, *Department of Veterans Affairs Fiscal Years 2022-28 Strategic Plan*, n.d.

[2] Office of Information and Technology, *FY [Fiscal Year] 2020–2026 VA Enterprise Roadmap*, March 31, 2020.

[3] "Federal Cloud Computing Strategy" (website), Office of Management and Budget, accessed April 4, 2023, https://cloud.cio.gov/strategy/.

[4] NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, December 10, 2020.

vendors. Each cloud service provider has a service-level agreement that outlines performance expectations and availability requirements. If a provider does not achieve and maintain agreed-upon service levels, VA may be eligible to recoup a percentage of applicable monthly service charges as a credit.

The VA Office of Inspector General (OIG) conducted this audit to determine if VA is effectively assessing and monitoring security and privacy controls for cloud computing in accordance with federal guidance. Based on the audit team's findings, the team also assessed VA's process for monitoring cloud service performance levels.

What the Audit Found

The audit team did not identify deficiencies in how VA completed the first six steps of the NIST risk management framework: preparing, categorizing, selecting, implementing, assessing, and authorizing controls. However, the team found deficiencies related to monitoring in step seven.[5] Notably, VA has not yet updated its guidance on security and privacy controls following a September 2020 change to NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.[6] Although OIT staff informed the team that they are working on updating the related policy, procedures, and directives, the team found systems were not compliant with the revised guidance as of June 2023. According to OIT, the anticipated policy adoption date is December 2023.

The audit team made two determinations related to weaknesses in the oversight and monitoring of its VAEC systems. This was due in part to OIT not effectively overseeing the management of security and privacy controls to make sure the systems and the information they contain are protected commensurate with the risk associated with their misuse or unauthorized disclosure. The OIG examined the six infrastructure systems and a sample of seven of the systems hosted on that infrastructure. For those 13 VAEC systems reviewed, the team found sufficient controls for 18 of the 20 security and privacy control families.[7] The two control families in which deficiencies were found were in the areas of securing personally identifiable information and supply chain management. Further, because required documentation was not always uploaded, the audit team could not verify that ongoing monitoring was occurring. Although no incursions or other impacts were identified in the course of this audit, VA will continue to lack assurance that VAEC controls are working as designed until it finishes updating its guidance and improves active monitoring of these systems.

[5] For more information on the risk management framework, see appendix A.

[6] VA requested in its technical comments that details be provided on the specific revision. Accordingly, the OIG included that it referred to Special Publication 800-53 (revision 5).

[7] NIST designed security and privacy controls to protect systems and the information they contain; similar controls are grouped into families. Each family contains security and privacy controls that are related to a specific topic that may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms.

The OIG also found that VA may be missing opportunities to recoup service credits when vendors do not meet their performance requirements, such as when incidents attributed to the vendor result in outages that exceed agreed-upon acceptable durations. According to the cloud service provider agreements, if the provider does not achieve and maintain agreed-upon service levels, then VA could be eligible for a credit toward future monthly service fees. Between June 2019 and December 2022 there were 10 cloud service outages eligible for claims for service credits due to outages attributed to the vendors. The audit team found VA did not request recoupment for nine of the 10 outages. This occurred because VA had not identified who is responsible for submitting the recoupment requests to the cloud service providers.

After meeting with the audit team, ECSO staff submitted one claim and created a process for requesting recoupment of service credits. However, ECSO did not develop a policy sufficient to identify, document, and submit cloud service incidents for potential recoupment of service credits and assign roles and responsibilities for doing so. Until VA finishes refining its newly established standard operating procedure, it remains at risk of not receiving service credits to which it is entitled. While VA recouped about $114,000 from one outage, the team was unable to determine how the amount was calculated; according to an ECSO official, the cloud service providers make that determination.

What the OIG Recommended

The OIG recommended the assistant secretary for information and technology develop a timeline for updating the security and privacy guidance to reflect the revisions to NIST Special Publication 800-53 and address identified weaknesses with personally identifiable information and supply chain management. The assistant secretary should also establish a mechanism to ensure continuous monitoring of the VAEC systems to include having and testing plans (such as contingency, incident response, and disaster recovery plans) and conducting scanning as required.[8] VA Directive 6517 and its accompanying handbook should also be updated to reflect the revised NIST requirements.[9] The OIG further recommended that the assistant secretary continue to improve criteria and its processes for submitting claims to recoup service credits and assign roles and responsibilities for submitting claims and monitoring outcomes.

VA Management Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with all five recommendations and submitted responsive action plans. The OIG will close the recommendations when OIT provides sufficient evidence demonstrating progress in addressing

[8] NIST Special Publication 800-53.

[9] VA Directive 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016; VA Handbook 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016; NIST Special Publication 800-53.

the intent of the recommendations and the issues identified. The OIG incorporated clarifying wording responsive to VA comments to the report. In a few instances, proposed edits were not made because, for example, both hosted and infrastructure systems required remediation (instead of edits indicating just hosted systems). Appendix D includes the full text of the assistant secretary's comments.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

ATO	authority to operate
ECSO	Enterprise Cloud Solutions Office
eMASS	Enterprise Mission Assurance Support Service
FISMA	Federal Information Security Modernization Act
ISSO	information system security officer
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
VAEC	Veterans Affairs Enterprise Cloud

Introduction

In fiscal year 2023, VA had budgetary resources of more than $378 billion to serve veterans and their families by providing benefits that include disability compensation, pension, education, training, health care, home loans, insurance, and burial.[10] According to its strategic plan, one of VA's objectives is to deliver systems that ensure convenient and secure access and enhance the delivery of these benefits, care, and services.[11] In addition, its strategic plan indicated desired outcomes for information technology and security to include improving cybersecurity, privacy protections, and resiliency; making certain that information and data are secure and easy to share with partners; and reducing system downtime. As such, according to VA's enterprise roadmap, it is undergoing an information technology modernization and digital transformation to enable improved customer service and interoperability with external partners by optimizing the cloud.[12]

VA rents access to the "cloud," which refers to technology solutions provided by outside vendors.[13] The cloud offers access to fully featured applications, software development and deployment environments, and computing infrastructure assets such as network-accessible data storage and processing. When developing cloud systems, federal agencies are responsible for following the National Institute of Standards and Technology (NIST) risk management framework: a comprehensive, flexible, repeatable, and measurable seven-step process designed to protect the confidentiality, integrity, and availability of information.[14] Agencies should also work to ensure an appropriate balance between the number and strength of controls and the risks associated with cloud computing solutions.[15] Further, key security considerations include the need to maintain security management practices, controls, and accountability over the privacy and security of data and applications.[16]

VA developed a cloud computing solution called the Veterans Affairs Enterprise Cloud (VAEC). According to VA, the VAEC enables VA to deliver services to veterans in a fast, cost-effective, and efficient manner. The VAEC is based on contracts with two cloud service providers, referred to in this report as vendors A and B. The VAEC hosts systems used by employees, veterans, contractors, and partners and supports the delivery of health care, compensation benefits, and

[10] "Department of Veterans Affairs (VA)" (web page), USASpending.gov, accessed June 6, 2023, https://www.usaspending.gov/agency/department-of-veterans-affairs?fy=2023.

[11] VA, *Department of Veterans Affairs Fiscal Years 2022-28 Strategic Plan*, n.d.

[12] Office of Information and Technology, *FY [Fiscal Year] 2020–2026 VA Enterprise Roadmap*, March 31, 2020.

[13] "Federal Cloud Computing Strategy" (website), Office of Management and Budget, accessed April 4, 2023, https://cloud.cio.gov/strategy/.

[14] NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, December 10, 2020.

[15] US Chief Information Officer, *Federal Cloud Computing Strategy*, February 8, 2011.

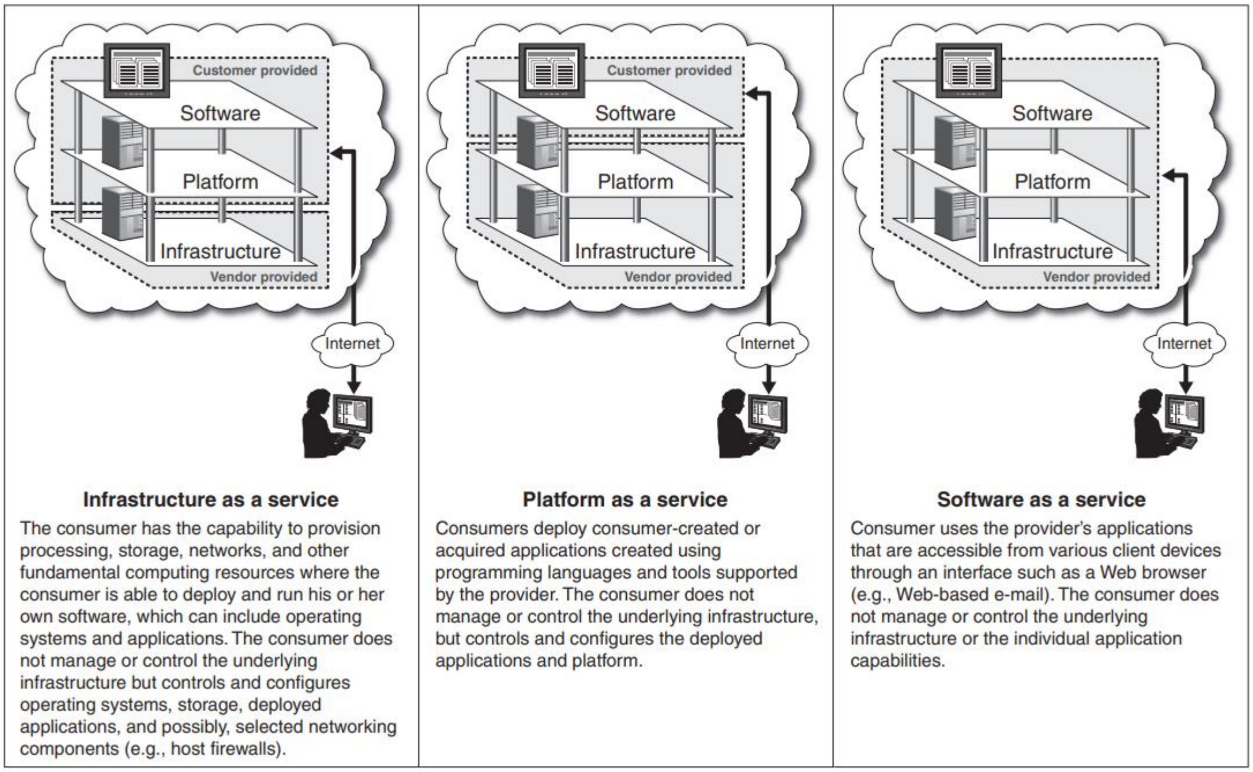
[16] US Chief Information Officer, *Federal Cloud Computing Strategy*.

home loan guarantees for veterans. The VAEC is also being used to help expand cloud-based telework, telehealth, and storage capabilities across VA. To access the VAEC, the department purchases cloud service provider credits from two vendors, referred to in this report as service credit vendors. VA also purchases software licenses, software maintenance, and technical support from service credit vendors. If a provider does not achieve and maintain agreed-upon service levels, VA may be eligible to recoup a percentage of applicable monthly service charges as a credit.

The VA Office of Inspector General (OIG) conducted this audit to ascertain whether VA is effectively assessing and monitoring security and privacy controls for cloud computing consistent with federal guidance. The audit team also examined VA's process for monitoring cloud service performance.

Overview of the Veterans Affairs Enterprise Cloud

Agencies can select different cloud services to support their missions. These services can range from a basic computing infrastructure on which agencies run their own software to a full computing infrastructure that includes vendor software applications. Figure 1 shows the VAEC's service models, which enable project teams to rapidly develop and deploy VA cloud applications.



Infrastructure as a service

The consumer has the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run his or her own software, which can include operating systems and applications. The consumer does not manage or control the underlying infrastructure but controls and configures operating systems, storage, deployed applications, and possibly, selected networking components (e.g., host firewalls).

Platform as a service

Consumers deploy consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying infrastructure, but controls and configures the deployed applications and platform.

Software as a service

Consumer uses the provider's applications that are accessible from various client devices through an interface such as a Web browser (e.g., Web-based e-mail). The consumer does not manage or control the underlying infrastructure or the individual application capabilities.

Figure 1. *Cloud computing service models.*
Source: Government Accountability Office, Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing, GAO-10-513, May 2010.

Six systems comprise the VAEC's infrastructure as a service, referred to in this report as "infrastructure systems" (three each from vendors A and B). VA does not manage or control the underlying cloud infrastructure for these six systems; rather, it has control over operating systems, storage, and deployed applications that VA provides in the cloud. The VAEC hosts more than 200 systems that can be classified as platform or software as a service; they are controlled through program offices. However, the audit team found some systems were not classified at all or were misclassified in Enterprise Mission Assurance Support Service (eMASS) as both platform and software as a service when they should have been labeled as one or the other.[17] Therefore, for the purpose of this audit, the team uses the term "hosted systems" when referring to non-infrastructure systems that can be platform or software as a service. The team reviewed a sample of seven hosted systems.[18]

Enterprise Cloud Solutions Office

The Office of Information and Technology's (OIT) Enterprise Cloud Solutions Office (ECSO) is the governing authority for VA cloud systems; it developed and operates the VAEC. ECSO's mission is to implement the VAEC and deliver secure and seamless cloud functionality to support the entire VA enterprise. ECSO also provides specialized expertise in and has oversight responsibilities for VAEC architecture, security, and operations to assist project teams either developing new systems or applications, or migrating legacy systems or applications to the VAEC. In addition, the office purchases cloud service provider credits from two service credit vendors that allow them to use the VAEC. VA staff have established service-level agreements with the vendors that outline performance expectations, availability requirements, and key processes and remedies for any evaluations. ECSO and VA's Technology Acquisition Center are responsible for monitoring these agreements.

Cloud Computing Authorities

There are several cloud computing authorities relevant to this audit. Table 1 provides an overview of these authorities, while the sections following the table provide key points to provide support and context for the team's finding.

[17] As detailed in later sections, eMASS is a web-based application tool used to generate a system security authorization package and automates the process for setting security controls.

[18] After excluding hybrid systems, systems without authorization to operate, and other categories defined in appendix C, the team selected seven of the remaining 148 hosted systems. Together with the six infrastructure systems, this accounted for the 13 systems on which the OIG based its findings for this report. Additional details of the team's methodology can be found in appendix B, and more information on its statistical sampling is provided in appendix C.

Table 1. Overview of Relevant Cloud Computing Authorities

Authority	Overview
Federal Information Security Modernization Act (FISMA)	FISMA requires agencies to protect federal information.
NIST	NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of US industry, federal agencies, and the public.
VA guidance	VA Directives 6500 and 6517 and their accompanying handbooks establish policies to ensure compliance with NIST and other relevant federal guidance.

Source: VA OIG summary of relevant authorities.

FISMA requires that NIST develops standards and guidelines for information security for federal agencies, including minimum requirements for providing adequate information security for all agency operations and assets, including cloud computing.[19] In response to the FISMA requirements, NIST developed a cloud computing technology roadmap and standards.[20]

Cloud Computing Security Risks

NIST and VA guidance specify the applicable security and privacy controls based on the risk level of the data in an information system.[21] Risk levels relate to the level of privacy and security needed so the information or data are not improperly disclosed or misused and consider the adverse effects on VA's operations, assets, or the individuals it identifies in the system should a breach occur. The framework begins by defining essential activities that personnel at all levels of the organization should know to prepare to manage security and privacy risks. This includes identifying and assigning key risk management roles, establishing a risk management strategy, and assessing organization-wide security and privacy risks.

The next step determines the information system security categorization level, which includes conducting a privacy threshold analysis and a privacy impact assessment. Both the privacy analysis and assessment are used to mitigate the risk of unauthorized access, data loss or misuse, or disclosure of information, and they help ensure that systems or applications that store sensitive information have the right level of security.[22] Specifically, a privacy threshold analysis is required to identify information technology systems that include sensitive information such as

[19] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) § 3553(b)(2).

[20] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011.

[21] NIST Special Publication 800-53; VA Handbook 6500, *Risk Management Framework for VA Information Systems–Tier 3: VA Information Security Program*, February 24, 2021.

[22] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, April 2010; VA Handbook 6508.1, *Procedures for Privacy Threshold Analysis and Privacy Impact Assessment*, July 30, 2015.

personally identifiable information and assess whether the system needs a privacy impact assessment. A privacy impact assessment identifies privacy risks and their effects for an information system. The assessment should address and mitigate risk at every stage of system development. It is required before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form. VA uses the privacy analysis and assessment to evaluate the information type in the system and determine the security categorization level.[23]

Establishing an appropriate security category requires determining the potential impact for each security objective associated with a particular information type. The security categorization is based on the security objectives—confidentiality, integrity, and availability—within the system. A 2019 Government Accountability Office report recognized that the use of cloud computing poses cybersecurity risks.[24] According to the report, risks arise when agencies and cloud service providers do not effectively implement security and privacy controls over cloud services. Weaknesses in these controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information. A breach of any security objective could have a low (limited), moderate (serious), or high (severe or catastrophic) adverse effect on organizational operations, assets, or individuals.[25]

Enterprise Mission Assurance Support Service

As noted earlier, VA uses eMASS (a web-based application tool) to generate a system security authorization package and automate the process for setting security controls for VA systems within the risk management framework. This includes dashboard reporting, workflow automation, and continuous monitoring that replicates the steps in the risk management framework. The capabilities of eMASS include establishing process controls for obtaining authorizations to operate applications and systems. In addition, eMASS automatically calculates the confidentiality, integrity, and availability levels for some information types based on risk assessment results.

Risk Management Framework

The NIST framework provides guidance for managing risks throughout information system design, development, implementation, operation, and disposal, and in the environments in which

[23] NIST, *Standards for Security Categorization of Federal Information and Information Systems,* Federal Information Processing Standards Publication (FIPS Pub) 199, February 2004. An information type is a category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, executive order, directive, policy, or regulation.

[24] Government Accountability Office, *Computing Security*, GAO-20-126, December 12, 2019.

[25] NIST, FIPS Pub 199.

those systems operate.[26] Federal agencies, contractors, and other entities that employ or operate a federal information system use NIST risk management standards and guidelines to develop and implement a risk-based approach to securing information. The framework provides a flexible, holistic, and repeatable seven-step process and links to a suite of NIST standards and guidelines to help programs meet FISMA requirements. This is an iterative process. After completing steps one through six, entities must continually monitor the controls, which could result in the need to restart the cycle. For example, if a change or deficiency is identified, then the entity will need to go back to step one. Figure 2 illustrates the seven-step process.

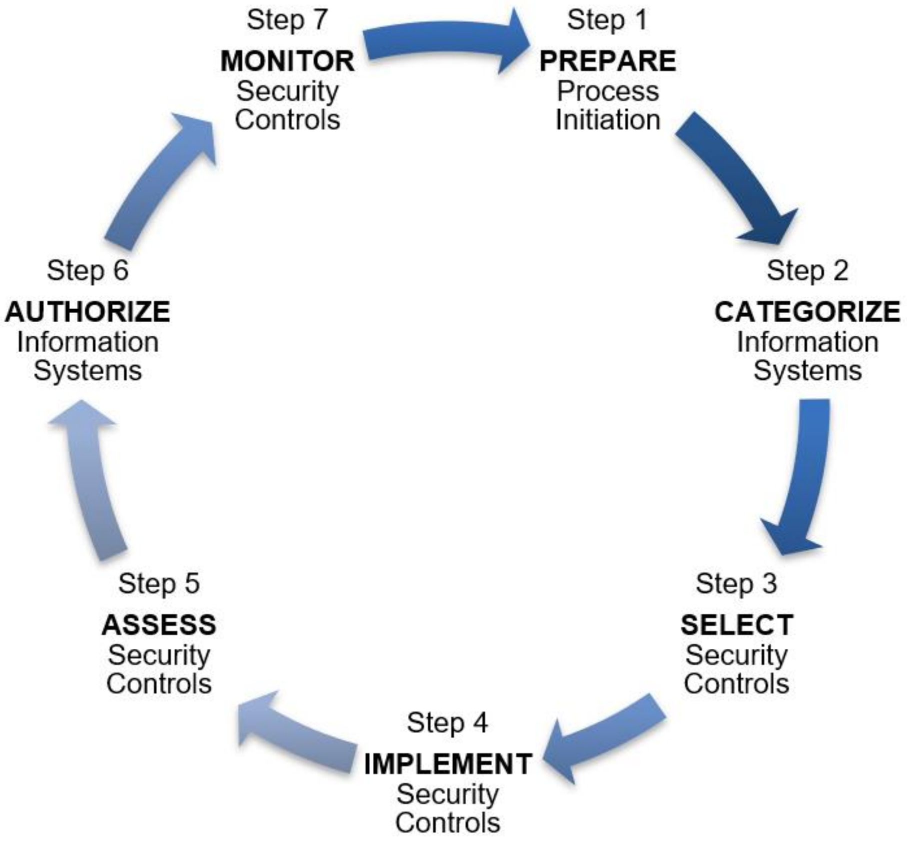


Figure 2. *OIG overview of the risk management framework.*
Source: *NIST Special Publication 800-53. For additional details on the risk management framework, see appendix A.*

Prior Related OIG Reports

Since 2017, the OIG's FISMA audits have repeatedly disclosed deficiencies related to VA's management of security within its cloud environment. In a May 2023 audit report, the OIG found that VA had not consistently implemented components of its agencywide information security

[26] NIST Special Publication 800-53.

risk management program to meet FISMA requirements.[27] The OIG identified several instances when systems did not undergo an independent assessment of security and privacy controls before being granted an authority to operate (ATO).[28] The OIG recommended VA implement an independent security and privacy control assessment process to evaluate the effectiveness of controls before granting authorization decisions. Further, the OIG recommended implementing an improved continuous monitoring program in accordance with NIST's risk management framework.

[27] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023.

[28] NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations,* December 2018. Authority to operate is a formal declaration by a designated approving official or entity that authorizes operation of an information system and explicitly accepts the risk to the agency.

Results and Recommendations

Finding 1: OIT Needs to Improve Oversight of the VAEC Systems

In September 2020, NIST updated its guidance and made considerable revisions to its security and privacy controls; however, as of June 2023, VA had not implemented these changes.[29] This occurred because OIT did not ensure policies and procedures reflected up-to-date security and privacy controls. Required controls help VA protect information systems and their contents from "unauthorized access, use, disclosure, disruption, modification, or destruction," to help provide confidentiality and integrity while maintaining data availability.[30] Although OIT staff informed the audit team that they are working on implementation, the team found some systems were not yet compliant and the targeted completion date for updated guidance was December 2023.

The audit team did not identify deficiencies in how VA completed steps 1–6 of the NIST risk management framework for the VAEC. As to step 7, continuous monitoring, the team did find weaknesses in documentation. Without documented assessments, VA lacks assurance that the VAEC systems are protected. Monitoring involves performing ongoing assessments and analyzing the effectiveness of security and privacy controls.[31] VA must ensure VAEC systems include the necessary security and privacy controls.[32]

The following elements support the OIG's finding:

- OIT did not apply updated NIST security controls to all VAEC systems.
- OIT needs to ensure continuous monitoring of the VAEC systems.

What the OIG Did

The audit team reviewed applicable laws, regulations, policies, and procedural guidance to determine if VA is effectively assessing and monitoring security and privacy controls for cloud computing. The team also reviewed documentation in eMASS to determine if appropriate controls were assigned for each system and if continuous monitoring was occurring. The team interviewed OIT staff including system stewards, information system owners, information system security officers (ISSOs), and authorizing officials. The team reviewed six infrastructure

[29] VA requested in its technical comments that details be provided on the specific revision. Accordingly, the OIG included that it referred to Special Publication 800-53 (revision 5).

[30] NIST Special Publication 800-37.

[31] Office of Information Security, "Authorization Requirements" (standard operating procedures version 1.41), October 13, 2022.

[32] NIST Special Publication 800-53; VA Handbook 6500.

systems (three each from vendors A and B) and seven hosted systems. For details on the audit scope and sampling methodology, see appendixes B and C.

OIT Did Not Apply Updated NIST Security Controls to All VAEC Systems

The OIG determined OIT did not effectively oversee its NIST risk management framework process. OIT is required by federal guidance and VA policy to ensure systems hosted on the VAEC and those that are part of the VAEC infrastructure as a service include the necessary security and privacy controls.[33] NIST designed security and privacy controls to protect systems and the information they contain commensurate with the risk associated with their misuse or unauthorized disclosure; similar controls are grouped into families. Each family contains security and privacy controls that are related to a specific topic that may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms. For example, access family controls include policy and procedures on account management, enforcement (who is admitted into the system), separation of duties (no one person can both act and authorize that action), and least privilege (the minimum access needed to perform one's duties). In total, there are 20 families of security and privacy controls.

As stated above, to evaluate whether OIT applied the required security and privacy controls, the audit team reviewed 13 systems: six infrastructure and a sample of seven systems (from a population of 148 hosted systems) on the VAEC. Of the seven hosted systems, six were selected randomly and one was selected judgmentally due to identified risks by VA.[34] During the research phase, the team reviewed multiple systems and found several raised security concerns. Then, in an interview with the team, the lead cybersecurity analyst mentioned that one of the systems under review had been taken off the network due to security concerns and put back on after it was granted an ATO with conditions. Therefore, the team judgmentally included this system in its review. The team found the 13 systems contained sufficient controls for 18 of the 20 required security and privacy control families.

However, none of the 13 systems contained controls related to two risk management control families: (1) personally identifiable information processing and transparency controls, and (2) supply chain risk management controls.[35] These two control families were added when NIST 800-53 was updated (to revision five) in September 2020. This revision considerably updated security and privacy controls, superseding prior versions.[36] Based on the results of the

[33] NIST Special Publication 800-53; VA Handbook 6500.

[34] See appendixes B and C.

[35] NIST Special Publication 800-53 identifies eight personally identifiable information processing and transparency controls and 12 supply chain risk management controls.

[36] NIST Special Publication 800-53; VA Handbook 6500.

sample review, the audit team estimated at least 101 of the 148 systems hosted on the VAEC did not include any controls from these two families.

The personally identifiable information processing and transparency controls focus on consent and privacy for user data and are designed to safeguard sensitive information. For example, one control helps "organizations take steps to eliminate unnecessary uses of social security numbers and other sensitive information." Another control ensures "organizations use privacy notices to inform individuals about how, under what authority, and for what purpose their personally identifiable information is processed." These and other family controls help an organization lower the risks associated with data breaches by having the right policies in place to store and manage personally identifiable information.

The supply chain risk management controls help mitigate the risk of the system being compromised. For example, one control provides tools and techniques that "may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle." Another control implements "safeguards or countermeasures to eliminate or reduce exploitable vulnerabilities and risk to an acceptable level."

Although the system steward and information system owner are responsible for assigning the correct controls, there were two authorizing officials who were ultimately responsible for ensuring the 13 systems reviewed had the correct controls assigned. All systems placed on the VAEC are also reviewed by ECSO staff to ensure the ATO process has been followed. According to the information technology specialist leading VA's transition to the revised standards, OIT completed an impact analysis in August 2021 to determine how the NIST update affected systems and stakeholders. The specialist also stated OIT was still in the process of updating policy to align with NIST standards, which includes working on training, control testing, and policy updates. OIT staff anticipated the updates to policy will be completed by December 2023. While the OIG recognizes that it takes time for VA to update its guidance, it should develop strategies to improve this process in the future. As previously discussed, without the required controls, veterans' personally identifiable information and VA systems are at an increased risk of being compromised.

OIT Needs to Ensure Continuous Monitoring of the VAEC Systems

According to NIST, continuous monitoring is ongoing awareness of information security, vulnerabilities, and threats. That information can help support organizational risk management and related decision-making. Monitoring involves having plans for areas such as contingency, incident response, and disaster recovery:

- **Contingency plans** document how the organization will operate when various conditions or events occur.

- **Incident response plans** help with ensuring rapid detection of incidents that minimize loss, correcting the weakness exploited, and restoring services.
- **Disaster recovery plans** are for processing critical applications in the event of a major hardware or software failure or destruction of facilities.[37]

System stewards and information system owners are required to manage and test all plans on a yearly basis (or when a significant change occurs). They are also required to document evidence of the tests in eMASS.[38] The audit team found that some systems did not have all documented contingency, incident response, or disaster plans; three systems were missing at least one plan. In addition, the audit team found that multiple systems did not have documented tests. Of note, some systems had a record of testing even though they did not have a documented plan. Table 2 provides an overview of the team's findings.

Table 2. Overview of VAEC System Monitoring

Category	Compliant	Noncompliant
Contingency plan documented	12	1
Contingency plan testing	9	4
Incident response plan documented	11	2
Incident response testing	11	2
Disaster recovery plan documented	12	1
Disaster recovery plan testing	5	8

Source: VA OIG analysis of eMASS data as of January 2023.

NIST and VA policy require documentation of continuous monitoring to maintain a system's ATO.[39] In addition to having the required plans and testing them, VA is required to conduct vulnerability scans. These scans allow organizations to identify system vulnerabilities related to security. These automated monthly scans are required and are intended to identify potential security and privacy concerns so action can be taken to protect the data. The cybersecurity operations center is required to perform this test monthly, and evidence of this testing is required to be uploaded into eMASS after it is completed by the system steward or the information security officer per the eMASS standard operating procedures.[40] The audit team found nine of the 13 systems reviewed were missing the scan documentation.

[37] "Glossary" (webpage), NIST Computer Security Resource Center, accessed June 14, 2023, https://csrc.nist.gov/glossary.

[38] VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021.

[39] NIST Special Publication 800-53; VA Directive 6500.

[40] Office of Information Security, "Authorization Requirements."

Although some interviewees indicated the scans were completed but the documentation had not been uploaded, the audit team could not verify that the scans were conducted. As a result of not uploading documents, VA lacks assurance that the controls are working as designed. Based on the team's findings from its sample, an estimated 123 of the 148 systems hosted on the VAEC did not have proof of continuous monitoring.[41]

Finding 1 Conclusion

The audit team did not identify deficiencies in how VA completed the first six steps of the NIST risk management framework for the VAEC. However, the team identified deficiencies in the seventh step related to monitoring. Specifically, OIT is not fully meeting its responsibilities for implementing security and privacy controls in the areas of personally identifiable information and supply chain management and documenting monthly scans of the VAEC systems.[42] In addition, VA's policies and procedures do not fully reflect updated requirements. The OIG recognizes that OIT is in the process of updating policy, procedures, and guidance to align with NIST standards. However, the omitted security and privacy controls undermine VA's ability to protect personally identifiable information and systems from being compromised. Although the OIG is unaware of any incursions due to the identified deficiencies, OIT must improve its oversight of continuous monitoring of the VAEC systems to ensure they are protected.

Recommendations 1–2

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

1. Develop a timeline for updating the security and privacy guidance to reflect the latest revisions to the National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and address identified weaknesses with personally identifiable information and supply chain management.
2. Establish a mechanism to ensure continuous monitoring of VA Enterprise Cloud systems to include having and testing contingency, incident response, and disaster recovery plans and conducting scanning as required.

[41] For details on the sampling methodology, see appendix C.

[42] NIST Special Publication 800-53; VA Handbook 6500.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 2 and submitted action plans with a target completion date of September 30, 2024. Appendix D includes the full text of the assistant secretary’s comments.

In response to recommendation 1, the assistant secretary stated that OIT has developed a projected timeline for updating security and privacy guidance to reflect the latest revisions to NIST Special Publication 800-53. The assistant secretary indicated OIT’s Infrastructure Operations will focus on prioritizing the scope of controls to those that contain a significant change and on control families that have been identified as an area of improvement for VA such as personally identifiable information and supply chain management.

For recommendation 2, the assistant secretary stated VA policies and processes are already in place to address this recommendation. However, he indicated the Office of Information Security’s VA Cloud Security Program Office will work with stakeholders to develop a validation process to help mitigate noncompliance.

The assistant secretary provided technical comments to clarify some of the wording and to propose edits related to oversight responsibility and to focus on hosted systems.

OIG Response

The assistant secretary’s planned actions are responsive to recommendations 1 and 2. The OIG will close the recommendations when OIT provides sufficient evidence demonstrating progress in addressing the intent of the recommendations and the issues identified. The OIG incorporated clarifying wording where appropriate and supported to address technical comments from the assistant secretary. The OIG did not make the proposed change from VAEC systems to VAEC “hosted” systems, as this would exclude the infrastructure systems. As detailed in the report, both the infrastructure and hosted systems require remediation. Regarding the effective oversight of security and privacy controls, the OIG did not make the proposed change indicating that the “applications systems hosted on the VAEC” are responsible under a “shared responsibility model.” The OIG maintains that OIT, not applications systems, is responsible for this oversight. Further, no documentation or explanation was provided regarding a shared responsibility model.

Finding 2: VA Did Not Request Recoupment of Service Credits for Cloud Service Outages for Nine of Ten Outages

According to agreements with vendors A and B, if the provider does not achieve and maintain agreed-upon service levels, then VA may be eligible for recoupment of a percentage of applicable monthly service charges. Service levels are based on performance criteria such as guaranteed availability, which include cloud service provider commitments for uptime and connectivity for each service. Service-level agreements with ECSO outline performance expectations, availability requirements, and key processes and remedies for any deficiencies identified in evaluations. The audit team found the VAEC had 201 major incidents between June 2019 and December 2022. As detailed below, OIT defines a major incident as a high-urgency outage affecting many users or VA services. Vendor A was at fault for eight cloud outages, vendor B was responsible for two, and VA for the remaining. The audit team found VA did not request recoupment of service credits for nine of the 10 vendor outages.

As a steward of taxpayer dollars, VA has a fiscal responsibility to request recoupment of service credits or justify not doing so. Failure to request recoupment on the nine outages occurred, in part, because VA did not have a process to identify, document, and submit cloud service incidents for potential recoupment. Further, VA did not identify who was responsible for submitting the recoupment requests to the cloud service providers. Without a formal process, VA is at risk of not receiving credits to which it is entitled. ECSO officials informed the audit team they were aware that they should be submitting recoupment requests and stated they were planning to implement a process. In addition, the service-level agreements do not include a reimbursement structure that would allow VA to determine the potential amount that could have been credited to the department. According to an OIT official, the cloud service providers make that determination. For the one service credit recoupment, VA received about $114,000.

What the OIG Did

The audit team reviewed VA's service-level agreements with both vendors and the contracts for purchasing the service credits. In addition to reviewing the documents, the team interviewed the contracting officers, contracting officers' representatives, and the ECSO leaders and staff with service-level agreement oversight responsibilities. The team requested and reviewed documentation associated with outages involving cloud services dating back to 2019.

VA Did Not Have a Process for Submitting Service Claims for System Outages

Service-level agreements with the VAEC's vendors are based on performance criteria such as guaranteed availability, which include cloud service provider commitments for uptime and connectivity for each service. As stated above, each service-level agreement contains an expected level of service. For example, the vendor A agreements generally establish an expected level of service of 99.90 percent to 99.99 percent uptime depending on the service. For the vendor B agreements, the expected level of service falls between 95 percent and 99.9 percent depending on the service. According to vendor A's service-level agreement, an incident means any single event or set of events that results in an outage. An outage is when an end user is unable to log in to their information system. An outage does not include unavailability due to network, hardware, or service maintenance or upgrades. Table 3 shows the accepted service availability standards.

Table 3. Accepted Service Availability Standards

Percent availability	Duration of outage per year (hours)	Duration of outage per month (minutes)
99.99	0.88	4.38
99.95	4.38	21.91
99.90	8.77	43.83
99.00	87.66	438.30
95.00	438.30	2,191.50

Source: VA OIG calculation of accepted outage time for different services.

Per the service-level agreement with vendor A, for a recoupment request to be considered, VA must submit a claim and supporting documentation to the vendor for review. The claim must be submitted to the vendor within two months of the end of the billing month in which the outage occurred. The service credit will be based on the estimated retail price for the applicable service, as determined by vendor A in its reasonable discretion; VA has no control over the amount of the service credit. The agreement with vendor B contains a similar process.

According to the service-level agreements, incidents that result in outages are potentially eligible for service credit recoupment. OIT guidance defines a major incident as a "high-impact, high-urgency outage that affects many users, depriving VA of crucial services such as patient care, benefits processing, or cemetery operations, demanding a response beyond the routine incident management process."[43] As previously stated, between June 2019 and December 2022, the VAEC had 201 major incidents. Of these, eight were for vendor A services and two were for vendor B services. The remaining were attributed to VA. Based on an interview with ECSO's acting director for Application Hosting, Cloud and Edge Solutions Infrastructure Operations, he was aware of three of the 10 major incidents.

Also according to OIT guidance, major incidents are categorized as either priority 1 (critical) or priority 2 (high); the team found six priority 1 and four priority 2 incidents.[44] Priority 1 incidents

[43] OIT, *Major Incident Management Process Version 1.0*, June 25, 2021.

[44] The other categories are priority 3 (moderate) and priority 4 (low).

affect one of the following: OIT, VA Central Office, the Veterans Benefits Administration, the Veterans Health Administration, the National Cemetery Administration, an application/resource that is affecting staff nationally, or enterprise applications. A priority 2 incident impacts a single facility or region within the Veterans Benefits Administration, the Veterans Health Administration, or the National Cemetery Administration, or applications specific to a single facility.

The longest priority 1 incident involving vendor A lasted 9.5 hours and resulted in users being unable to access multiple cloud-based applications such as the Master Veterans Index, Joint Longitudinal Viewer (for patient health records), Veterans Benefits Management System, Person Service Identity Management, and Data Access Services. The longest priority 1 incident involving vendor B was for 3.25 hours and resulted in users across VA being unable to access approximately 67 applications and services. Vendor A’s longest priority 2 incident lasted 11.72 hours and affected usage in one region. Vendor B did not have any priority 2 incidents. The audit team did not determine whether these incidents exceeded the accepted service availability standards seen in table 3; according to an OIT official, the vendors make that determination.

VA requires permanent directives and handbooks to be recertified within five years of issuance to ensure the current policy and procedures are consistent with other enterprise directives and handbooks.[45] However, the audit team found VA Directive 6517 on risk management for cloud computing and its accompanying handbook were not updated after five years and did not address who was responsible for monitoring service agreements or service levels.[46] In addition, there were no policies, procedures, or mechanisms in place to trigger a recoupment request. According to the cloud security lead, OIT was aware that the directive and its accompanying handbook were outdated and they have been in the process of updating this guidance. The update process requires multiple offices to review the guidance and provide comments. The Office of Information Security then reviews the comments and decides if changes are warranted. According to the cloud security lead, this process has occurred repeatedly and additional delays were due to the handbook needing to be developed before the directive could be approved. Without clear processes for determining when an outage warrants a request for recoupment, VA is potentially not receiving credits to which it is entitled.

During an October 2022 interview with the acting director of ECSO’s Applications Hosting, Cloud and Edge Solutions, the audit team discussed the lack of service credit recoupment and identified potential outages that could be eligible for recoupment. In November 2022, ECSO staff requested a credit recoupment from vendor A for one identified outage; VA received a

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

[46] VA Directive 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016; VA Handbook 6517, *Risk Management Framework for Cloud Computing Services*, November 15, 2016.

service credit recoupment of about $114,000 in December 2022. The team was made aware of the request and recoupment in a July 2023 meeting. At this meeting, the director of ECSO also informed the team that ECSO had developed a standard operating procedure for recoupment of service credits. However, the team noted the document provided does not identify roles, responsibilities, and when it should be initiated.

Finding 2 Conclusion

Despite being eligible to request recoupment of service credits, VA did not request them for nine of 10 cloud service outages between December 2020 and December 2022. This occurred because VA has not identified who is responsible for submitting the recoupment requests to the vendors. After meeting with the audit team, ECSO staff submitted the one claim and created a standard operating procedure for requesting recoupment of service credits. However, ECSO did not include information sufficient to identify, document, and submit cloud service incidents for potential recoupment of service credits and assign roles and responsibilities. Until VA finishes refining the standard operating procedure, it will remain at risk of not receiving service credits to which it is entitled. While VA recouped about $114,000 from one outage, the team was unable to determine how the amount was calculated; according to an ECSO official, the cloud service providers make that determination.

Recommendations 3–5

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

3. Ensure VA Directive and Handbook 6517 are updated to reflect the revised National Institute of Standards and Technology requirements.
4. Continue to improve criteria and processes for submitting claims for recoupment of service credits.
5. Assign roles and responsibilities for submitting claims for service credits and monitoring outcomes.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 3 through 5 and submitted action plans for each recommendation.

In response to recommendation 3, the assistant secretary said OIT’s Infrastructure Operations will work with the Office of Information Security subject matter experts for cloud policy to ensure the revisions for VA Directive 6517 on risk management for cloud computing and the associated handbook are aligned with NIST requirements and cybersecurity framework. The target completion date is September 30, 2024.

For recommendation 4, the assistant secretary indicated VA is in the process of refining its newly established standard operating procedure to minimize the risk of VA not receiving service credit recoupments and anticipates completion by October 15, 2023.

Finally, in response to recommendation 5, the assistant secretary reported OIT's Infrastructure Operations developed and utilized a standard operating procedure for submitting claims for service credits and monitoring outcomes. Additionally, he stated VA is in the process of refining the newly established standard operating procedure. The target completion date is also October 15, 2023.

The assistant secretary also provided technical comments to clarify some of the wording and to propose edits related to refining its newly established standard operating procedure and improving its criteria and processes for submitting claims to recoup service credits.

OIG Response

The assistant secretary's planned actions are responsive to recommendations 3 through 5. The OIG will close the recommendations when OIT provides sufficient evidence demonstrating progress in addressing the intent of the recommendations. The OIG incorporated clarifying wording where appropriate and supported to address the two technical comments from the assistant secretary.

Appendix A: Risk Management Framework

The National Institute of Standards and Technology's (NIST) risk management framework provides guidance for managing risk throughout information system design, development, implementation, operation, and disposal, and in the environments in which those systems operate.[47]

Step 1: Prepare

The system steward or the information system owner takes the first step in the risk management framework by preparing security and privacy plans, identifying key risk management roles, developing an organization-wide management strategy, and formulating a continuous monitoring strategy.

Step 2: Categorize

The system steward or the information system owner reviews the information processed, stored, and transmitted by the system and determines the adverse impact of loss of confidentiality, integrity, and availability of the system. The information system security officer (ISSO) also reviews this information and coordinates with the system steward and information system owner and provides input.

Step 3: Select

Next, the system steward or information system owner selects, tailors, and documents the controls necessary to protect the system and organization in line with the risk in the security and privacy plan. Systems inherit some of the security and privacy controls from the cloud service provider, which the system steward and information system owner document. The system steward or information system owner also document any additional controls based on the security and privacy plans. Once the controls are selected and documented, the ISSO approves them. The strategy for continuous monitoring is also further developed and refined in coordination with the ISSO.

Step 4: Implement

After the controls have been selected, the system steward or the information system owner implements the controls for the system and the organization. The security and privacy plans created during the process are also updated to reflect that the controls have been implemented. The ISSO performs a review of the control implementation.

[47] NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, December 10, 2020.

Step 5: Assess

The system steward or information system owner assesses if the controls are operating as intended and meet the security and privacy requirements of the system. A control assessor determines if the submitted security and privacy controls are working as intended and approves the validation.

Step 6: Authorize

An official authorizes the system by issuing an “authority to operate” (ATO). The authorizing official confirms that the system or application has passed all requirements to become operational. The ATO is a formal declaration that sanctions the operation of a business product and explicitly accepts the risk to the agency. The length of an ATO varies based on the risks of the system as determined by the authorizing official. Some ATOs are issued for as few as 90 days, and some are issued for as long as three years, with the majority being issued for one year. After the ATO expires, the system goes back to step one and all following steps must be repeated.

Step 7: Monitor

While a system has an active ATO, the system steward or information system owner needs to maintain ongoing situational awareness regarding the security and privacy posture of the system. They also need to ensure the system supports the risks and continued management decisions that may have an impact on the system. Continuous monitoring takes many forms such as running scans to ensure the system continues to operate as designed. The ISSO is also involved with monitoring the system for security threats and ensuring the controls are designed to protect against any new risks.

Appendix B: Scope and Methodology

Scope

The Office of Inspector General (OIG) performed its audit work from August 2022 through July 2023 to evaluate, identify, and analyze VA's cloud infrastructure to ensure VA is protected from a variety of security and privacy risks, threats, and weaknesses.

Methodology

To determine if the appropriate security and privacy risk standards were applied, the audit team reviewed VA systems that went through the authority to operate (ATO) process and were hosted on the Veterans Affairs Enterprise Cloud (VAEC) as of the audit start date. The team developed a checklist to assess if each system contained the necessary documentation and approvals within the VAEC based on security and privacy risk standards and guidelines. As part of the checklist, the team reviewed supporting documentation to determine if the correct system classification was assigned. To determine whether the VAEC systems had the appropriate controls, the team reviewed documents uploaded to the Enterprise Mission Assurance Support Service (eMASS) to support security and privacy control compliance; the team compared those documents with National Institute of Standards and Technology (NIST) and VA requirements. Further, by reviewing the documents, the team evaluated whether continuous monitoring was in place.

In addition, the audit team conducted interviews with Office of Information and Technology (OIT) staff to determine their process for reviewing authorization packages to ensure they are following VA's policies and procedures. Team members also interviewed authorizing officials, Enterprise Cloud Solutions Office (ECSO) staff members, information system owners, ISSOs, and system stewards. Further, the audit team obtained and reviewed OIT contracts with both vendors and service-level agreements with vendor A and vendor B. Finally, the team interviewed the contracting officers and contracting officers' representatives to assess VA's processes for monitoring cloud service providers.

Internal Controls

The audit team assessed the internal controls of the VAEC significant to the audit objective. This included an assessment of the five internal control components to include control environment, risk assessment, control activities, information and communication, and monitoring.[48] In addition, the team reviewed the principles of internal controls as associated with the objective. The team identified the following two components and three principles as significant to the

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

objective.[49] The team identified internal control weaknesses during this audit and proposed recommendations to address the following control deficiencies:

- Component 3: Control Activities
    - Principle 12: Management should implement control activities through policies.
- Component 5: Monitoring
    - Principle 16: Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
    - Principle 17: Management should remediate identified internal control deficiencies on a timely basis.

Fraud Assessment

The audit team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant within the context of the audit objectives, could occur during this audit. The team exercised due diligence in staying alert to any fraud indicators by

- reviewing a sample of systems to determine if there was a risk of noncompliance with provisions of laws and regulations and
- reviewing cloud service provider contract terms and deliverables to ensure VA policies were followed.

The OIG did not identify any instances of fraud or potential fraud during this audit.

Data Reliability

The audit team conducted data reliability tests throughout the fieldwork phase of the audit. The team requested the statistician develop a random sample to test data reliability for 10 non-selected systems. The statistician included 10 data reliability primary samples and 10 data reliability backup samples. The 10 systems reviewed for the data reliability test were compared in eMASS and the VAEC system list to verify the data export did not contain missing or erroneous data. For the 10 systems reviewed, all data on the spreadsheet, eMASS, and the VAEC system list were consistent. The team also used a data reliability checklist to assess the

[49] Since the audit 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 audit.

data received. This reliability check of the data is only representative of the information in these spreadsheets, not all systems on the VAEC.

Government Standards

The OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that the OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on audit objectives. The OIG believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

Appendix C: Statistical Sampling Methodology

Approach

To accomplish the objective, the audit team reviewed 13 systems: six infrastructure and a sample of seven hosted systems. The team used sampling to quantify the extent of controls and monitoring compliance with National Institute of Standards and Technology (NIST) 800-53 and VA Handbook 6500 requirements. The team developed a checklist and obtained documentation via the Enterprise Mission Assurance Support Service (eMASS) and interviews.

Population

The team audited two populations as of August 17, 2022. The first population consisted of all six Veterans Affairs Enterprise Cloud (VAEC) systems controlled by the Enterprise Cloud Solutions Office (ECSO) that comprise the VAEC infrastructure as a service. The second population was a subset of the 214 systems hosted on the VAEC. From these 214 systems, the team excluded 66 systems that fell into one of the following categories: hybrid systems, where an authority to operate (ATO) was not issued; systems that were currently being reviewed as a part of a Federal Information Security Modernization Act audit to ensure no duplication of effort; systems that were considered storage of data; and systems that were considered a subpart of a major system. After the exclusions, the second population had 148 hosted systems.

Sampling Design

The audit team reviewed the six infrastructure systems from the first population and a sample of seven hosted systems from the second population. These seven systems were selected from three strata. Six systems were selected via random sampling: three from a VAEC vendor A stratum of 71 systems and three from a VAEC vendor B stratum of 76 systems. The final system, hosted by vendor B, was selected from its own *certainty* stratum. Because this system was judgmentally selected based on audit risk, not probability, this system was not considered representative of other systems in the population for estimation purposes. Table C.1 provides details on the strata.

Table C.1. Stratum Population and Sample Sizes

Stratum	Population systems	Sampled systems	Weight
VAEC Vendor A	71	3	23.7
VAEC Vendor B	76	3	25.3
Certainty (Vendor B)	1	1	1

Source: VA OIG statistician's stratified population. Data used for analysis and projections were obtained from the VAEC system list.

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 estimated the percentage of systems in the population with errors by (1) summing the weights of all systems with errors, and (2) dividing this value by the sum of the sampling weights for all systems. Table C.1 shows the weights associated with systems sampled from the second population.

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 approximately 90 percent of the time. The OIG statistician employed statistical analysis software to calculate 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.

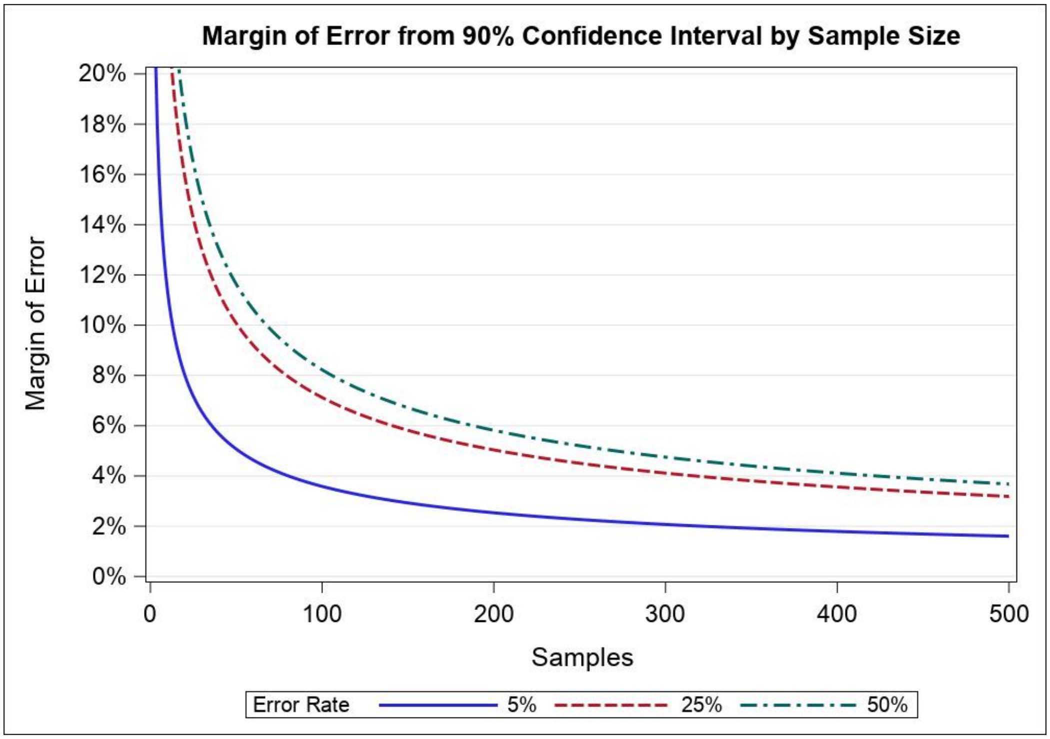


Figure C.1. *Effect of sample size on margin of error.*
Source: VA OIG statistician's analysis.

Projections

Table C.2. shows the projection for the number of the VAEC systems without appropriate controls and monitoring.

Table C.2. Statistical Projections Summary for the VAEC Systems

Estimate name	Estimate number	One-sided lower bound		Sampled systems with errors	Sample size
		Margin of error	Lower		
Appropriate controls not assigned	148 (100%)	47	101	7	7
No continuous monitoring	123 (82.9%)	51	72	6	7

Source: VA OIG analysis of data and information obtained from seven sampled the VAEC systems. These estimates related to the percentage and counts of system errors.

Note: For the hosted systems population, all seven sample units had the errors "appropriate controls not assigned." Therefore, the upper limit is 100 percent."

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: August 21, 2023

From: Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: OIG Draft Report: VA Should Strengthen Enterprise Cloud Security and Privacy Controls, (Project Number 2022-03525-AE-0149) (VIEWS 10638315)

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

1. Thank you for the opportunity to review the Office of Inspector General (OIG) Draft Report, *VA Should Strengthen Enterprise Cloud Security and Privacy Controls*.
2. The Office of Information and Technology (OIT) submits the attached written comments.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachments

Attachment

Office of Information and Technology
Comments on Office of Inspector General Draft Report,
VA Should Strengthen Enterprise Cloud Security and Privacy Controls
Project Number 2022-03525-AE-0149
(VIEWS 10638315)

Recommendation 1: Develop a timeline for updating the security and privacy guidance to reflect the latest revisions to the National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and address identified weaknesses with personally identifiable information and supply chain management.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information Technology (OIT) concurs with the recommendation and has developed a projected timeline for updating security and privacy guidance to reflect the latest revisions to the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*. The approach of OIT's Infrastructure Operations (IO) to the Revision 5 controls transition is to focus on prioritizing the scope of controls to those that contain a significant change (i.e., an impact that caused a process, people, control, technology or policy change beyond language clarification) and control families that have been identified within a Notice of Findings and Recommendation as an area of improvement for VA (such as personally identifiable information and supply chain management).

IO's collaborative approach will entail drafting, tailoring and implementing supply chain related security controls and enhancements. In addition, IO worked to develop "The Privacy Collaboration Index," which VA will use to determine the appropriate level of collaboration between policy and privacy in relation to Revision 5 control updates. IO is targeting December 2023 for its policy adoption deadline for NIST 800-53, Revision 5, which includes addressing the identified weaknesses with personally identifiable information and supply chain management related controls.

Target Completion Date: September 30, 2024.

Recommendation 2: Establish a mechanism to ensure continuous monitoring of VA Enterprise Cloud systems to include having and testing contingency, incident response, disaster recovery, and business continuity plans and conducting scanning as required.[50]

Comments: Concur. VA policies and processes are already in place to address this recommendation. VA Enterprise Cloud (VAEC) and all hosted systems are to follow VA assessment and authorization standard operating procedure (SOP) and continuous monitoring requirements. However, the Office of Information Security (OIS) VA Cloud Security Program Office (VACSPO) will work with stakeholders to develop a validation process to help mitigate non-compliance.

Target Completion Date: September 30, 2024.

Recommendation 3: Ensure VA Directive and Handbook 6517 are updated to reflect the revised National Institute of Standards and Technology requirements.

[50] The draft report inadvertently included business continuity plans in the recommendation; the team did not review these plans.

Comments: Concur. IO will work with OIS subject matter experts for cloud policy, to include VACSPO, to ensure the revisions for Directive 6517, *Risk Management for Cloud Computing Services*, and the associated Handbook, are aligned with NIST 800-53, Revision 5 requirements and Cybersecurity Framework.

Target Completion Date: September 30, 2024.

Recommendation 4: Develop criteria and processes for submitting claims for recoupment of service credits.[51]

Comments: Concur. VA is currently in the process of refining its newly established SOP to minimize the risk of VA not receiving service request recoupments.

Target Completion Date: October 15, 2023.

Recommendation 5: Establish a procedure that includes assigning roles and responsibilities for submitting claims for service credits and monitoring outcomes.

Comments: Concur. IO developed and utilized an SOP for submitting claims for service credits and monitoring outcomes. After meeting with the audit team, IO staff submitted one claim and created a process for submitting a service credit recoupment. As noted above, VA is currently in the process of refining the newly established SOP.

Target Completion Date: October 15, 2023.

[51] In response to VA comments, the team changed “Develop” to “Continue to improve” criteria and processes for submitting claims for recoupment of service credits.

Technical Comments:

Reference Page ii, Para 3, Lines 4-7: Paragraph reads:

> *"Notably, VA has not yet updated its guidance on security and privacy controls following a September 2020 NIST change. Although OIT staff informed the team that they are working on updating the related policy, procedures, and directives, the team found systems were not compliant as of June 2023."*

OIT Recommended Edit: Revise paragraph to read:

> *"Notably, VA has not yet updated its guidance on security and privacy controls, per 800-53, Revision 5, following a September 2020 NIST change. Although OIT staff informed the team that they are working on updating the related policy, procedures, and directives, the team found systems were not compliant with draft 800-53, Revision 5, guidance as of June 2023.*

Reference Page ii, Para 4, Lines 1-7: Paragraph reads:

> *"The audit team made two determinations related to weaknesses in the oversight and monitoring of its VAEC systems. This was due in part to ECSO not effectively overseeing the management of security and privacy controls to make sure the systems and the information they contain are protected commensurate with the risk associated with their misuse or unauthorized disclosure. The OIG examined the six "infrastructure systems" and a sample of seven of the systems hosted on that infrastructure. For those 13 VAEC systems reviewed, the team found sufficient controls for 18 of the 20 security and privacy control families."*

OIT Recommended Edit: Revise paragraph to read:

> *"The audit team made two determinations related to weaknesses in the oversight and monitoring of its VAEC hosted systems. This was due in part to applications systems hosted in the VAEC not effectively overseeing the management of security and privacy controls they are responsible for under the shared responsibility model to make sure the systems and the information they contain are protected commensurate with the risk associated with their misuse or unauthorized disclosure. The OIG examined the six "infrastructure systems" hosted in the VAEC and a sample of seven of the systems hosted on that infrastructure. For those 13 VAEC hosted systems reviewed, the team found sufficient controls for 18 of the 20 security and privacy control families."*

Reference Page iii, Para 2, Lines 4-5: Sentence reads:

> *"Until VA remedies these deficiencies, it will remain at risk of not receiving credit payments to which it is entitled."*

OIT Recommended Edit: Revise sentence to read:

> *"VA is currently in the process of refining its newly established standard operating procedure to minimize risk of VA not receiving service request recoupments."*

Reference Page iii, Para 3, Lines 1-7: Paragraph reads:

> *"The OIG recommended the assistant secretary for information and technology develop a timeline for updating the security and privacy guidance to reflect the revisions to NIST special publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and address identified weaknesses with personally identifiable information and supply chain management. The assistant secretary should also establish a mechanism to ensure continuous*

> *monitoring of the VAEC systems to include having and testing plans (such as contingency, incident, continuity, and disaster plans) and conducting scanning as required."*

OIT Recommended Edit: Revise paragraph to read:

> *"The OIG recommended for systems hosted in the VAEC the assistant secretary for information and technology develop a timeline for updating the security and privacy guidance to reflect the revisions to NIST special publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and address identified weaknesses with personally identifiable information and supply chain management. The assistant secretary should also establish a mechanism to ensure continuous monitoring of the VAEC hosted systems to include having and testing plans (such as contingency, incident, continuity, and disaster plans) and conducting scanning as required."*

Reference Page iii, Para 3, Lines 9-11: Sentence reads:

> *"The OIG further recommended that the assistant secretary develop criteria and processes for submitting claims to recoup service credits and establish a procedure that includes assigning roles and responsibilities for submitting claims and monitoring outcomes."*

OIT Recommended Edit: Revise sentence to read:

> *"The OIG further recommended that the assistant secretary continue to improve criteria and its processes for submitting claims to recoup service credits and establish a procedure that includes assigning roles and responsibilities for submitting claims and monitoring outcomes."*

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.
Audit Team	Al Tate, Director Carolyn Burnett Cynthia Christian Omar Madrigal Keila Tugwell-Core
Other Contributors	Kathy Berrada Kendal Ferguson 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 Accountability
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.