DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Mission Accountability Support Tracker Lacked Sufficient Security Controls

REVIEW

REPORT #21-03080-142

JUNE 22, 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

The VA Office of Inspector General (OIG) evaluated the merits of a May 2021 hotline complaint alleging that the Veterans Benefits Administration (VBA) disregarded privacy procedures so it could more quickly use a system without receiving the appropriate security authorization. The tool, the Mission Accountability Support Tracker (MAST), helps quantify the amount of work VBA's support services staff perform. Support Services Division (SSD) staff in VBA's regional offices are responsible for services related to facility, equipment, and vehicle management; reasonable accommodation requests; and identification card issuance and renewal. VBA employees can request these services in MAST, which provides a centralized system to track and maintain SSD requests, including sending out real-time status updates on previously entered requests.

Because support services employees use personally identifiable information (PII) in their work (such as employee names and personal contact information), this information could be compromised by entering it into an unauthorized application that is not secure.[1] The complaint also alleged that VBA knew that MAST did not have an approved privacy threshold analysis or privacy impact assessment, yet knowingly "loaded" PII into the application.[2] Privacy threshold analysis and privacy impact assessments mitigate the risk of unauthorized access and subsequent data misuse, changes, loss, or disclosure of information. The assessments also help ensure that systems or applications have security controls that are appropriate for the sensitivity of the information stored. Finally, the complaint alleged that VBA started training staff on how to use MAST without a completed privacy threshold analysis or privacy impact assessment, claiming that VBA was aware that a pause in the use was needed until these issues were corrected.[3]

[1] National Institute of Standards and Technology (NIST) Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information,* April 2010, defines PII as any information that can be used to distinguish or trace an individual's identity. VA Handbook 6500, *Risk Management Framework for VA Information Systems VA Information Security Program*, February 24, 2021, defines PII as "any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual." The Federal Information Security Management Act (FISMA) requires NIST to develop technical guidance. For more information about federal standards, see appendix A.

[2] NIST Special Publication 800-122; VA Handbook 6508.1, *Procedures for Privacy Threshold Analysis and Privacy Impact Assessment*, July 30, 2015. A privacy threshold analysis is required to identify information technology systems that include sensitive personal information and affect the privacy of individuals and assesses whether a privacy impact assessment is needed. A privacy impact assessment is a process to identify and help personnel mitigate privacy risks within an information system. It should address risk at every stage of system development and is required before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form.

[3] Appendix B presents the review's scope and the methodology for reviewing the allegations.

What the Review Found

As detailed in the sections that follow, the OIG found that VBA and the Office of Information and Technology (OIT) did not adequately govern MAST. The OIG substantiated the allegations related to the following determinations:

1. VBA and OIT did not correctly follow privacy and security procedures. Specifically,
    a. VBA's privacy threshold analysis was inaccurate and OIT did not conduct a privacy impact assessment; and
    b. OIT's misclassification of MAST as an asset resulted in insufficient security controls.
2. VBA lacked the authority to operate MAST before using it in regional offices.[4]

VBA's Privacy Threshold Analysis Was Inaccurate and OIT Did Not Conduct a Privacy Impact Assessment

VBA is required to follow the National Institute of Standards and Technology (NIST) risk management framework.[5] The framework explains how to manage risk throughout information system design, development, implementation, operation, and disposal and in the environments in which those systems operate.[6] In implementing this process for MAST, VBA and OIT should have obtained an authority to operate from an authorizing official.[7] Obtaining an authority to operate requires (1) performing a privacy threshold analysis and a privacy impact assessment and (2) classifying the system at the appropriate level. These steps help ensure the required security controls match the sensitivity of the information contained in the system and are present before use. However, the OIG determined that VBA and OIT did not follow the required procedures for MAST before deploying this system.

The review team found that although VBA's privacy threshold analysis correctly indicated that MAST would contain PII, VBA incorrectly indicated that OIT did not need to conduct a privacy

[4] "Authority to operate" permits the use of a business product and explicitly accepts the risk to the agency. An approving official signs the authority to operate after a certification agent confirms that the system has passed all requirements to become operational.

[5] 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. Appendix A of this report contains detailed information on security standards and guidelines.

[6] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUBS) 199, February 2004; Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, rev. 5, September 2020, includes updates as of December 10, 2020.

[7] NIST Special Publication 800-37. Authorizing officials can formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Their authority is synonymous with accreditation authority.

impact assessment to fully evaluate the system's privacy vulnerabilities. Nevertheless, OIT should have determined an assessment was necessary. Although OIT approved the privacy threshold analysis, key personnel did not identify VBA's incorrect privacy impact assessment determination or other inaccuracies that should have been noted for a system marked as having PII. Instead, OIT approved VBA's analysis and did not conduct the required assessment for MAST. These issues occurred, in part, because VBA did not follow the required veteran-focused integration process (VIP) to develop MAST.[8]

VIP specifically integrates OIT into system development and provides direction, procedures, and processes that staff must follow for successful information technology project management. Because VBA officials did not follow VIP as required, they missed an opportunity to fully partner with staff from OIT's Office of Information Security in implementing information technology security requirements. Because VBA did not follow an approved project management process, OIT was not properly involved during MAST's project life cycle. Furthermore, MAST did not have the appropriate security controls applied for the PII it contained. For example, users could see requests from other regional offices with protected information—material that should have been limited to those with a need to know.

Misclassification of MAST as an Asset Resulted in Insufficient Security Controls

The team also found that OIT incorrectly classified MAST as an asset instead of a minor application. Minor applications require more security controls than assets due to the sensitive nature of information they contain, such as PII.[9] Because OIT categorized MAST as an asset instead of a minor application, the system lacked security controls to protect its PII. As of September 2021, MAST was reclassified as a minor application. Although OIT has addressed this issue for MAST, OIT should ensure that it correctly classifies all applications and that security controls are implemented.

VBA Lacked the Authority to Operate MAST before Using It in Regional Offices

VBA also began training SSD staff at four regional offices on using MAST in September 2020 and rolled it out to all regional offices by the end of November 2020, even though the privacy threshold analysis was not signed until January 2021. Because required steps were either not performed or were incorrectly conducted, the OIG concluded that VBA did not have the

[8] VA OIT, Veteran-focused Integration Process Guide 3.2, December 2018.

[9] NIST Special Publication 800-18, rev 1, *Guide for Developing Security Plans for Federal Information Systems,* February 2006. A minor application is "an application … that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."

authority to operate MAST before it began using it in regional offices, substantiating that allegation in the hotline complaint.[10]

The OIG also determined that VBA's SSD staff inappropriately entered PII unnecessary for related business tasks, even though the system did not have the necessary information technology security controls or the authority to operate. The review team learned that SSD staff in regional offices had differing understandings and practices concerning what PII they could enter into MAST. As a result, these offices stored unnecessary PII in MAST and stored sensitive information that could be accessible to unauthorized users.

VBA mishandled information because MAST did not have safeguards to prevent inappropriate PII storage, and VBA did not provide adequate oversight of users' practices. In addition, VBA officials did not develop the required policies and procedures to explain how regional offices were to use MAST. By inputting unauthorized PII such as personal contact information into MAST, VBA regional staff risked misuse, loss, or disclosure of that information—particularly because the system's security controls were deficient.

What the OIG Recommended

The OIG recommended that the assistant secretary for OIT and chief information officer ensure minor applications are not misclassified as assets and undergo the appropriate privacy accreditation and certification process. The OIG also called for the implementation of appropriate security and privacy controls during the development of information technology systems before being hosted on VA's network. The under secretary for benefits should also establish a mechanism to make certain that proper OIT project management processes and protocols are followed when establishing information technology systems or applications. Finally, the OIG recommended establishing policies and procedures to ensure staff use MAST appropriately and that the system does not maintain unnecessary PII.

VA Comments and OIG Response

The under secretary for benefits and the assistant secretary for OIT and chief information officer concurred or concurred in principle with all four recommendations. However, the under secretary for benefits and the assistant secretary for OIT and chief information officer did not provide acceptable action plans for recommendations 1, 2, and 3.

The assistant secretary for OIT and chief information officer concurred with the first recommendation to develop controls to help ensure minor applications are not misclassified as assets and undergo the appropriate security accreditation and certification process. VA reported it had remediated the identified issues for MAST and requested closure of the recommendation,

[10] As to the allegation that VBA was aware a pause was needed to complete needed assessments before the program could be used, the team concluded that the framework was clear about those requirements.

indicating that it has a standard operating procedure that addresses the classification of minor applications. However, this procedure was in effect at the time of this review and did not prevent the issues identified in this report. Therefore, the OIG will keep this recommendation open until VA demonstrates progress toward ensuring the procedure is followed.

The assistant secretary for OIT and chief information officer and the under secretary for benefits concurred with recommendation 2 to make certain that appropriate security and privacy controls are implemented during the development of information technology systems before being hosted on VA’s network. VA reported it had remediated the identified issues for MAST and requested closure of the recommendation, indicating that it has a standard operating procedure that addresses the classification of minor applications. As with recommendation 1, the procedure was in effect at the time of this review and did not prevent the issues identified in this report. Until VA takes steps to ensure the procedure is followed, the recommendation will remain open.

The under secretary for benefits, in conjunction with the assistant secretary for OIT and chief information officer, concurred in principle with recommendation 3 to establish a mechanism to gain assurance that proper OIT project management processes and protocols are followed when establishing information technology systems and applications. VA’s response indicated VBA follows OIT processes and protocols. However, as previously discussed, these controls were not followed for MAST. As such, the OIG will keep this recommendation open until VA shows progress in addressing the intent of the recommendation.

The under secretary for benefits concurred with recommendation 4 to establish policies and procedures to ensure MAST is used appropriately and does not contain unnecessary PII. The under secretary stated VBA will update the MAST user guide to include specific language restricting the inclusion of PII in open data fields and will conduct training for end users on the updates.

Appendix C includes the full text of comments from the assistant secretary for OIT and chief information officer and the under secretary for benefits.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

DevSecOps	development, security, and operations
eMASS	Enterprise Mission Assurance Support Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
MAST	Mission Accountability Support Tracker
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
PII	personally identifiable information
PIV	personal identity verification
SSD	Support Services Division
VBA	Veterans Benefits Administration
VIP	veteran-focused integration process

Introduction

The VA Office of Inspector General (OIG) evaluated the merits of a May 2021 hotline complaint alleging that the Veterans Benefits Administration (VBA) disregarded privacy procedures so it could more quickly use a system without receiving the appropriate security authorization. The system, the Mission Accountability Support Tracker (MAST), is a tool to quantify and track the amount of work VBA's support services employees perform and to track requests for their assistance from other departments within VBA. The complaint indicated that because VBA did not fully complete privacy procedures and receive authorization to operate the system, personally identifiable information (PII) entered into the unauthorized system could be at risk of being compromised.

According to the National Institute of Standards and Technology (NIST), PII is any information that can be used to distinguish or trace an individual's identity, such as name; social security number; date and place of birth; mother's maiden name; biometric records; and any other information that can be linked to an individual, such as medical, educational, financial, and employment information.[11] PII can also include personal identity verification (PIV) numbers, which link an individual's social security number, date of birth, and home and email addresses. Specifically, the complaint alleged that VBA staff knowingly entered PII into MAST without the approved privacy threshold analysis or privacy impact assessment, as required.[12] Both of these security assessments mitigate risk of unauthorized access, data loss or misuse, or disclosure of information, and they help to ensure that systems or applications store sensitive information with the right level of security. Finally, the complaint alleged that VBA started training staff on how to use MAST without a completed privacy threshold analysis or privacy impact assessment, claiming that VBA was aware that it needed to pause using the application until these issues were corrected.

VA's Persistent Challenges with Information Security

Information security is a high-risk area throughout the government, and VA is no exception. As the examples below demonstrate, the OIG has repeatedly found that although VA has made

[11] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, April 2010.

[12] NIST Special Publication 800-122; VA Handbook 6508.1, *Procedures for Privacy Threshold Analysis and Privacy Impact Assessment*, July 30, 2015. A privacy threshold analysis is required to identify information technology systems that include sensitive personal information that affect the privacy of individuals. The privacy threshold analysis also assesses whether there is a need for a privacy impact assessment. A privacy impact assessment identifies and mitigates privacy risks in an information system, should address risk at every stage of system development, and is required before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form.

progress in some areas, it has not consistently implemented components of its own agencywide information security risk management program:

- Although VA has made advances in developing, documenting, and distributing policies and procedures as part of its security risk management program, the fiscal year 2021 Federal Information Security Modernization Act (FISMA) audit identified continuing significant deficiencies related to access, configuration management, change management controls, and service continuity practices designed to protect mission-critical systems from unauthorized access, alteration, or destruction.[13] Additional details about the FISMA audit and federal standards for protecting PII can be found in appendix A.
- The Office of Information and Technology (OIT) lacked involvement in the deployment of the Veterans Health Administrations' initial information technology system for the Family Caregiver Program—the Caregiver Application Tracker. The lack of OIT involvement hindered the implementation of subsequent systems designed for the program and resulted in an inaccurate security assessment.[14]
- OIT inappropriately set the security risk level for VBA's Beneficiary Fiduciary Field System at a moderate level instead of high because risk managers did not follow established standards and did not consider the protected health information and PII stored in the system's database.[15]
- Some applications were in use on the VA network without proper authorization, and others were not granted authority to operate by OIT.[16]
- Sensitive personal information was left unprotected on two shared network drives at the Milwaukee regional office. The OIG determined the mishandling of sensitive personal information was a national issue.[17]

VA needs to continue to address these identified weaknesses and the information security issues discussed in this report by ensuring risk management procedures are consistently and properly

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

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

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

[16] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019*, Report No. 19-06935-96, March 31, 2020.

[17] VA OIG, *Mishandling of Veterans Sensitive Personal Information on VA Shared Network Drives*, Report No. 19-06125-218, October 17, 2019. Sensitive personal information includes individually identifiable information, individually identifiable health information, protected health information, and privacy-protected information.

applied to all its systems and applications. Failure to do so leaves sensitive personal information inadequately protected.

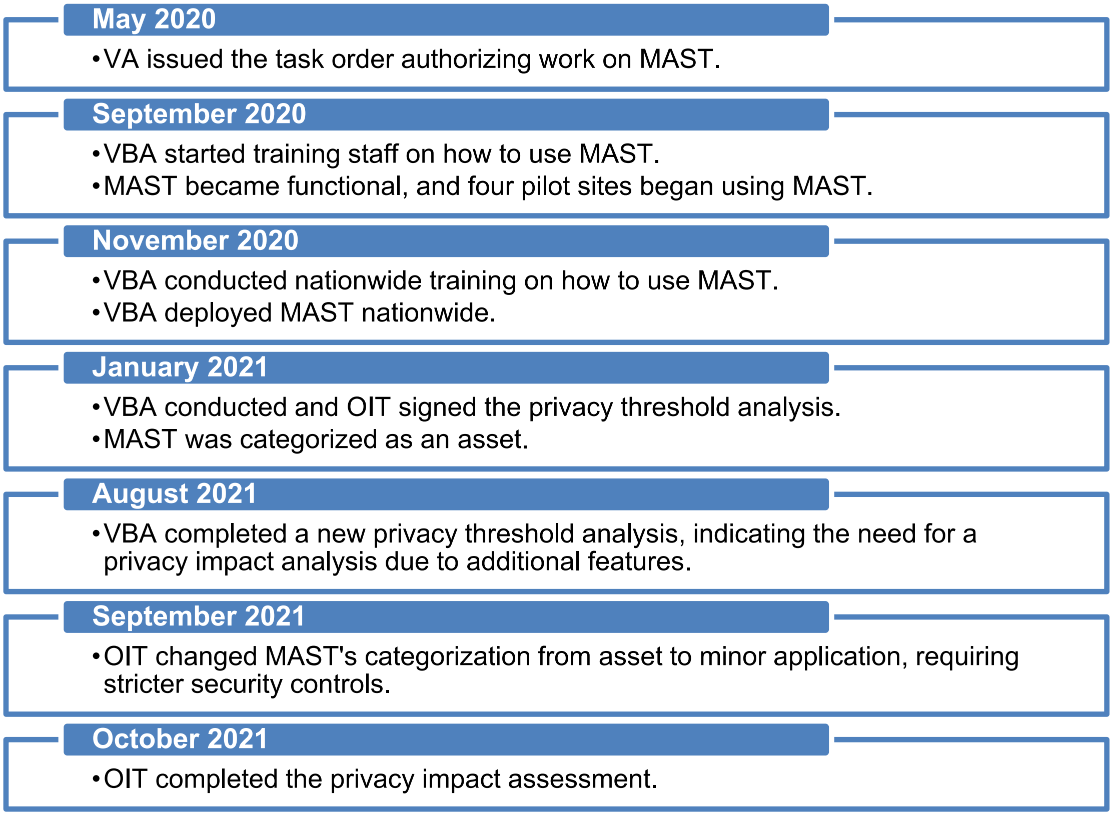
Mission Accountability Support Tracker

MAST was designed to provide VBA's Support Services Division (SSD) managers with a tool to quantify the amount of work SSD employees perform. Using MAST, SSD managers can run reports or view individual tasks to see the number of requests their employees process. SSD staff in VBA regional offices are responsible for facility, equipment, and vehicle management; reasonable accommodation requests; and PIV functions, including issuing and renewing identification cards so employees can access facilities and systems. VBA employees can request these SSD services in MAST, which provides a centralized system to submit, log, track, and maintain requests, including sending out real-time status updates on entered requests. MAST was intended to store limited PII, such as employee and contractor names, work phone numbers, and email addresses, in addition to sensitive information linked to PIV numbers such as social security numbers for VA employees and contractors.

MAST Development Timeline

In 2017, VBA contracted with Accenture Federal Services to design future applications, such as MAST, on the Salesforce platform—a moderate-risk, Federal Risk and Authorization Management Program cloud environment.[18] In 2020, a task order was issued authorizing Accenture to begin work on MAST. According to an SSD chief who was a project lead for MAST, VBA's under secretary for benefits and the deputy under secretary for the Office of Field Operations both approved the project. The initial task order was for approximately $491,000, and the original contract included options for future task orders. As of October 2021, the project cost for MAST was about $1.25 million. Figure 1 shows a high-level timeline of key steps in the implementation of MAST.

[18] "FedRAMP," accessed November 18, 2020, https://www.fedramp.gov/about. The Federal Risk and Authorization Management Program was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government.



May 2020

- VA issued the task order authorizing work on MAST.

September 2020

- VBA started training staff on how to use MAST.
- MAST became functional, and four pilot sites began using MAST.

November 2020

- VBA conducted nationwide training on how to use MAST.
- VBA deployed MAST nationwide.

January 2021

- VBA conducted and OIT signed the privacy threshold analysis.
- MAST was categorized as an asset.

August 2021

- VBA completed a new privacy threshold analysis, indicating the need for a privacy impact analysis due to additional features.

September 2021

- OIT changed MAST's categorization from asset to minor application, requiring stricter security controls.

October 2021

- OIT completed the privacy impact assessment.

***Figure 1.** Overview of MAST implementation timeline.*

Source: VA OIG analysis.

Risk Management Framework Used by VA

VA is required to follow FISMA, which also tasked NIST with developing standards and guidelines for federal agency information security.[19] The NIST Federal Information Processing Standards (FIPS) govern information security requirements for minimizing the risk to protected information. The NIST framework provides guidance for managing risk throughout information system design, development, implementation, operation, and disposal, and in the environments in which those systems operate.[20]

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

[20] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication (FIPS PUBS) 199, February 2004; Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, rev. 5, September 2020, includes updates as of December 10, 2020.

The framework consists of seven steps, which make up a process that repeats throughout the risk management life cycle:[21]

1. Prepare to execute the risk management framework from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
2. Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
3. Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
4. Implement the controls and describe how the controls are employed within the system and its environment of operation.
5. Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
6. Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the nation is acceptable.
7. Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

The risk management framework begins by establishing the context and priorities for managing security and privacy risk. The next step determines the information system security categorization level, which includes conducting a privacy threshold analysis and a privacy impact assessment. VA uses these assessments to analyze the information in the system and determine the security level.[22] VA also uses the Enterprise Mission Assurance Support Service (eMASS) to generate a system security authorization package.[23] After a certification agent confirms that the system or application has passed all requirements to become operational, it is granted authority to operate. "Authority to operate" is a formal declaration by a designated

[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.

[22] NIST Special Publication 800-122; VA Handbook 6508.1, *Procedures for Privacy Threshold Analysis and Privacy Impact Assessment*, July 30, 2015.

[23] eMASS is a web-based application that automates the process of setting security controls for VA systems throughout the risk management framework.

approving official that sanctions the operation of a business product and explicitly accepts the risk to the agency.[24] Figure 2 shows the risk management framework process.

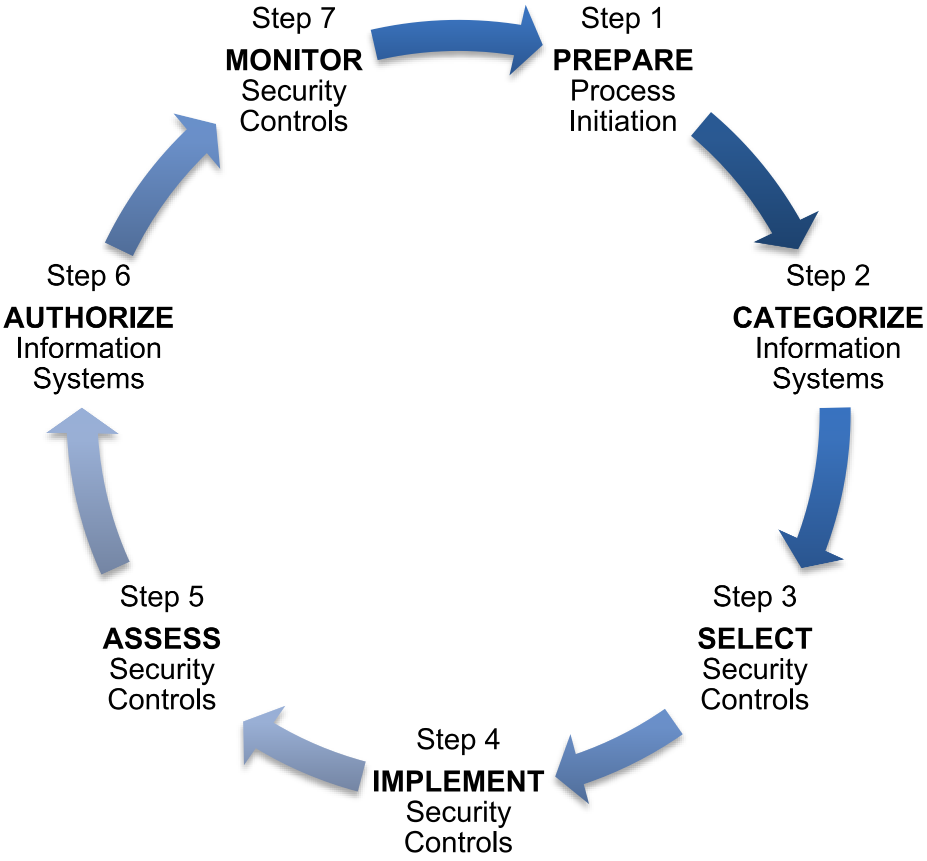


Figure 2. *Overview of NIST's risk management framework process.*

Source: OIG modification of figure in NIST Special Publication 800-53, rev. 5.

NIST Special Publication 800-53 and VA Handbook 6500 specify the applicable security controls based on the risk level of the data in an information system.[25] See appendix A of this report for detailed information on security standards and guidelines.

[24] NIST Special Publication 800-37. "Authority to operate" permits the use of a business product and explicitly accepts the risk to the agency. The authority to operate is signed after a certification agent confirms the system has passed all requirements to become operational. Authorizing officials can formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Their authority is synonymous with accreditation authority.

[25] NIST Special Publication 800-53; VA Handbook 6500, *Risk Management Framework for VA Information Systems–Tier 3: VA Information Security Program*, March 2015.

Enterprise Mission Assurance Support Service for Categorizing the Security Level of Systems or Applications

OIT categorizes VA systems or applications in eMASS using a web-based application that automates the process of setting security controls. Based on the risk assessment results, eMASS automatically populates the confidentiality, integrity, and availability for some information types. Once security controls are applied, eMASS does not allow changes to the control information. There is dashboard reporting in eMASS, workflow automation, and continuous monitoring that create a repository of the information created during the seven steps of the risk management framework.

Salesforce Hosts MAST, but Controls Vary for Its Applications Based on OIT Categorization

Salesforce is a cloud-based platform that hosts various systems and applications—including MAST. OIT categorizes the information technology hosted on Salesforce as assets or as minor or major applications:

- **Assets** are applications residing within the same platform, such as Salesforce. Assets do not require any additional controls.
- **Minor applications** require attention to security due to the risk and magnitude of harm resulting from loss, misuse, or unauthorized access to the information in the application. Minor applications include 177 security and privacy application controls, in addition to the controls in Salesforce.
- **Major applications** include mission-critical systems that require special management oversight and tighter security as the risk of harm is even greater than with minor applications if there is loss, misuse, or unauthorized access to information in the application. Major applications include 188 security and privacy application controls, in addition to the controls in Salesforce.

Results and Recommendations

Finding: VBA and OIT Did Not Adequately Govern MAST

The OIG substantiated the allegation that VBA disregarded privacy procedures when developing MAST and populating it with PII, thereby putting that information at risk of misuse. Specifically, the review team found VBA did not prepare an accurate privacy threshold analysis for MAST. Then, OIT did not thoroughly read that analysis and depended on VBA's assertion that no further assessment was needed, which led OIT to incorrectly conclude it did not need to conduct a privacy impact assessment. These privacy procedures are used to determine the level of security controls for an application based on its classification as an asset, a minor application, or a major application. As noted above, OIT originally classified MAST as an asset rather than a minor application that has heavier security controls. Furthermore, VBA did not use the required project management process for deploying MAST. Using the correct project management process would have positioned VBA to work more closely with OIT to obtain the authority to operate before using MAST. Because VBA did not follow this process, OIT was not fully involved in the development and MAST did not have the appropriate security controls required for the PII it contained. VBA also began training staff on how to use MAST without a completed privacy threshold analysis or privacy impact assessment, despite clear guidance that the application could not be used until these actions were properly accomplished.

The OIG confirmed the allegation that VBA staff entered PII into the unauthorized MAST application without adequate security controls in place to protect the information. This occurred in part because VBA officials did not provide SSD staff with sufficient guidance, such as policies and procedures explaining how to use MAST and how to prevent entering information that should not be stored in the application. VBA and OIT need to implement the required security controls for MAST. Policies and procedures should also limit PII used in MAST to only what is needed, and more effectively protect it from misuse.

The finding builds on the following determinations:

- VBA and OIT did not correctly follow privacy and security procedures.
  - VBA's privacy threshold analysis was inaccurate and OIT did not conduct a privacy impact assessment.
  - OIT incorrectly classified MAST as an asset, resulting in inadequate security controls for the sensitivity of its information.
- VBA lacked the authority to operate MAST before using it in regional offices.

What the OIG Did

The team reviewed MAST's privacy threshold analysis to evaluate whether it needed a privacy impact assessment and had adequate security controls. The review team interviewed staff in three VBA regional offices: Denver, Colorado; Oakland, California; and St. Petersburg, Florida. During these interviews, SSD staff demonstrated how they used MAST. To determine whether MAST contained PII, as alleged, the team interviewed SSD chiefs, supervisors, and personnel. Additionally, the team interviewed OIT's information system security officer, privacy officer, and other personnel involved in categorizing and maintaining MAST to determine whether they established appropriate privacy and security controls. To assess whether the development and implementation of MAST met requirements, the team reviewed VA directives and handbooks, FIPS, and NIST security and privacy guidelines. Further discussion of the scope and methodology of this review can be found in appendix B.

VBA and OIT Did Not Correctly Follow Privacy and Security Procedures

As part of the overall risk management framework process, VBA needs to obtain an authority to operate before using a new information technology system or application. During this process for MAST, VBA and OIT should have (1) performed a privacy threshold analysis, which would determine if a privacy impact assessment was also needed, and (2) classified the application at the appropriate level on Salesforce and in eMASS. These steps help ensure required security controls are in place before use and that the controls match the sensitivity of the information. However, the OIG determined that VBA and OIT did not follow the required procedures for MAST before deploying the application on Salesforce and substantiated the allegation that VBA started training staff and using MAST before the required steps were completed.

Although VBA did perform a privacy threshold analysis, it incorrectly concluded a privacy impact assessment was not necessary. This determination was not consistent with NIST or VA requirements because MAST contained PII.[26] As stated earlier, a privacy impact assessment identifies privacy risks within an information system and helps personnel mitigate these risks. Privacy impact assessments should address risk at every stage of system development and are required before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form such as PII. Despite the privacy threshold analysis not being signed until January 2021, VBA began training SSD staff at four regional offices on the use of MAST in September 2020, and all regional offices were using MAST by the end of November 2020 contrary to clear guidance.

[26] NIST Special Publication 800-122; VA Handbook 6508.1.

VBA's Privacy Threshold Analysis Was Inaccurate and OIT Did Not Conduct a Privacy Impact Assessment

The OIG substantiated allegations that VBA's privacy threshold analysis for MAST was inaccurate and that OIT did not conduct a privacy impact assessment. According to NIST's risk management framework, VBA should have completed a privacy threshold analysis before using MAST. However, VBA conducted the analysis in January 2021—four months after four pilot offices began using MAST.[27] As stated earlier, the privacy threshold analysis determines whether a system or application contains PII and what privacy requirements apply. The review team found that although VBA's delayed analysis correctly indicated that MAST would contain PII, VBA officials incorrectly indicated that OIT did not need to conduct a privacy impact assessment. However, an assessment was required to fully evaluate MAST's privacy vulnerabilities.

Although OIT's privacy officer, information system security officer, and information system owner approved the privacy threshold analysis, they did not identify the incorrect privacy impact assessment determination or other inaccuracies. For example, the review team found that the privacy threshold analysis stated a data field containing PIV identification numbers would be encrypted when it was not. If PIV identification numbers are unencrypted, individuals' social security numbers, dates of birth, and home and email addresses could be compromised. If OIT had followed the directions on the privacy threshold analysis review form, it would have discovered these deficiencies during the review.[28]

When completing the privacy threshold analysis, VBA indicated at the beginning of the form that MAST contained PII. Any system or application that contains PII needs a privacy impact assessment. However, VBA incorrectly marked at the end of the form that no assessment was needed, and OIT did not complete one. However, OIT should have reviewed the entire form and noticed the discrepancy that MAST contained limited PII but was marked as not needing a privacy impact assessment—as it is not possible for both these statements to be true. OIT is required to assess the privacy threshold analysis in accordance with VA Handbook 6500 to determine whether there is a need for a privacy impact assessment and if any other privacy requirements apply to the IT system. Accordingly, the review team found that OIT should have determined an assessment for MAST was necessary since it contains PII. Instead, it approved VBA's analysis and did not conduct the required assessment for MAST. Without this assessment, VBA could not ensure that MAST's security controls were sufficient for the information it contained. After the OIG started its review in August 2021, VBA and OIT began taking steps to address this oversight.

[27] VBA personnel involved in preparing the privacy threshold analysis included a program manager, contracting officer representative, and SSD chiefs.

[28] VA Privacy Threshold Analysis, Version Date: April 1, 2020.

VBA is required to conduct a new privacy threshold analysis when a system or application changes its functions, which MAST did when it added General Services Administration Fleet Management functionalities in August 2021.[29] OIT signed the new analysis on August 9, 2021. This new privacy threshold analysis correctly indicated that OIT should complete a privacy impact assessment, which OIT completed in October 2021. Although VBA and OIT have addressed this issue for MAST due to the additional functionality, MAST's privacy controls were insufficient from the time it was implemented until the new privacy impact assessment was complete. It is important that all new systems and applications undergo the appropriate security accreditation and certification process to ensure the necessary privacy controls are implemented.

OIT Incorrectly Classified MAST as an Asset, Resulting in Inadequate Security Controls for the Sensitivity of Its Information

The review team also found that OIT's Digital Transformation Center incorrectly classified MAST as an asset on Salesforce and in eMASS when it should have been classified as a minor application. An application's classification determines the level of security and privacy controls the application needs to be authorized to operate. Minor applications require more security controls than assets due to the sensitive nature of information they contain, such as PII.[30] Because OIT categorized MAST as an asset instead of a minor application, the system lacked security controls to protect PII. For example, minor applications are required to limit who can view data, while assets do not have this requirement.[31] According to an OIT manager, OIT is in the process of reviewing and reclassifying assets as minor applications on Salesforce and in eMASS, as appropriate. As of September 27, 2021, MAST was reclassified as a minor application. Although OIT has addressed this issue for MAST, OIT should ensure that it correctly classifies all applications and that security controls are implemented.

VBA Did Not Use the Veteran-Focused Integration Process for MAST

Classification issues with MAST occurred in part because VBA did not follow the required veteran-focused integration process (VIP) to develop the system.[32] VIP is designed to track and

[29] NIST Special Publication 800-122; VA Handbook 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*, October 15, 2014. "A PTA must be completed…when a major change occurs to an existing IT system." Major change is defined as "[a] change to the information collected or maintained that could result in greater disclosure of information or change in the way personal data is used."

[30] NIST Special Publication 800-18, rev 1, *Guide for Developing Security Plans for Federal Information Systems,* February 2006. A minor application is "an application … that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application."

[31] NIST Special Publication 800-53. The control AC-3 is called "access enforcement."

[32] VA OIT, *Veteran-focused Integration Process Guide*, ver. 3.2, December 2018. "VIP, a lean-agile framework, allows more frequent delivery of essential IT services and minimal oversight processes, enhances the ability to track and monitor IT performance, and strengthens management oversight and accountability."

monitor system performance, as well as strengthen management oversight and accountability. Furthermore, VIP integrates OIT into system development and provides direction, procedures, and processes that staff must follow for successful information technology project management. The VIP framework was mandated for any project that touches the VA network, unless OIT's deputy assistant secretary of development security and operations (DevSecOps) approves use of the streamlined DevSecOps release process.[33]

A program analyst for the Office of Business Integration stated VBA followed the DevSecOps process instead of VIP; however, he was mistaken. The analyst believed that the DevSecOps process was used, as the analyst stated VBA staff provided all MAST documentation to OIT's Digital Transformation Center and included staff from the center on calls discussing schedules and deadlines for architectural design reviews, guidance on design approach, and instructions for deploying applications on Salesforce.[34] Although OIT's Digital Transformation Center was involved, it is not part of the DevSecOps process, and VBA staff never applied to the deputy assistant secretary of DevSecOps for approval to use the DevSecOps process. According to OIT's project special forces enterprise data service investment manager who heads that process, the analyst was mistaken, and VBA did not use either VIP or DevSecOps to develop MAST.

As part of the authority-to-operate process, VBA staff should have involved OIT's Office of Information Security personnel in MAST development and implementation. OIT has specific guidance on how to develop new information technology projects. If VBA had followed VIP or the DevSecOps process, OIT would have been more engaged.[35] Instead, due to VBA's lack of adequate and coordinated governance, OIT was not effectively involved. Because VBA officials did not follow VIP as required, they missed the opportunity for Office of Information Security personnel to help implement information technology security requirements. For example, this office must take security measures such as comparing MAST's security features to VA and NIST requirements and identify missing security controls.[36] Additionally, the office is mandated to review the privacy threshold analysis to ensure that VBA's determination was accurate.[37] All these steps would have shown that MAST did, in fact, require a privacy impact assessment.

[33] "DevSecOps Release Process," VA OIT, accessed October 7, 2021, https://vaww.oit.va.gov/oit/devsecops/release-process/. (This is an internal website not publicly accessible.)

[34] The center was created in 2018 to accelerate VA's digital modernization and use of emerging technologies to better serve veterans and military families.

[35] VA Directive 0214, *Department of Veterans Affairs Enterprise Governance Structure and Process*, May 14, 2019. Governance is the process of management or oversight by which VA leaders make informed decisions, provide strategic direction, and maintain accountability based on objectives, risks, and resources.

[36] NIST Special Publication 800-37. "The risk management framework includes activities to prepare organizations to execute the framework at appropriate risk management levels … In addition, it establishes responsibility and accountability for the controls implemented within an organization's information systems and inherited by those systems."

[37] NIST Special Publication 800-122; VA Handbook 6508.1, *Procedures for Privacy Threshold Analysis and Privacy Impact Assessment*, July 30, 2015.

MAST Security Controls Were Not Sufficient to Protect PII

Because VBA did not follow the correct process to obtain authority to operate, MAST did not have the required security controls for applications with the PII that MAST contains. For example, MAST did not have a requirement to log the user out after a period of inactivity; instead, the user remains logged in, and MAST continues to run even when not in use.[38] This creates the risk that unauthorized users could access data by simply going to an authorized user's station and opening the system. In addition, according to NIST, PII should be viewed only by those with a need to know to complete their job.[39] However, MAST users with supervisory access or higher can view requests for all regional offices, not just their own. For example, an SSD supervisor at the St. Petersburg regional office showed the review team a supply request from the Winston-Salem regional office that contained the requester's personal address, which is unauthorized PII for MAST. As the next section underscores, unauthorized access and misuse, loss, or changes to data can result in greater harm when the system stores unnecessary PII. The PII in MAST included home addresses and dates of birth, which were not required for functionality. By not sufficiently limiting who can view this information, VBA unnecessarily placed PII at risk.

VBA Lacked the Authority to Operate MAST before Using It in Regional Offices

Because MAST was not established with the appropriate security controls to safeguard sensitive information, some regional offices' practice of entering PII into MAST potentially put that information at risk. The privacy threshold analysis was not completed until January 2021 (after nationwide deployment), and a privacy impact assessment along with an authority to operate was not performed. The authority to operate would have ensured the required security controls were present before use and matched the sensitivity of the information contained in MAST.

Users Improperly Entered PII into MAST and Used the System Differently

The review team found that although MAST was designed to contain limited PII for VA employees and contractors, such as names, phone numbers, email addresses, and PIV numbers, staff at some regional offices entered additional PII such as home addresses and dates of birth. Users had potentially been doing so since September 2020, when four pilot regional offices began using MAST, and the system was deployed nationwide in November 2020.

[38] NIST Special Publication 800-53. Control AC-2 (5) is called "account management inactivity log out."

[39] NIST, FIPS Pub 199; NIST Special Publication 800-53.

The review team determined that regional office staff did not always understand what PII they could enter into MAST, and offices had different practices for using the system. For example, the Oakland regional office staff used MAST infrequently and, as a result, were unfamiliar with the system and its PII requirements. Some staff at the Denver regional office added the requesting employee's date of birth into the comment field of MAST, even though the system did not have suitable security controls for protecting this type of information. Conversely, the St. Petersburg regional office, a pilot site that had been using MAST longer than the other offices, was aware of the areas in the system that could contain PII. St. Petersburg employees reviewed requests to actively ensure unnecessary PII was not entered into the system and returned requests with PII to the originator.

Overall, SSD staff were unsure when to use MAST instead of other systems available to them. According to an SSD chief, MAST was never intended to replace a system or process already in place. However, some staff were using MAST to supplement PIV card processing in USAccess.[40] SSD staff use the USAccess system to complete the PIV process. Because USAccess was designed to process PIV cards from issuance to destruction, it is equipped with the necessary security and privacy controls intended for PII. In contrast, according to an SSD chief who was a project lead for MAST, it is only intended to track how many PIV requests each SSD employee processed. However, the review team found that SSD employees at the Denver regional office were using comment fields to enter unnecessary PII into MAST in hopes of speeding up the PIV card issuance process, putting the information at risk.

VBA officials did not provide appropriate guidance to SSD staff on how to ensure MAST did not contain PII for which it was not designed. Without guidance such as standard operating procedures, VBA regional office staff did not know how to use MAST. By inputting PII into MAST instead of the appropriate and more secure applications, staff put that information at risk unnecessarily—particularly because MAST's security controls were deficient when regional offices began using the system.

During this review, the team also found that SSD staff were storing spreadsheets containing PII on an unsecured network shared drive. The drive was accessible to regional office SSD network users, even though unauthorized users should not be able to access PII without a business need.[41] Although not related to MAST, this is a serious mismanagement of PII. The team notified the SSD officials at the regional office so that corrective actions could be taken to end this practice.

[40] USAccess is a shared service that provides PIV card credentialing services and support for federal employees and contractors at established locations throughout the country.

[41] VA Directive 6500, *VA Cybersecurity Program*, January 23, 2019.

Conclusion

VBA and OIT did not comply with established processes for developing MAST. By not properly conducting the steps to obtain an authority to operate or following the VIP process, VBA and OIT did not ensure the appropriate security and privacy controls were in place to protect the PII within MAST. VBA and OIT have taken steps to correct these deficiencies, such as conducting a new privacy threshold analysis, conducting a privacy impact assessment, and classifying MAST as a minor application. However, VBA needs to ensure future information technology projects follow an approved OIT project management process. Furthermore, VBA needs to provide sufficient guidance to staff to ensure MAST is used as intended so that the PII of VA employees and contractors remains secure.

Recommendations 1–4

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

1. Develop controls to help ensure minor applications are not misclassified as assets and undergo the appropriate security accreditation and certification process.
2. In conjunction with the under secretary for benefits, make certain that appropriate security and privacy controls are implemented during the development of information technology systems before being hosted on VA's network.

The OIG made the following recommendations to the under secretary for benefits:

3. In conjunction with the assistant secretary for information and technology, establish a mechanism to gain assurance that proper Office of Information Technology project management processes and protocols are followed when establishing information technology systems and applications.
4. Establish policies and procedures to ensure the Mission Accountability Support Tracker is used appropriately and does not contain unnecessary personally identifiable information.

VA Management Comments

The assistant secretary for OIT and chief information officer concurred with recommendation 1 to develop controls to help ensure minor applications are not misclassified as assets and undergo the appropriate security and accreditation and certification process. VA reported that in August 2021, OIT's Office of Information Security Governance Risk and Compliance division directed the DevSecOps Salesforce Security Team to identify and change all Salesforce platform applications previously classified as assets as minor applications within eMASS. In November 2021, MAST completed approval and authorization in eMASS as a minor application, which ensures that all the appropriate security controls are in place within the Salesforce platform. The Office of Information Security has a published standard operating procedure to accurately document security and privacy controls in eMASS. VA requested this recommendation be closed based on the actions taken.

The assistant secretary for OIT and chief information officer, in conjunction with the under secretary for benefits, concurred with recommendation 2 to make certain that appropriate security and privacy controls are implemented during the development of information technology systems before being hosted on VA's network. Per revised direction provided by the Office of Information Security Governance Risk and Compliance, all applications for the Salesforce platform are evaluated and presented to the Office of Information Security Governance Risk Compliance division for determination as a minor or major application; the DevSecOps security team will ensure and document in eMASS that all required security artifacts are governed and controlled per policy. The initial privacy threat analysis completed for MAST indicated a privacy impact assessment was not required; however, in July 2021, an amended analysis was completed indicating an assessment was required. The assessment was completed in October 2021. VA reported it had remediated the identified issues for MAST and requested closure of the recommendation, stating it has a standard operating procedure to accurately document security and privacy controls in eMASS.

The under secretary for benefits and the assistant secretary OIT and chief information officer concurred in principle with recommendation 3 to establish a mechanism to gain assurance that proper OIT project management processes and protocols are followed when establishing information technology systems and applications. VA's response indicated VBA follows OIT processes and protocols including the Digital Transformation Center standard operating procedures for the VA Salesforce platform, the VA Digital Transformation Center System Integrator checklist, and the policy handbook dated spring 2021. VA also reported VBA's adherence to and utilization of these resources are confirmed by OIT's Digital Transformation Center and the Salesforce Government Cloud Security team, the information system security officer, system steward, and information security officer. VA's response indicated VBA follows OIT processes and protocols and no additional mechanism is warranted; therefore, they requested closure of the recommendation.

The under secretary for benefits concurred with recommendation 4 to establish policies and procedures to ensure MAST is used appropriately and does not contain unnecessary PII. The under secretary stated VBA will update the MAST user guide to include specific language restricting the inclusion of PII in open data fields and will train end users on the updates.

Appendix C includes the full text of comments from the assistant secretary for OIT and chief information officer and the under secretary for benefits.

OIG Response

The under secretary for benefits and the assistant secretary for OIT and chief information officer concurred or concurred in principle with all four recommendations. However, the under secretary for benefits and the assistant secretary for OIT and chief information officer did not provide acceptable action plans for recommendations 1, 2, and 3.

Although the assistant secretary for OIT and chief information officer requested closure of recommendation 1, the OIG notes the referenced standard operating procedure was in effect at the time of this review and did not prevent the issues identified in this report. The OIG recognizes that MAST is now classified as a minor application; however, this recommendation will remain open until VA develops a control to ensure minor applications are not misclassified as assets and undergo the appropriate security accreditation and certification process.

The assistant secretary for OIT and chief information officer in conjunction with the under secretary for benefits also requested closure of recommendation 2, again referring to the standard operating procedure. However, as with recommendation 1, the procedure was in effect at the time of this review and did not prevent the issues identified in this report. Therefore, until VA takes steps to make certain that appropriate security and privacy controls are implemented during the development of information technology systems before being hosted on VA’s network, the recommendation will remain open.

The under secretary for benefits and the assistant secretary for OIT and chief information officer requested the OIG close recommendation 3. However, as previously discussed, these controls were not followed for MAST. Therefore, the OIG will keep recommendation 3 open until VA establishes a mechanism to gain assurance that proper OIT project management processes and protocols are followed when establishing information technology systems and applications.

For recommendation 4, the under secretary for benefits reported a target completion date for corrective actions of September 30, 2022. The OIG will close this recommendation when it receives sufficient evidence that the user guide has been updated and progress is demonstrated toward training end users.

Appendix A: Background on Security Standards

Information Security Standards and Guidelines

VA is required to follow federal information security standards, including the E-Government Act of 2002.[42] The act established FISMA and 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 security controls over information resources that support federal operations and assets. FISMA defines three security objectives for information and information systems:

- **Confidentiality.** Preserve 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.** Guard 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.** Ensure 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.[43]

FISMA tasked NIST to develop standards and guidelines for information security for all federal agencies.[44] FIPS Publication 199 addresses the FISMA requirements to establish security categories for both information and information systems.[45] 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.

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

[43] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Pub 199, February 2004.

[44] NIST, FIPS Pub 199.

[45] NIST, FIPS Pub 199.

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.
- **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 these security requirements.[46] These requirements cover 17 areas related to 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 to 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.

[46] NIST, *Minimum Security Requirements for Federal Information and Information Systems*," FIPS PUBS 200*,* March 2006.

- **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 or authorities.
- **Risk assessment.** Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting 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.

Prior VA OIG FISMA Audit

In an April 2021 audit report, the OIG found that VA had not consistently implemented components of its agencywide information security risk management program to meet FISMA requirements.[47] The OIG identified several instances of systems that were granted an authority to operate without undergoing an independent assessment of security controls. The OIG recommended the assistant secretary for information and technology consistently implement an improved continuous monitoring program in accordance with NIST's risk management framework. Specifically, VA should implement an independent security control assessment process to evaluate the effectiveness of security controls before granting authorization decisions. This is a repeat recommendation from prior years.

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

Appendix B: Scope and Methodology

Scope

The OIG review team performed its review from August 2021 through March 2022 to assess the allegations that VBA disregarded VA security and privacy procedures when developing and implementing MAST.

Methodology

To gain an understanding of the planning and implementation of MAST, the review team interviewed OIT officials including the information system owner, the privacy officer, and the information systems security officer. The team also interviewed VBA personnel including several SSD chiefs; SSD supervisors and personnel; the assistant director of acquisitions; and several program analysts with information security, security categorization, or risk-assessment responsibilities. The review team also interviewed SSD employees to determine whether they were aware of any security flaws, vulnerabilities, or security and privacy issues within MAST such as the collection of PII. The team observed end-user actions, such as entering data and accessing records, to determine if the appropriate access controls were in place to protect the data and evaluate access privileges.

The review team also examined the privacy threshold analysis for MAST to determine if OIT identified and mitigated the risks associated with the system. The team examined system development and implementation plans, risk assessment policy, security planning policy, and other information pertaining to controls used to protect PII collected, processed, and retained by MAST. To determine whether MAST had the appropriate security, privacy, and program management controls, the team reviewed documents uploaded to eMASS and the repository for all documents used to support security and privacy control compliance and compared those documents with NIST and VA requirements.

Internal Controls

The review team assessed the internal controls of VBA and OIT significant to the review objective. This included an assessment of the five internal control components: control environment, risk assessment, control activities, information and communication, and monitoring.[48] In addition, the team reviewed the principles of internal controls associated with the objective. The team identified the following component and principle as significant to the

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

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

- Component 3: Control Activities
    - Principle 12: Management should implement control activities through policies.

The review team identified deficiencies for Component 3: Control Activities. VBA did not follow policies and procedures for the development of MAST and did not establish policies for the use of MAST. These deficiencies are discussed in the report finding and addressed in the recommendations.

Fraud Assessment

The review team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant in the context of the review objectives, could occur during this review. 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 review.

Data Reliability

The OIG did not obtain electronic data that required a data reliability assessment.

Government Standards

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

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

Appendix C: VA Management Comments

Department of Veterans Affairs Memorandum

Date: April 22, 2022

From: Assistant Secretary for Information and Technology and Chief Information Officer (005), Director, Northeast District, Veterans Benefits Administration, Performing the Delegable Duties of the Under Secretary for Benefits (20)

Subj: OIG Draft Report: Mission Accountability Support Tracker Lacked Sufficient Security Controls—Project Number 2021-03080-AE-0148 (VIEWS 07175889)

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

1. The Office of Information and Technology (OIT) and the Veterans Benefits Administration (VBA) are responding to the Office of Inspector General (OIG) Draft Report, Mission Accountability Support Tracker Lacked Sufficient Security Controls.

2. OIT and VBA submit 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	Thomas J. Murphy
Assistant Secretary for Information and Technology and Chief Information Officer	Director, Northeast District, Veterans Benefits Administration, Performing the Delegable Duties of the Under Secretary For Benefits

Attachment

005 Attachment

Office of Information and Technology and Veterans Benefits Administration Comments on Office of Inspector General Draft Report, Mission Accountability Support Tracker Lacked Sufficient Security Controls Project Number 2021-03080-AE-0148 (VIEWS 07175889)

The Office of Information and Technology (OIT) and the Veterans Benefits Administration (VBA) concur with the findings in the Office of Inspector General's (OIG) draft report and provide the following comments in response to the recommendations:

Recommendation #1:

The OIG recommends the Assistant Secretary for Information and Technology develop controls to help ensure minor applications are not misclassified as assets and undergo the appropriate security accreditation and certification process.

Comments: Concur.

In August 2021, OIT's Office of Information Security (OIS) Governance Risk and Compliance (GRC) division directed the Development Security and Operations (DevSecOps) Salesforce Security team to identify and change all Salesforce platform applications previously classified as assets (as of January 2021) as minor applications within the GRC tool, Enterprise Mission Assurance Support System (eMASS).

In November 2021, the Mission Accountability Support Tracker (MAST) completed approval and authorization in eMASS as a minor application, which ensures that all the appropriate security controls are in place as minor applications within the Salesforce platform.

In addition to MAST remediations, OIS has a published Standard Operating Procedure (SOP) for Department-wide use to accurately document security and privacy controls in eMASS. All information systems that have minor applications must follow these procedures.

The Department of Veterans Affairs (VA) requests closure of Recommendation 1. Supporting evidence is provided in the attached SOP.

Recommendation #2:

The OIG recommends the Assistant Secretary for Information and Technology in conjunction with the Under Secretary for Benefits, make certain that appropriate security and privacy controls are implemented during the development of information technology systems before being hosted on VA's network.

Comments: Concur.

The response is limited to the scope of the MAST application on the Salesforce platform and minor applications. Per revised direction provided by OIS GRC, all applications for the Salesforce platform are evaluated and presented to the OIS GRC committee for determination (minor or major application), while DevSecOps security team will ensure and document in eMASS that all required security artifacts are governed and controlled per policy.

With regards to the privacy documentation, in January 2021, DevSecOps Salesforce Security Office received the initial Privacy Threat Analysis (PTA) determination from the Privacy Office that a Privacy

Impact Assessment (PIA) was not required. In July 2021, DevSecOps Salesforce Security Office received an amended PTA stating the PIA was required. In October 2021, the PIA was completed and signed.

In addition to MAST remediations, OIS has a published SOP for use throughout the Department to accurately document security and privacy controls in eMASS. All information systems that have minor applications must follow these procedures.

VA requests closure of Recommendation 2. Supporting evidence is provided in the attached SOP.

Recommendation 3:

The OIG recommends the Under Secretary for Benefits, in conjunction with the Assistant Secretary for Information and Technology, establish a mechanism to gain assurance that proper Office of Information Technology project management processes and protocols are followed when establishing information technology systems and applications.

Comments: Concur in principle.

A mechanism exists by which VBA follows OIT processes and protocols including: the Digital Transformation Center (DTC) SOPs for VA Salesforce platform and VA DTC System Integrator checklist and Policy Handbook Spring 2021 (both attached). VBA also references https://www.oit.va.gov/marketplace/ as well as the VA Information Technology Process Request intake as deemed required. VBA's adherence to and utilization of these resources is confirmed by OIT's DTC and the Salesforce Government Cloud Security team, the Information System Security Officer, System Steward and Information Security Officer and, as such, no additional mechanism is warranted given OIT's assessment of VBA as a customer and partner in full compliance with established procedures.

VA requests closure of Recommendation 3.

Recommendation 4:

The OIG recommends the Under Secretary for Benefits establish policies and procedures to ensure the Mission Accountability Support Tracker is used appropriately and does not contain unnecessary personally identifiable information.

Comments: Concur.

VBA will update the MAST User Guide to include more specific language restricting the inclusion of personally identifiable information in open data fields. In addition, VBA will conduct training for end-users on the changes to the User Guide.

Target Completion Date: September 30, 2022.

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

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Review Team	Al Tate, Director Cynthia Christian Kendrick Levett Sherry Livingston Omar Madrigal Keila Tugwell-Core
Other Contributors	Melissa Bentley Kim Cragg Christopher Dong

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.