DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Veterans Data Integration and Federation Enterprise Platform Lacks Sufficient Security Controls

AUDIT

REPORT #21-01123-97

JUNE 1, 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

Exchanging health information across electronic platforms is essential to improving care for our nation's veterans and enables VA and community providers to develop comprehensive care plans, improve continuity of care, reduce duplicative tests, and avoid clinical errors when patients see different providers. Since the electronic platforms involved with the data exchanges contain veterans' sensitive personal information, they must have required security controls to protect that information from unauthorized access and disclosure.[1]

The Veterans Data Integration and Federation Enterprise Platform (VDIF) allows VA to share sensitive health information, such as medical chart notes and laboratory results, with the Department of Defense and participating community care providers through the Joint Health Information Exchanges (JHIE) and the eHealth Exchange.[2] By law, VA is required to ensure the safe sharing of veterans' sensitive personal information.[3] Linking information across an extremely diverse and highly fragmented healthcare system can create technical challenges and increase vulnerabilities. Therefore, establishing the appropriate security categorization (as described below) for VDIF is necessary to protect veterans' sensitive personal information.

All electronic systems used by the federal government must be assigned a security categorization level that determines which controls are applied based on the risk of data breaches and privacy violations that could lead to more serious threats such as identity theft (see appendix A for further information about the low, medium, and high risk categories). If the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals, then the system must be categorized as "high" with appropriate controls implemented.[4] The VA Office of Inspector General (OIG) audited whether the Office of Information and Technology (OIT) developed and implemented security controls for VDIF that are sufficient to ensure confidentiality, data integrity, and the safeguarding of veterans' sensitive health information on the JHIE and the

[1] Sensitive personal information includes individually identifiable information, individually identifiable health information, protected health information, and privacy-protected information.

[2] JHIE allows VA, the Department of Defense, and private sector systems to exchange and share veterans' health information with community providers. The eHealth Exchange is a data-sharing network of governmental and nongovernmental exchange partners who share information under a multipurpose set of standards and services designed to support a broad range of information exchange activities using various technical platforms and solutions. The eHealth Exchange is also the largest nationwide health data sharing network of federal and nonfederal healthcare partners securely sharing information via the internet, connecting more than 75 percent of all hospitals in the country, 70,000 medical groups, 8,300 pharmacies, and over 120 million patients.

[3] The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, (1996); 45 C.F.R. § 164.306(a); Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[4] NIST, "Standards for Security Categorization of Federal Information and Information Systems," *Federal Information Processing Standards Publications (FIPS PUBS) 199*, Department of Commerce, February 2004.

eHealth Exchange in accordance with federal standards. See appendixes B and C for details about the scope and methodology of the audit.

What the Audit Found

The OIG found OIT allowed VDIF to become operational without effectively executing all the risk management framework steps developed by the National Institute of Standards and Technology (NIST).[5] The framework includes six steps that address the security concerns of organizations related to the design, development, implementation, operation, and disposal of information systems and the environments in which those systems operate. Although OIT followed the steps, it inappropriately categorized two of VDIF's security objectives in the Enterprise Mission Assurance Support Service (eMASS)—a web-based application that automates setting security controls for VA systems. The confidentiality and availability security objectives were set at a moderate categorization risk level, even though they were approved at a high level, according to eMASS. This resulted in 22 important security controls not being applied, risking the personal health information of more than 10 million veteran records. Furthermore, OIT did not adequately determine whether the controls that were implemented were done correctly and produced the desired security outcome.

Due to ineffective oversight, OIT did not properly follow NIST and VA policy requirements for setting VDIF's security controls at a high level. According to OIT's product manager and system steward for VDIF, OIT personnel did not adequately oversee the controls on VDIF and failed to follow proper program management processes or protocols in reviewing and monitoring them.[6] The product manager further indicated this was due to the loss of key individuals responsible for reviewing the security controls. In addition, VDIF's information system security officer stated he was not part of the project planning process for the system but approved the privacy threshold analysis and privacy impact assessment that indicated VDIF's security categorization should be set at a high level.[7] As a result, VDIF became operational with security controls that did not ensure confidentiality, data integrity, and the safeguarding of veterans' sensitive health information on the JHIE and the eHealth Exchange.

Since VDIF allows VA and participating community care partners to share health information with the JHIE and eHealth Exchange, the lower system security setting and fewer controls increased the risk of data breaches and unauthorized modification, use, or destruction of

[5] NIST, "Standards for Security Categorization of Federal Information and Information Systems;" Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," *NIST Special Publication 800-53, rev. 4*, National Institute of Standards and Technology, April 2013, includes updates as of January 22, 2015.

[6] System stewards and information system owner are officials with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing the organization's generation, collection, processing, dissemination, and disposal.

[7] The privacy impact assessment identifies the level of security risk associated with a program or technology.

veterans' sensitive personal information. The Veterans Health Administration's program manager for Enterprise Program Management Office Information Assurance, who is the information system owner for VDIF, stated many VA systems that contain protected health information and personally identifiable information default to the highest security level. Nevertheless, the system owner justified VDIF's moderate risk level categorization for the confidentiality and availability security objectives, stating these categorizations do not affect the health of the patient and do not directly harm veterans.

The OIG disagrees with the system owner's statement based on federal guidance, VA's privacy impact assessment, and medical research. According to NIST guidance, security categories are based on the potential impact if critical information and systems are jeopardized. Security categorization for information types is based on the security objectives—confidentiality, integrity, and availability—within the system. 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.[8] Here, the impact of a data breach would have a high impact on individuals.

VDIF's privacy impact assessment shows that VDIF transmits visual displays of personally identifiable information and personal health information. Per the privacy impact assessment, if this information was breached or accidentally released inappropriately it could result in financial, personal, or emotional harm to the individuals whose information is contained in the system. The assessment also indicated that data breaches would have an irreparable impact on major applications or general system functions, image, or reputation, such that the catastrophic result would not be able to be repaired or could result in loss of major tangible assets or resources, including posing a threat to human life. On May 20, 2021, VA updated the privacy impact assessment but did not change the risk level of VDIF to moderate.

Moreover, there is evidence of direct individual harm from a data breach of sensitive personal information such as that stored in VDIF, which would justify categorizing the system risk as high. The authors of a medical research review state that "patients whose private health information becomes available can suffer embarrassment, paranoia, or mental pain. Even though these injuries may not have measurable external effects—the patients may suffer no financial injury or encounter no stigma from others—they are still injuries."[9] Another study concluded that "the stress associated with interpersonally invasive crimes can be destabilizing in many ways;

[8] NIST, FIPS Pub 199.

[9] W. Nicholson Price II and I. Glenn Cohen, "Privacy in the age of medical big data," January 7, 2019, https://www.nature.com/articles/s41591-018-0272-7.

this may be especially true for those with mental illnesses."[10] If veterans do not have confidence that VA will protect their information, they may not seek needed treatment.

What the OIG Recommended

The OIG recommended the assistant secretary for OIT and chief information officer ensure VDIF's security objectives are all categorized at a high risk level based on the sensitive personal information maintained in the system and the approved risk assessment. In addition, the OIG recommended taking steps to reestablish VDIF in eMASS to ensure appropriate security controls are implemented and assessed at the high risk level. The OIG also recommended the assistant secretary ensure OIT provides appropriate oversight and follows proper program management processes and protocols when establishing and monitoring security controls for IT systems.

VA Comments and OIG Response

The assistant secretary for OIT and chief information officer did not concur with recommendation 1 to categorize VDIF at a high risk level. The assistant secretary said that while VA shares the OIG's concern with protecting sensitive information, assigning the system categorization level is the responsibility of the chief information officer and the authorizing official. He said VA properly categorized the system as moderate. While OIT's case manager, information system owner, information system security officer, and system steward all reviewed and approved VDIF's risk security categorization as high, the assistant secretary did not explain why he said the system was appropriately categorized as moderate.

The assistant secretary also did not concur with recommendation 2 to reestablish VDIF in eMASS at the high risk level. He stated VA has implemented additional security controls through a privacy overlay within eMASS. While the overlay added 71 additional controls in eMASS at the moderate level, it still did not address the controls needed at the high level.[11] Although the assistant secretary requested the OIG close recommendations 1 and 2, the OIG maintains the system should be set at the high risk level to protect veterans' sensitive information. The OIG encourages VA to reconsider to more fully mitigate the potential risk of data breaches and privacy violations.

Based on the finding that some of the moderate security controls for VDIF were not assessed properly, the OIG made a third recommendation—that OIT provide appropriate oversight and

[10] Jonathon Klopp, LCPC, Shane Konrad, MD, Jason Yanofski, MD, and Anita Everett, MD, "Identity Theft in Community Mental Health Patients," May 2007, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2921312/.

[11] NIST Special Publication 800-53, rev 4. An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The baseline is a set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.

follow proper program management processes and protocols when establishing and monitoring security controls for IT systems. The assistant secretary concurred with this recommendation, which the OIG will close when it receives sufficient evidence showing progress in addressing the intent of the recommendation and taking corrective actions. 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

eMASS	Enterprise Mission Assurance Support Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IT	information technology
JHIE	Joint Health Information Exchanges
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
VDIF	Veterans Data Integration and Federation Enterprise Platform

Introduction

The ability to exchange health data across electronic platforms is essential to improving care for our nation's veterans. The electronic exchange of healthcare information lets VA and community providers develop comprehensive care plans, improve continuity of care, reduce duplicative tests, and avoid clinical errors when patients see different providers. Data exchanges involving veterans' sensitive personal information must have appropriate security controls in place to adequately protect that information from unauthorized use or disclosure.[12] All electronic systems have security levels that are applied based on the risk of harm that could result in the event of a data breach or privacy violation.

The VA Office of Inspector General (OIG) audited whether the Office of Information and Technology (OIT) developed and implemented sufficient security controls for the Veterans Data Integration and Federation Enterprise Platform (VDIF)—VA's primary data-sharing platform with non-VA providers—to ensure confidentiality, data integrity, and safeguarding of veterans' sensitive health information on the Joint Health Information Exchanges (JHIE) and the eHealth Exchange.[13]

Veterans Data Integration and Federation Enterprise Platform

VA uses VDIF to share health information, such as clinical notes and laboratory reports, with the Department of Defense and participating community care providers through the JHIE and the eHealth Exchange. VDIF replaced VA's legacy system, the Veterans Health Information Exchange, in April 2020 because VDIF is cloud-based, which allows it to integrate with VA's new electronic health record system on the JHIE.

Risk Management

VA is required by law to ensure the safe sharing of sensitive personal information.[14] Sharing information across systems in an extremely diverse and highly fragmented healthcare universe

[12] Sensitive personal information includes individually identifiable information, individually identifiable health information, protected health information, and privacy-protected information.

[13] The Joint Health Information Exchanges allows VA, the Department of Defense, and private sector systems to exchange and share veterans' health information with community providers. The eHealth Exchange is a data sharing network of governmental and nongovernmental exchange partners who share information under a multipurpose set of standards and services, which are designed to support a broad range of information exchange activities using various technical platforms and solutions. The eHealth Exchange is also the largest nationwide health data sharing network of federal and nonfederal healthcare partners securely sharing information via the internet, connecting more than 75 percent of all hospitals in the country, 70,000 medical groups, 8,300 pharmacies, and over 120 million patients.

[14] The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, (1996); 45 C.F.R. § 164.306(a); Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

can create technical challenges and vulnerabilities.[15] Therefore, establishing the appropriate security controls for VDIF is critical to reduce the risks of unauthorized use or disclosure of veterans' sensitive personal information.

VA is required to comply with the Federal Information Security Management Act (FISMA), which mandates that federal agencies secure information and systems that support their operations and assets. FISMA tasked the National Institute of Standards and Technology (NIST) to develop standards and guidelines for information security for federal agencies.[16] These standards and guidelines are known as Federal Information Processing Standards (FIPS). These standards, along with other publications, lay out the framework for managing risk through the design, development, implementation, operation, and disposal of information systems and the environments in which those systems operate.[17]

The framework consists of six steps:

1. Categorize the information system based on an impact assessment.[18]
2. Select the applicable security control baseline based on the security categorization and apply tailoring guidance.
3. Implement the security controls and document the design, development, and implementation details for the controls.
4. Assess the security controls to determine if the controls are implemented correctly, operating as intended, and producing the desired level of security.
5. Authorize information system operation based on a determination of whether the risk resulting from the operation and use of the information system is acceptable.
6. Monitor the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness and compliance with legislation, executive orders, directives, policies, regulations, and standards.

Figure 1 shows the risk management framework.

[15] "Health Information Exchange Policy Issues," Digital Healthcare Research Archive, accessed January 19, 2022, https://digital.ahrq.gov/key-topics/health-information-exchange-policy-issues.

[16] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[17] NIST, "Standards for Security Categorization of Federal Information and Information Systems;" Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," *NIST Special Publication 800-53, rev. 4*, National Institute of Standards and Technology, April 2013, includes updates as of January 22, 2015.

[18] The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. See appendix A for further information about the low-, medium-, and high-risk categories.

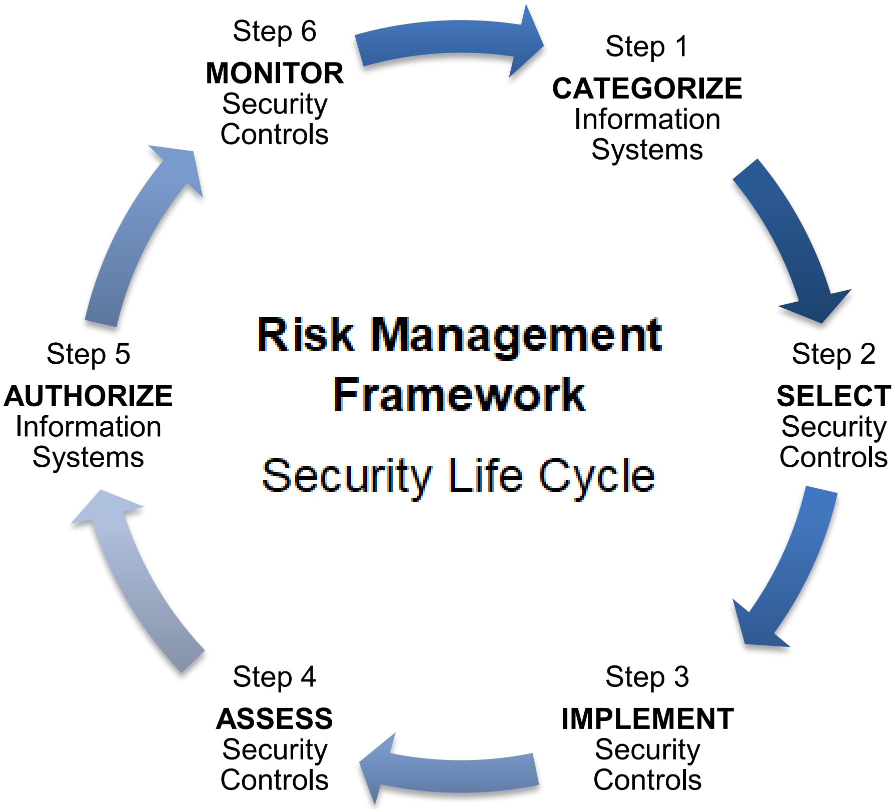

Figure 1. *Overview of NIST's risk management framework security life cycle.*
Source: OIG's interpretation of NIST Special Publication 800-53 Revision 4 Security Life Cycle.

Categorizing the security level for VDIF was part of the first step in the NIST risk management framework. The process begins with a privacy threshold analysis, which VA uses to analyze the information in the system and determine the security level.[19] The privacy threshold analysis identifies whether an information technology (IT) system includes sensitive personal information that affects the privacy of individuals and whether a privacy impact assessment is needed. The privacy impact assessment identifies and mitigates privacy risks within an information system. It should address risk at every stage of the system development life cycle and is required before developing or procuring IT that collects, maintains, or disseminates information in an identifiable form. It also demonstrates that the system owner has incorporated privacy protections throughout the development life cycle of an IT system. The privacy impact assessment identifies the level of security risk associated with a program or technology. NIST Special Publication 800-53 and VA Handbook 6500 establish the applicable security controls based on the risk level of the data in an

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

information system.[20] Appendix A contains detailed information on security standards and guidelines, including the low, medium, and high categories.

Enterprise Mission Assurance Support Service

The Enterprise Mission Assurance Support Service (eMASS) is a web-based application that automates the process of setting security controls for VA systems throughout the risk management framework. This includes dashboard reporting, workflow automation, and continuous monitoring that replicates the risk management framework. The capabilities of eMASS include context to understand mission impact by establishing process control mechanisms for obtaining authorization to operate decisions.[21] eMASS automatically populates the confidentiality, integrity, and availability for some information type based on the risk assessment results.

Previous VA OIG Reports

The OIG has issued two audit reports addressing the risk categorization of electronic systems since September 2019:

- In the *Audit of Program of Comprehensive Assistance for Family Caregivers: IT System Development Challenges Affect Expansion*, the OIG found VA did not establish the appropriate security risk category or fully assess the system's privacy vulnerabilities.[22] Specifically, OIT did not adequately consider the protected health information as part of its Caregiver Record Management Application risk assessment determination. The Veterans Health Administration, the information owner and steward, did not participate in assessing the security risk categorization of the Caregiver Record Management Application as required by NIST. The OIG recommended to the acting assistant secretary for information and technology, in conjunction with the acting under secretary for health, that VA reevaluate elevating the system's risk category to better protect health information and other sensitive data and establish agency-wide policies and responsibilities for managing IT projects.

[20] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," VA Handbook 6500, *Risk Management Framework for VA Information Systems—Tier 3: VA Information Security Program*, March 2015.

[21] Joint Task Force Transformation Initiative, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," *NIST Special Publication 800-37*, rev. 2, December 2018. Authority to operate is a formal declaration by a designated approving authority that authorizes operation of a business product and explicitly accepts the risk to the agency. The authority to operate is signed after a certification agent confirms that the system has passed all requirements to become operational.

[22] VA OIG, *Audit of Program of Comprehensive Assistance for Family Caregivers: IT System Development Challenges Affect Expansion,* Report No. 20-00178-24, June 8, 2021.

- In the *Audit of Security and Access Controls for the Beneficiary Fiduciary Field System Need Improvement*, the OIG found OIT inappropriately set the security risk level for the Beneficiary Fiduciary Field System at moderate instead of high because risk managers did not follow established standards and did not consider whether information for beneficiaries and fiduciaries stored in the system's database was sufficiently protected.[23] The OIG made four recommendations to the assistant secretary for information and technology, in conjunction with the under secretary for benefits, to include reevaluating the risk determination for the Beneficiary Fiduciary Field System, improving controls over end-user access levels, fully enabling audit logs to accurately and comprehensively track access to system records, and improving separation of duties issues.

[23] VA OIG, *Audit of Security and Access Controls for the Beneficiary Fiduciary Field System Need Improvement,* Report No. 18-05258-193, September 12, 2019.

Results and Recommendations

Finding: OIT Did Not Ensure VDIF Had the Appropriate Security Controls

The OIG found OIT's security objectives for VDIF were not set at the appropriate high risk level based on the approved categorization in eMASS. Instead, VDIF was set at a moderate risk level in eMASS, an outcome that OIT's product manager and system steward for VDIF attributed to human error.[24] Although OIT correctly categorized the integrity security objective as high risk, it categorized the confidentiality and availability objectives as moderate risk, resulting in 22 important security controls—such as real-time alerts for responding to system audit processing failures and backing up physical systems and components to protect information—not being applied. The lower setting potentially jeopardized the confidentiality, integrity, and availability of over 10 million records containing veterans' sensitive personal information.

OIT's product manager and system steward for VDIF also indicated OIT personnel did not adequately oversee the controls on VDIF and failed to follow proper program management processes or protocols in reviewing and monitoring them. The product manager confirmed this was due to the loss of key individuals responsible for reviewing the security controls.

Three elements contributed to this finding:

- Veterans' sensitive personal information is not secure and is potentially at risk.
- OIT inaccurately set VDIF's security level and did not adequately assess VDIF security controls.
- OIT did not effectively oversee the management of the security controls for VDIF.

What the OIG Did

The audit team reviewed VDIF's security privacy threshold analysis and privacy impact assessment to evaluate whether the system had adequate security controls and oversight when it was set up in eMASS. The team also reviewed VDIF's authority to operate to determine if OIT's decision to host VDIF on Amazon Web Services met all applicable security requirements. The team interviewed the VDIF product manager and system steward, the information system owner, contractor personnel responsible for maintaining VDIF, a Veterans Health Administration privacy specialist, information system security officers, and a cybersecurity analyst. The team

[24] System stewards and information system owner are officials with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing the organization's generation, collection, processing, dissemination, and disposal.

completed a review of sampled security, privacy, and program management controls. Further discussion of the scope and methodology of this audit can be found in appendixes B and C.

Veterans' Sensitive Personal Information is Not Secure and at Risk of Misuse

VDIF contains more than 10 million veteran records with sensitive personal information that can be shared with community care partners through the JHIE and eHealth Exchange. Improper management of security settings for the system puts that information at risk in the following ways:

- Intentional or unintentional acts may lead to a data breach, unauthorized modification, or destruction of veterans' health information.[25]
- The design and structure of VDIF tools do not ensure data quality and reliability.[26]
- Unavailable or unreliable information could cause inefficiencies in accessing and retrieving critical healthcare information on demand, which could affect care decisions and, ultimately, veterans' health.[27]

According to VDIF's privacy impact assessment, VDIF disseminates a visual display of personally identifiable information and other highly delicate personal health information. The assessment also stated if this information was breached or accidentally released inappropriately, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system. Furthermore, the assessment indicated that a breach would have an irreparable effect on major applications or general system functions, image, or reputation, such that the catastrophic result would not be able to be repaired or set right again. A breach could also result in loss of major tangible assets or resources, including posing a threat to human life. On May 20, 2021, VA updated the privacy impact assessment but did not change the risk level of VDIF to moderate.

While a security breach may not pose a direct threat to a veteran's life, it could cause emotional distress. Medical researchers have found that "patients whose private health information

[25] Jingcong Zhao, "Conducting an Information Security Risk Assessment," November 22, 2019, https://hyperproof.io/resource/information-security-risk-assessment-a-primer.

[26] Valerie A. Yeager et al., "Challenges to Conducting Health Information Exchange Research and Evaluation: Reflections and Recommendations for Examining the Value of Health Information Exchange," September 4, 2017, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5983050.

[27] eHealth Connecticut, "Benefits and Risks of Health Information Exchange," accessed October 6, 2020, http://ehealthconnecticut.org/LinkClick.aspx?fileticket=RaMv530zwic%3D&tabid=79. (As of January 25, 2022, this link is no longer valid). Shailendra Sinhasane, "7 Benefits of Health Information Exchange With Potential Challenges," March 20, 2019, https://mobisoftinfotech.com/resources/blog/health-information-exchange-benefits-and-challenges/.

becomes available can suffer embarrassment, paranoia, or mental pain. Even though these injuries may not have measurable external effects—the patients may suffer no financial injury or encounter no stigma from others—they are still injuries."[28] Researchers also indicated that "the stress associated with interpersonally invasive crimes can be destabilizing in many ways; this may be especially true for those with mental illnesses."[29] Furthermore, according to researchers, "without privacy and security assurances, patients will withhold information from their providers to avoid having it used inappropriately."[30] Millions of veterans trust VA to keep their information secure. This includes sensitive diagnoses and treatment information. If veterans are unable to rely on VA to protect their information, they may not seek needed treatment.

OIT Inaccurately Set VDIF's Security Level and Did Not Adequately Assess the Controls

Veterans Health Administration's privacy officer, OIT's information system security officer, and the VDIF information system owner conducted the required privacy impact assessment of the system. On June 13, 2019, they approved the privacy impact assessment, which appropriately defined VDIF as a high-risk system. However, OIT did not comply with the results of the assessment when it instead set the categorizations for the confidentiality and availability security objectives at a moderate risk level.

The Veterans Health Administration's program manager for Enterprise Program Management Office Information Assurance, who is the information system owner for VDIF, stated many VA systems that contain protected health information and personally identifiable information default to the highest security level. The system owner also indicated that the operations team, the program management team, and the Veterans Health Administration concurred with the decision to keep VDIF at a moderate risk level. The system owner further stated that where the security categorization does not affect the health of the patient and there is no threat of direct harm to a veteran, the system should be reduced to moderate. Based on federal guidance, VA's privacy impact assessment, and medical research, the OIG disagrees with this assertion.

NIST guidance states security categories are based on the potential organizational impact if certain events occur that jeopardize necessary information and systems. The security categorization for information type is based on the security objectives—confidentiality, integrity, and availability—within the system. A breach of any security objective could have a low

[28] W. Nicholson Price II and I. Glenn Cohen, "Privacy in the age of medical big data," January 7, 2019, https://www.nature.com/articles/s41591-018-0272-7.

[29] Jonathon Klopp, LCPC, Shane Konrad, MD, Jason Yanofski, MD, and Anita Everett, MD, "Identity Theft in Community Mental Health Patients," May 2007, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2921312/.

[30] Deven McGraw, James X. Dempsey, Leslie Harris, and Janlori Goldman, "Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange," March/April 2009, https://www.healthaffairs.org/doi/10.1377/hlthaff.28.2.416.

(limited), moderate (serious), or high (severe or catastrophic) adverse effect on organizational operations, assets, or individuals.[31] OIT contradicted the privacy impact assessment when it established VDIF in eMASS with a moderate risk level.

Based on the risk assessment rating results, a system steward selects the risk levels in eMASS for the confidentiality, integrity, and availability for each information type.[32] eMASS then automatically populates a list of security controls. For VDIF, despite the privacy impact assessment indicating a high level should be assigned, a system steward selected a moderate risk level categorization for the confidentiality and availability security objectives. As a result, eMASS did not populate all the required controls for a high-risk system for VDIF.

The audit team identified 22 security controls required for high-risk systems that OIT did not implement because all the security objectives were not set at the corresponding risk level. For example, OIT did not implement the control enhancement that requires an organization to use a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. Furthermore, OIT did not implement the control enhancement that requires backing up internal audit records onto a physically different system or system component than the one being audited. This control enhancement helps to ensure that if the information system being audited is compromised, the audit records are not compromised as well.[33] Appendix A contains additional examples of high categorization controls not implemented. Even some of the moderate security controls for VDIF were not assessed properly. According to VA Handbook 6500, OIT is required to assess the security controls and ensure assessors have access to the information system and environment of operation where the security controls are employed.

The audit team reviewed a sample of controls and estimates that 70 percent were noncompliant. Errors included outdated policies, lack of evidence that the security control was implemented, and no evidence that it was tested. For example, the audit team found policies that OIT relies on for managing IT security were not updated since 2010, although VA Directive 0999 requires updates to existing policies every five years.[34] It is important to update policies and procedures so security controls address modern cybersecurity vulnerabilities. The team also found other control evaluations lacked documentation to support the control was tested and functioning properly or found the supporting documentation did not relate to the specific control. VA

[31] NIST, FIPS Pub 199.

[32] According to FIPS Publication 199, security categories are based on the potential organizational impact if certain events occur that jeopardize necessary information and systems. The security categorization for information type is based on the security objectives—confidentiality, integrity, and availability—within the system. The potential impact of each security objective could have a low (limited), moderate (serious), or high (severe or catastrophic) adverse effect on organizational operations, assets, or individuals.

[33] NIST Special Publication 800-53, rev 4.

[34] VA Handbook 0999, *Enterprise Directives Management Procedures*, August 1, 2019.

Handbook 6500 requires documentation, such as test results, to support that the controls are in place and functioning to protect sensitive protected health information and personally identifiable information.

The OIG found that OIT had created plans of action for controls it identified as noncompliant. A plan of action and milestones is a document that identifies tasks needing to be accomplished for noncompliant control evaluations. The plan of action and milestones details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. However, many of the tasks were not addressed and were past their completion dates. Addressing them is important because they represent identified security or privacy risks that must be managed.

VDIF's IT product manager said the lack of documentation of control evaluations was the result of turnover. He said VDIF started with two experienced contractors; however, they were replaced with two new contractors. One contractor is dedicated to VDIF, while the other has additional non-VDIF responsibilities. The dedicated contractor confirmed he had to review about 1,700 assessment procedures. This included reviewing control descriptions and supplemental guidance to understand the requirements and obtaining sufficient supporting documentation to determine whether the control was compliant.

OIT Did Not Effectively Oversee the Management of the Security Controls for VDIF

The OIG determined OIT did not effectively oversee its risk management framework process. OIT is required by law and VA policy to ensure the security level for VDIF was sufficient to ensure confidentiality, data integrity, and safeguarding of veterans' sensitive health information on the JHIE and the eHealth Exchange. OIT could not provide documentation showing why it contradicted the privacy impact assessment and how VDIF was established in eMASS with a moderate risk level for the confidentiality and availability security objectives. The IT product manager, a system steward of VDIF, said he had no knowledge of who completed the risk assessment. While the manager should have been aware, he indicated that if an assessment was completed and it was inaccurate, it was his responsibility to make the necessary corrections. In addition, VDIF's information system security officer stated he was not part of the project planning process, noting that the decision to place VDIF on Amazon Web Services moderate was before his time and that "the OIG should investigate it because it seems weird." However, he approved the privacy threshold analysis and privacy impact assessment, which indicated VDIF's security categorization should be set at a high level.[35]

During the OIG's audit, VDIF's product manager indicated that the privacy impact assessment was completed in the *DevSecOps Information Assurance System Security Categorization Report* on April 19, 2021. This resulted in OIT reestablishing the confidentiality security objective at a high risk level; however, it has not updated the categorization of the availability objective. The product manager also said the confidentiality rating set during VDIF's categorization meeting was based on guidance from NIST 800-60. Since VDIF contains more than 10 million veteran records with sensitive personal information, OIG found the high risk level most appropriate.[36] As mentioned previously, OIT officials had initially agreed that the system should be set at high. Additionally, OIT's information system owner acknowledged that VDIF's integrity and impact categories were assessed as high. According to FIPS 199, if loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals, then the system must be categorized as high with appropriate controls implemented. While OIT had already conducted the required privacy threshold analysis and privacy impact assessment, they were not used to appropriately categorize the security level for VDIF before the system was hosted on Amazon Web Services.

Conclusion

Given the sensitivity of veteran information transmitted by VDIF, the information is vulnerable to increased risks if there are insufficient security controls. A compromise of security controls could potentially jeopardize the confidentiality, integrity, and availability of protected health information, personally identifiable information, and other sensitive information. Since the risk of a compromise poses significant threats to the health and safety of veterans, as well as their confidence in the integrity of VA healthcare, OIG disagrees with setting a moderate risk level for VDIF and believes it should have been set at high. OIT also should provide appropriate oversight of VDIF security controls.

[35] The information system security officer's role includes assisting in the determination of the appropriate security categorization of an IT system commensurate with the FIPS 200 impact level. NIST, "Minimum Security Requirements for Federal Information and Information Systems," *Federal Information Processing Standards Publications (FIPS PUBS) 200*, Department of Commerce, March 2006.

[36] NIST, "Guide for Mapping Types of Information and Information Systems to Security Categories," *NIST Special Publication 800-60,* August 2008.

Recommendations 1–3

The OIG recommended the assistant secretary for information and technology and chief information officer:

1. Ensure the Veterans Data Integration and Federation Enterprise Platform security objectives are all set at a categorization level of high based upon both the sensitive personal information maintained in the system and the approved risk assessment.
2. Act to reestablish the Veterans Data Integration and Federation Enterprise Platform in the Enterprise Mission Assurance Support Service to ensure appropriate security controls are implemented and the system is assessed at the high risk level.
3. Ensure the Office of Information Technology provides appropriate oversight and follows proper program management processes and protocols when establishing and monitoring security controls for IT systems.

Management Comments

The assistant secretary for OIT and chief information officer did not concur with recommendation 1 to categorize VDIF at a high risk level. The assistant secretary said that while VA shares the OIG's concern with protecting sensitive information, assigning the system categorization level is the responsibility of the chief information officer and authorizing official. He also said VA properly categorized the system as moderate and implemented additional security controls through the privacy overlay within eMASS.

Further, the assistant secretary did not concur with recommendation 2 to reestablish VDIF in eMASS to ensure appropriate security controls are implemented and the system is assessed at the high risk level. The assistant secretary said VA properly categorized the confidentiality, integrity, and availability of VDIF. According to the assistant secretary, using the Committee on National Security Systems Instruction 1253 baseline, and the eMASS privacy overlay, VDIF added an additional 71 controls to the moderate control baseline.[37]

The assistant secretary concurred with recommendation 3 and provided an acceptable action plan. The assistant secretary stated OIT will ensure the personally identifiable information confidentiality impact evaluation process is implemented and communicated to information system owners; the process identifies required controls to be added to systems' baselines.

[37] Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2017; NIST Special Publication 800-53, rev 4. An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The baseline is a set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.

Appendix D includes the full text of the assistant secretary's comments.

OIG Response

Although the assistant secretary for OIT and chief information officer requested the OIG close recommendations 1 and 2, the OIG maintains the system should be set at the high risk level to protect veterans' sensitive information. The OIG acknowledges that the assistant secretary has the authority to assign a system categorization level for VDIF. However, VA clearly recognized the need for additional protection mechanisms and security controls for VDIF, as it applied a privacy overlay in eMASS. While the overlay added 71 additional controls in eMASS at the moderate level, it still did not address the controls needed at the high level. Further, while OIT's case manager, information system owner, information system security officer, and system steward all reviewed and approved VDIF's risk security categorization as high, the assistant secretary did not explain why he said the system was appropriately categorized as moderate. The OIG encourages VA to reconsider to more fully mitigate the potential risk of data breaches and privacy violations.

The OIG will close recommendation 3 when it receives sufficient evidence showing progress in addressing the intent of the recommendation and corrective actions.

Appendix A: Background

Information Security Standards and Guidelines

VA is required to follow federal information security standards, including FISMA.[38] The law recognized the importance of information security to the economic and national security interests of the United States. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA defines three security objectives for information and information systems:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, which includes ensuring confirmation of information transfer and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

FISMA tasked NIST to develop standards and guidelines for information security for all federal agencies. FIPS Publication 199 addresses the FISMA requirements to establish security categories for both information and information systems.[39] The security categories are based on the potential impact on an organization and individuals should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

FIPS Publication 199 defines three levels of potential impact on organizations or individuals from a security breach.

- **Low impact:** The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- **Moderate impact:** The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

[38] E-Government Act of 2002, Title III—Federal Information Security Management Act of 2002, Pub. L. No. 107-347, §§ 301-305 (2002).

[39] NIST, FIPS Pub 199.

- **High impact:** The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

FIPS Publication 200 Security-Related Areas

FIPS Publication 200 specifies minimum security requirements for information and information systems for executive agencies and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.[40] The minimum security requirements cover 17 security-related areas regarding protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. The following are descriptions of some of the security-related areas.

- **Access control**—limit access to authorized users and to the types of transactions and functions that authorized users are permitted to exercise.
- **Audit and accountability**—create, protect, and retain audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity and ensure that the actions of individual information system users can be uniquely traced.
- **Certification, accreditation, and security assessments**—periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; authorize the operation of organizational information systems and any associated information system connections; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- **Identification and authentication**—identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- **Incident response**—establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate organizational officials and/or authorities.
- **Risk assessment**—periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting

[40] NIST, FIPS Pub 200.

from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

- **System and Information integrity**—identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response.

High Categorization Controls

OIT inaccurately established VDIF's risk security categorization level as moderate instead of high resulting in 22 security controls not being implemented. The following are examples of control enhancements that were not implemented.[41]

- **Response to Audit Processing Failures/Audit Storage Capacity**—requires the information system provide a warning when allocated audit record storage volume reaches an organization-defined percentage of repository maximum audit record storage capacity. NIST Supplemental Guidance states organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.
- **Response to Audit Processing Failures/Real-Time Alerts**—requires the information system provide real-time alert when audit failure events occur. NIST Supplemental Guidance states alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).
- **Contingency Plan/Capacity Planning**—requires the organization conduct capacity planning so that sufficient information processing, telecommunications, and environmental support exist during contingency operations. NIST Supplemental Guidance states capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyberattacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.
- **Contingency Training/Simulated Events**—requires the organization incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

[41] NIST Special Publication 800-53, rev 4.

- **Information System Backup/Separate Storage for Critical Information**—requires the organization store backup copies of critical information system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system. Supplemental Guidance states critical information system software includes operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.
- **Cryptographic Key Establishment and Management/Availability**—requires the organization maintain availability of information in the event of the loss of cryptographic keys by users. NIST Supplemental Guidance states escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

Appendix B: Scope and Methodology

Scope

The OIG performed its audit work from March 2021 through January 2022 to evaluate if OIT developed and implemented effective security controls to ensure confidentiality, data integrity, and safeguarding of veterans' protected health information on the JHIE and the eHealth Exchange for VDIF.

Methodology

The audit team interviewed the VDIF product manager, information system security officers, system owner, and contractor personnel responsible for maintaining VDIF. The team also examined the security risk analysis and the authority to operate VDIF and reviewed the security privacy threshold analysis and impact assessment for VDIF to determine if OIT identified and mitigated the risks associated with the system. The team reviewed a random sample of 30 security controls and a combination of 62 judgmentally selected security, privacy, and program management controls from a total of 389. The controls that were judgmentally selected were identified as significant due to their importance for the entire control family.

To determine whether the selected control was compliant, the team reviewed artifacts that were uploaded to eMASS, the repository for all documents used to support security and privacy control compliance, and compared those documents to NIST 800-53 and VA 6500 requirements. By June 23, 2021, 67 percent of the statistically sampled and 79 percent of the judgmentally selected security and privacy controls were noncompliant due to missing documentation, incomplete support, or out of date policies and procedures. The audit team discussed the types of security and privacy control issues identified to date with OIT during a meeting on June 25, 2021.

Internal Controls

The OIG determined that internal controls were significant to the audit objective. The OIG assessed the internal controls of OIT relevant to the audit objective. This included an assessment of the five internal control components including control environment, risk assessment, control activities, information and communication, and monitoring. In addition, the team reviewed the principles of internal controls associated with the audit objective. The OIG identified five components and their associated principles as significant to the audit objective, identified internal control weaknesses and proposed recommendations specifically related to the finding.

- Component 1: Control Environment, Principle 2—The oversight body should oversee the entity's internal control system.

- Component 2: Risk Assessment, Principle 7—Management should identify, analyze, and respond to risks related to achieving the defined objectives.
- Component 3: Control Activities, Principle 11—Management should design the entity's information systems and related control activities to achieve objectives and respond to risks.
- Component 3: Control Activities, Principle 12—Management should implement control activities through policies.
- Component 4: Information and Communications, Principle 13—Management should use quality information to achieve the entity's objectives.
- Component 5: Monitoring Activities, Principle 16—Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
- Component 5: Monitoring Activities, Principle 17—Management should remediate identified internal controls 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 soliciting the OIG's Office of Investigations for indicators and did not identify any instances of fraud or potential fraud during this audit.

Data Reliability

The OIG obtained electronic spreadsheets from eMASS that listed security and privacy controls in place for VDIF and their compliance status and traced the selected control artifacts located in eMASS to supporting documentation. The OIG believes the security and privacy 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 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 determine whether OIT properly developed and implemented IT security and privacy controls, the audit team reviewed a sample of IT security and privacy controls as of March 2, 2021. IT controls include controls relating to security, privacy, and program management such as remote access, data retention and disposal, and risk management strategy. The team used statistical sampling to quantify the extent of security and privacy controls compliance with NIST 800-53 and VA Handbook 6500 requirements.

Population

The review population included 389 security and privacy controls as of March 2, 2021.

Sampling Design

The population of security controls were stratified into two groups. The team judgmentally selected 62 controls, which included controls for policies, privacy controls, and controls identified as noncompliant in eMASS. The audit team also selected a statistical sample of 30 security controls from the remaining population of security controls as seen in table C.1.

Table C.1. Statistical Strata for VDIF Security Controls

Strata	Strata description	Sample size	Population size
1	Judgmental strata	62	62
2	Statistical selection strata	30	327
	Total	**92**	**389**

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

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 error rate estimates by first summing the sampling weights for all sample records that contained the given error, then dividing that value by the sum of the weights for all sample records.

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 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.

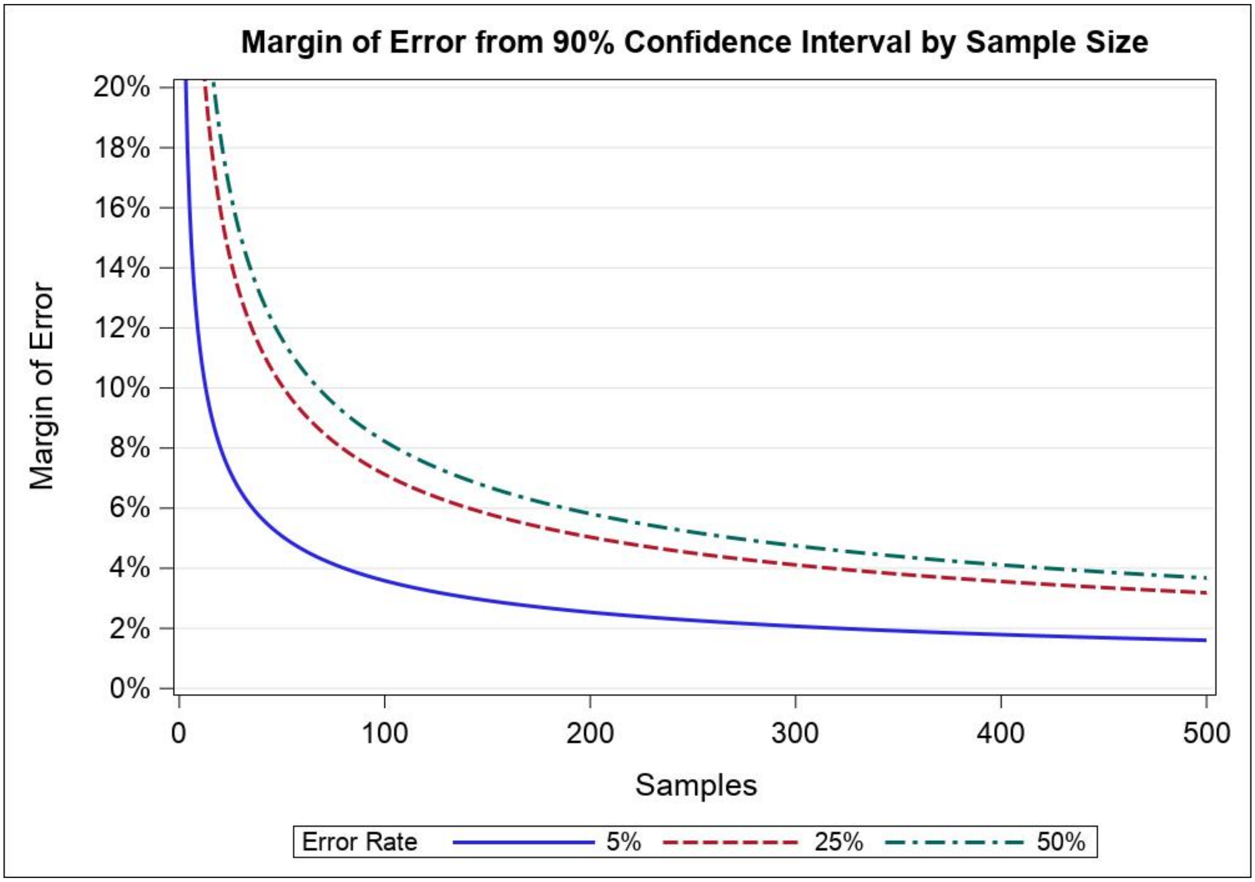

Figure C.1. *Effect of sample size on margin of error.*
Source: VA OIG statistician's analysis.

Projections

Table C.2 shows the projection for the number of VDIF security controls with and without compliance errors.

Table C.2. Statistical Projections Summary for VDIF Security Controls

Compliance error	Estimate	Margin of error based on 90 percent confidence interval	90 percent confidence interval lower limit	90 percent confidence interval upper limit	Sample size
No	117 (30%)	46 (12%)	71 (18%)	163 (42%)	18
Yes	272 (70%)	46 (12%)	226 (58%)	318 (82%)	74
Total	**389**				**92**

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

Appendix D: Management Comments

Department of Veterans Affairs Memorandum

Date: March 23, 2022

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

Subj: OIG Draft Report: Veterans Data Integration and Federation Enterprise Platform Lacks Sufficient Security Controls, Project Number 2021-01123-AE-0047 (VIEWS 06787053)

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

1. The Office of Information and Technology (OIT) is responding to the Office of Inspector General (OIG) Draft Report, Veterans Data Integration and Federation Enterprise Platform Lacks Security Controls.

2. The Veterans Data Integration and Federation Enterprise Platform (VDIF) allows the Department of Veterans Affairs (VA) to share sensitive health information, such as medical chart notes and laboratory results, with the Department of Defense and participating community care providers through the Joint Health Information Exchanges and the eHealth Exchange. By law, VA is required to ensure the safe sharing of Veterans' sensitive personal information. Linking information across an extremely diverse and highly fragmented healthcare system can create technical challenges and increase vulnerabilities. Therefore, establishing the appropriate security categorization for VDIF is necessary to protect Veterans' sensitive personal information.

3. OIT submits written comments, supporting documentation and a target completion date for each recommendation.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

005 Attachment

Office of Information and Technology
Comments on OIG Draft Report
Veterans Data Integration and Federation Enterprise Platform Lacks Sufficient Security Controls, Project Number 2021-01123-AE-0047 (VIEWS 06787053)

Recommendation #1:

The OIG recommends the Assistant Secretary for Information and Technology ensure the Veterans Data Integration and Federation Enterprise Platform security objectives are all set at a categorization level of "high" based upon both the sensitive personal information maintained in the system and the approved risk assessment.

OIT Comments: Non-Concur.

The Department of Veterans Affairs (VA) shares the Office of Inspector General's (OIG) concern with protecting sensitive information, however the authority to assign system categorization level is the responsibility of the Chief Information Officer and the Authorizing Official. VA has properly categorized the Veterans Data Integration and Federation (VDIF) Enterprise Platform system as Moderate. However, since there is Personally Identifiable Information (PII) associated with the system, the Department has implemented additional security controls through the "Privacy Overlay" within the Department's Governance, Risk and Compliance tool, Enterprise Mission Assurance Support Service (eMASS).

Target Implementation Date: Complete. Recommend closure.

Recommendation #2:

The OIG recommends the Assistant Secretary for Information and Technology act to reestablish the Veterans Data Integration and Federation Enterprise Platform in the Enterprise Mission Assurance Support Service to ensure appropriate security controls are implemented and the system is assessed at the high risk level.

OIT Comments: Non-Concur.

VA properly categorized the confidentiality, integrity, and availability of VDIF. The OIG states that an additional 24 information security controls were not added to VDIF due to an inappropriate classification. However, using the Committee on National Security Systems Instruction 1253 baseline, and the eMASS Privacy overlay, VDIF had an additional 71 controls added to the control baseline consistent with the identification of PII and Personal Health Information (PHI) on the system. While VA appropriately categorized the VDIF system, the presence of PII applied the Privacy Overlay to the system, recognizing additional protection mechanisms and security controls are required.

Target Implementation Date: Complete. Recommend closure.

Recommendation #3:

The OIG recommends the Assistant Secretary for Information and Technology ensure the Office of Information Technology provides appropriate oversight and follows proper program management processes and protocols when establishing and monitoring security controls for IT systems.

OIT Comments: Concur.

The Office of Information and Technology will ensure the PII Confidentiality impact evaluation process based on National Institute of Standards and Technology Special Publication 800-122, is implemented and communicated to information system owners. This process will identify the security and privacy controls required to be added to the baseline to address PII and PHI in systems.

Target Implementation Date: December 31, 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.
Audit Team	Al Tate, Director Justice Baek Carolyn Burnett Cynthia Christian Elijah Hancock Omar Madrigal Douglas Neesen Robert Skaggs Herman Woo
Other Contributors	Lee Giesbrecht Dyanne Griffith Charles Hoskinson Yongling Tu

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.