VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Veterans Benefits Administration

Review of Alleged Lack of Audit Logs for the Veterans Benefits Management System

April 28, 2016
15-03802-222

ACRONYMS AND ABBREVIATIONS

CSUM	Common Security User Manager
ISO	Information Security Officer
OIG	Office of Inspector General
VA	Department of Veterans Affairs
VARO	VA Regional Office
VBA	Veterans Benefits Administration
VBMS	Veterans Benefits Management System

To Report Suspected Wrongdoing in VA Programs and Operations:

Telephone: 1-800-488-8244

Email: vaoighotline@va.gov

(Hotline Information: www.va.gov/oig/hotline)

Highlights: Review of Alleged Lack of Audit Logs for VBA's VBMS

Why We Did This Audit

In April 2015, the Office of Inspector General (OIG) received an anonymous allegation that the Veterans Benefits Administration (VBA) failed to integrate suitable audit logs into the Veterans Benefits Management System (VBMS).

What We Found

We substantiated the allegation that VBA failed to integrate suitable audit logs that clearly reported all security violations occurring in VBMS. We tested the existence and accuracy of audit logs by having 17 employees at 3 VA Regional Offices (VAROs) attempt to access same-station veteran employee compensation claims in VBMS.

Although audit logs identified security violations for 15 of the 17 employees, the logs did not show that the security violations occurred within VBMS. Instead, the audit logs indicated that the violations occurred in the Share application used by VARO employees or an unknown system. The other two employees did not appear on the audit logs. We could not determine why the two employees did not appear on the audit logs.

This occurred because VBA officials did not develop sufficient system requirements to ensure that audit logs exist and are accessible to Information Security Officers (ISO). As a result, ISOs were unable to effectively detect, report, and respond to security violations occurring within VBMS. Until VBA resolves this issue, its VAROs will be more susceptible to fraudulent compensation claims processing.

What We Recommended

We recommended the Acting Under Secretary for Benefits develop system requirements for integrating audit logs into VBMS. We also recommended the Assistant Secretary for Information and Technology integrate audit logs into VBMS based on the requirements provided by the Acting Under Secretary for Benefits. Finally, we recommended the Acting Under Secretary for Benefits test the audit logs to ensure the logs capture all potential security violations.

Agency Comments

The Acting Under Secretary for Benefits and the Assistant Secretary for Information and Technology concurred with our recommendations and provided acceptable corrective action plans. We will monitor their implementation. The Acting Under Secretary also provided technical comments, which we took into consideration.

Gary K Abe

GARY K. ABE
Acting Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

Results and Recommendations 1

Finding VBA Did Not Integrate Audit Logs Into the Veterans Benefits Management System...1

Recommendations...3

Appendix A Scope and Methodology 5

Appendix B Management Comments – Under Secretary for Benefits 6

Appendix C Management Comments – Assistant Secretary for Information and Technology 9

Appendix D Contact and Staff Acknowledgments..11

Appendix E Report Distribution 12

RESULTS AND RECOMMENDATIONS

Finding VBA Did Not Integrate Audit Logs Into the Veterans Benefits Management System

In April 2015, the Office of Inspector General received an anonymous allegation that the Veterans Benefits Administration (VBA) failed to integrate suitable audit logs into the Veterans Benefits Management System (VBMS). Audit logs allow Information Security Officers (ISOs) to review, audit, and intervene in potential security violations. The complainant asserted that this functionality existed in other legacy claims processing systems.

Background

In 2013, VBA developed a Transformation Plan designed to eliminate a compensation claims backlog. The transformation will use VBMS to end VBA's reliance on the outmoded paper-intensive processes that hinder timely claims processing. VBMS is an information technology system designed to help claims adjudicators reach timely and informed decisions. VBMS is a technology solution designed to help eliminate the existing claims backlog by providing a technology platform for quicker and more accurate claims processing.[1]

Criteria

The Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, establishes organizational requirements for creating, protecting, and retaining audit records for monitoring, analyzing, investigating, and reporting unlawful, unauthorized, or inappropriate information system activity. In addition, organizations must also be able to identify the actions of individual system users so they can hold the users accountable for their actions. VA Handbook 6500 (*Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*) states that information systems must generate detailed audit logs to facilitate reconstruction of events if a system has been compromised.

What We Did

To address this allegation, we reviewed Federal and VA information security criteria related to the implementation and use of audit logs in information systems. We tested the existence, accuracy, and usefulness of audit logs by observing 17 VA Regional Office (VARO) employees attempt to improperly access same-station veteran employee compensation claims in VBMS.

[1] *Department of Veterans Affairs (VA) Strategic Plan to Eliminate the Compensation Claims Backlog*, dated January 25, 2013.

We observed the employees perform this test in the following VBMS modules:

- Core (VBMS-Core)
- Rating (VBMS Rating)
- Award (VBMS Award)

Because VBMS is in a production environment, we did not instruct VARO employees to modify or change any part of a claim they were able to access. Subsequent to the employees attempting to access VBMS, we asked the on-site ISOs to retrieve the available audit logs, which came from the Common Security User Manager (CSUM) system. We then evaluated the audit logs to determine whether the security violations from our tests appeared in the logs and whether the information was clear and useable for the ISOs. We did not identify any fraudulently processed claims because we did not evaluate actual claims processing transactions to test for fraudulent activity as part of our review.

What We Found

We substantiated the allegation that VBA did not integrate suitable audit logs into VBMS. The audit logs available to ISOs after our testing did not show that the security violations occurred within VBMS. The audit logs identified security violations for 15 of the 17 employees who accessed same-station veteran employee claims through VBMS. However, the audit logs indicated that the violations occurred in Share[2] or an unknown system. The other two employees did not appear on the audit logs. We could not determine why the two employees did not appear on the audit logs. Subsequent to our review, VBA's Office of Business Process Integration also found the same deficiency through their tests of the audit logs and concurred that the audit logs did not provide meaningful information to ISOs.

Why This Occurred

Officials in the Office of Business Process Integration told us that they did not develop requirements to ensure that audit logs would identify security violations occurring in VBMS. Since VBMS uses CSUM, they assumed that the same audit log capability and functionality available for legacy claims processing systems would have automatically existed for VBMS. As such, the Office of Business Process Integration never developed appropriate requirements to ensure that audit logs accurately identify security violations that occur in VBMS.

What Resulted

ISOs were unable to effectively detect, report, and respond to security violations occurring within VBMS. Consequently, VAROs will be at an increased risk of not being able to detect an employee who inappropriately

[2] Share is an application used by VARO employees to access multiple data sources needed to process veterans' claims.

processes a coworker's claim or even his or her own claim until VBA resolves this issue.

Recommendations

1. We recommended the Acting Under Secretary for Benefits develop and provide the Office of Information and Technology with system requirements for integrating audit logs containing the data security officers need to intervene in potential security violations into the Veterans Benefits Management System.

2. We recommended the Assistant Secretary for Information and Technology integrate audit logs into the Veterans Benefits Management System based on the requirements provided by the Acting Under Secretary for Benefits.

3. We recommended the Acting Under Secretary for Benefits test the newly integrated audit logs to ensure that the logs capture all potential security violations.

Management Comments

The Acting Under Secretary for Benefits and the Assistant Secretary for Information and Technology concurred with our recommendations and provided acceptable corrective action plans. The Acting Under Secretary for Benefits also provided technical comments, which we took into consideration.

VBA stated that the functionality of the Veterans Services Network currently in production, including audit logs, should have been maintained, with VBMS application information passed to the legacy audit-log services. Thus, the OIG report incorrectly stated that the Office of Business Process Integration did not provide requirements for audit logs because there were no new requirements to submit.

VBA also stated that the scenario we used to validate criteria was narrow and created a false impression of VBA information security weaknesses because any actions actually taken by a user would be separately logged into the VBA Corporate Database. VBA asserted that the sensitive access report reviewed by the audit team was designed only to address a small subset of all audit logging scenarios and security controls for VBA systems.

Lastly, VBA asserted that the information provided by the audit team regarding this complaint is insufficient to enable VBA to independently reproduce our contention that two employees who attempted to access sensitive records did not appear on the audit logs. VBA would need more detailed information such as screenshots and detailed test scripts describing each user action, as well as the configuration of either the user or sensitive record.

OIG Response

We consider the corrective actions acceptable and we will monitor their implementation. However, we disagree with VBA management's assertions regarding our audit report.

Our review determined that the functionality of providing suitable audit logs for ISOs to review was not maintained even though it was maintained for other legacy systems. Moreover, VBA stated it would develop requirements to clarify how VBMS data should be represented in the audit log reports. Thus, we continue to maintain that VBA did not develop appropriate requirements to ensure that audit logs accurately identified security violations occurring in VBMS for ISOs to review.

We also disagree with management's assertion that we created a false impression of VBA information security weaknesses. The Hotline allegation revolved around whether VBMS provided suitable audit logs to ISOs that would allow the ISOs to effectively detect, report, and respond to potential security violations occurring within VBMS. Our review substantiated the allegation that the audit logs provided to ISOs did not meet their needs and the ISOs agreed with our observations.

Finally, we take exception with management's assertion that we did not provide sufficient information to enable VBA to independently reproduce our conclusion that two employees who attempted to access sensitive records did not appear on the audit logs. Our tests identified two employees who did not appear on the audit logs after they attempted to access same-station veteran employee compensation claims in VBMS. However, it goes beyond the scope of our review for us to capture such items as detailed test scripts describing each user action, as well as the configuration of both the user and the record being reviewed. Moreover, it does not change the fact that two employees who attempted to access sensitive records did not appear on the audit logs.

Appendix A Scope and Methodology

We conducted our review from June through December 2015. We performed site visits and testing procedures at three VAROs:

- VARO Houston, TX
- VARO Waco, TX
- VARO Seattle, WA

We tested the existence and accuracy of audit logs by having 17 VARO employees attempt to access same-station veteran employee compensation claims in VBMS.

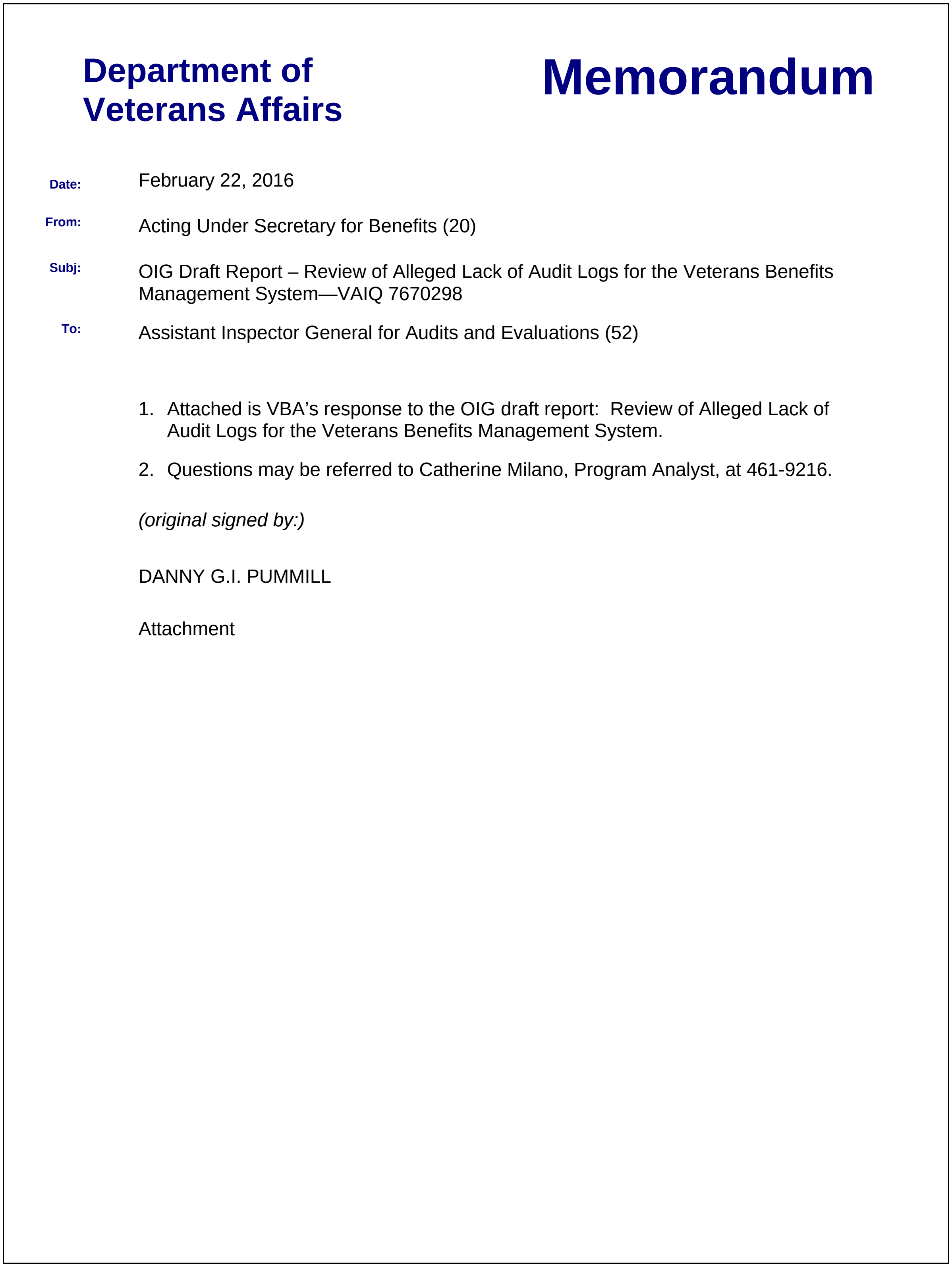
Data Reliability

We obtained electronic audit logs from on-site ISOs. We compared the information in the audit logs to the VBMS security violations we observed to determine whether the audit logs accurately reported the violations. We concluded that the data were not sufficiently reliable for information security officers to take actions to review, audit, and intervene in potential security violations. As a result, we made recommendations to integrate suitable audit logs into VBMS.

Government Standards

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Appendix B Management Comments – Under Secretary for Benefits



Department of Veterans Affairs

Memorandum

Date: February 22, 2016

From: Acting Under Secretary for Benefits (20)

Subj: OIG Draft Report – Review of Alleged Lack of Audit Logs for the Veterans Benefits Management System—VAIQ 7670298

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

1. Attached is VBA's response to the OIG draft report: Review of Alleged Lack of Audit Logs for the Veterans Benefits Management System.
2. Questions may be referred to Catherine Milano, Program Analyst, at 461-9216.

(original signed by:)

DANNY G.I. PUMMILL

Attachment

Attachment

Veterans Benefits Administration (VBA)
Comments on OIG Draft Report

Review of Alleged Lack of Audit Logs for the
Veterans Benefits Management System

VBA provides the following comments:

VBA information systems supporting compensation, pension, and vocational rehabilitation and employment benefits capture two fundamental types of audit data: 1) logging of inquiries and actions performed on records VBA considers to be sensitive, and 2) logging of actions creating or updating any records. Each of these logs serves separate purposes.

The requirement to create audit logs is not a new requirement for VBMS, as VBMS is built on the VETSNET services already in production. VBMS is a web application connecting to our corporate database through the use of shared web-logic services, wrapped on top of legacy tuxedo services developed as part of the VETSNET project. As such, the functionality of the VETSNET services currently in production, including audit logs, should have been maintained, with VBMS application information passed to the legacy audit-log services. The OIG report incorrectly states that the Office of Business Process Integration (OBPI) did not provide requirements for audit logs; however, there were no new requirements to submit.

VBA systems log inquiries and actions performed on records VBA considers to be sensitive to ensure the private information of employees, employee relatives, and Veterans in the public eye (politicians, Veterans involved in legal altercations, celebrities, etc.) is only accessed by a subset of all VBA employees. These logs also maintain a record of these accesses so they can be analyzed to ensure users who accessed those records have a legitimate business need to do so. The logs are reviewed and monitored by the Office of Information and Technology (OIT) Information Security Officers (ISOs) at local regional offices (ROs) to ensure adherence of local users to the VA Rules of Behavior, VA Handbook 6500, and supplemental VBA security policies (including sensitivity). Separate from these logs, VBA systems also have access and functional controls to prevent employees from colluding on the claims of other employees and to ensure separation of duties between staff involved in approving monetary awards and payment of benefits.

VBA systems also log all actions creating or updating records in the VBA Corporate Database to allow VBA to reconstruct events if VBA systems are compromised and to maintain an audit trail identifying the users and applications involved in an action on a particular record. These include critical actions such as establishment of a claim, disability ratings, generation and authorization of monetary awards, and payments. The logs do not, however, contain logs of inquiries. These logs are maintained in the VBA Corporate Database as journal tables and are regularly used by VBA and OIT staff to investigate defects and system operations. They are also provided daily to Office of Inspector General (OIG) criminal investigators through database snapshots for use in their investigations.

The scenario OIG used to validate its criteria (broadly stated as compliance with information security standards) was narrow and creates a false impression of VBA information security weaknesses. As described above, the sensitive access report reviewed by OIG is only designed to address a small subset of all audit logging scenarios and security controls for VBA systems. From an overall information security context, its utility is in tracking user accesses, where a user was denied access by appropriate system controls or where a user was able to access a sensitive record and that access was logged so it could be reviewed at a later date for business need. Any actions actually taken by a user (as opposed to inquiries), a malicious actor, or another system on the record, would be separately logged in the VBA Corporate Database.

The information provided by OIG regarding this Hotline complaint is insufficient to enable VBA to independently reproduce OIG's contention that the two employees who attempted to access sensitive records did not appear on the audit logs. To correct or confirm such an issue, VBA would need to reproduce it, which would require information such as screenshots, detailed test scripts describing each user action, as well as the configuration of both the user and the record being reviewed. Variation on any of these items (which could occur due to user error or configuration of either the user or sensitive record) could have caused the audit logs to not successfully record a security violation. VBA would welcome additional specific information in order to test and assess the accuracy of the complaint. If OIG does not have additional specific information, VBA, in coordination with OIG, is willing to create and jointly execute a more rigorous test regimen where the specific information OIG failed to capture is collected and can be used to address system issues found.

VBA acknowledges that errors in the attributional information for the specific application, in which a sensitive violation inquiry occurred could be confusing to an ISO. This attributional information is useful when investigating a violation, but not essential to confirm a violation occurred and identify who was responsible. As is indicated in the response to recommendation 1 that follows, VBA will perform assessments in coordination with OIT to identify all areas where VBMS data provided on existing audit reports used by ISOs is not clearly attributable to the VBMS application. Requirements will be provided to clarify how VBMS data should be represented on the reports.

The following comments are submitted in response to the recommendations in the OIG draft report:

Recommendation 1: We recommended the Acting Under Secretary for Benefits develop and provide the Office of Information and Technology with system requirements for integrating audit logs containing the data security officers need to intervene in potential security violations into the Veterans Benefits Management System.

VBA Response: Concur in principle. VBA provided the business requirements for logging the information required as part of our development of the VETSNET system and communicated the need to maintain core backend functionality as part of the Veterans Benefits Management System (VBMS) development. Technical design and systems requirements are developed and implemented by OIT.

While the fundamental effectiveness of VBA's systems controls are in place, VBA will work with OIT to identify all areas where VBMS data provided on existing audit reports used by ISOs is not clearly attributable to the VBMS application and develop requirements to clarify how VBMS data should be represented on the reports. VBA anticipates completion of testing and a submission of its findings and requirements to OIT by July 31, 2016.

Target Completion Date: July 31, 2016

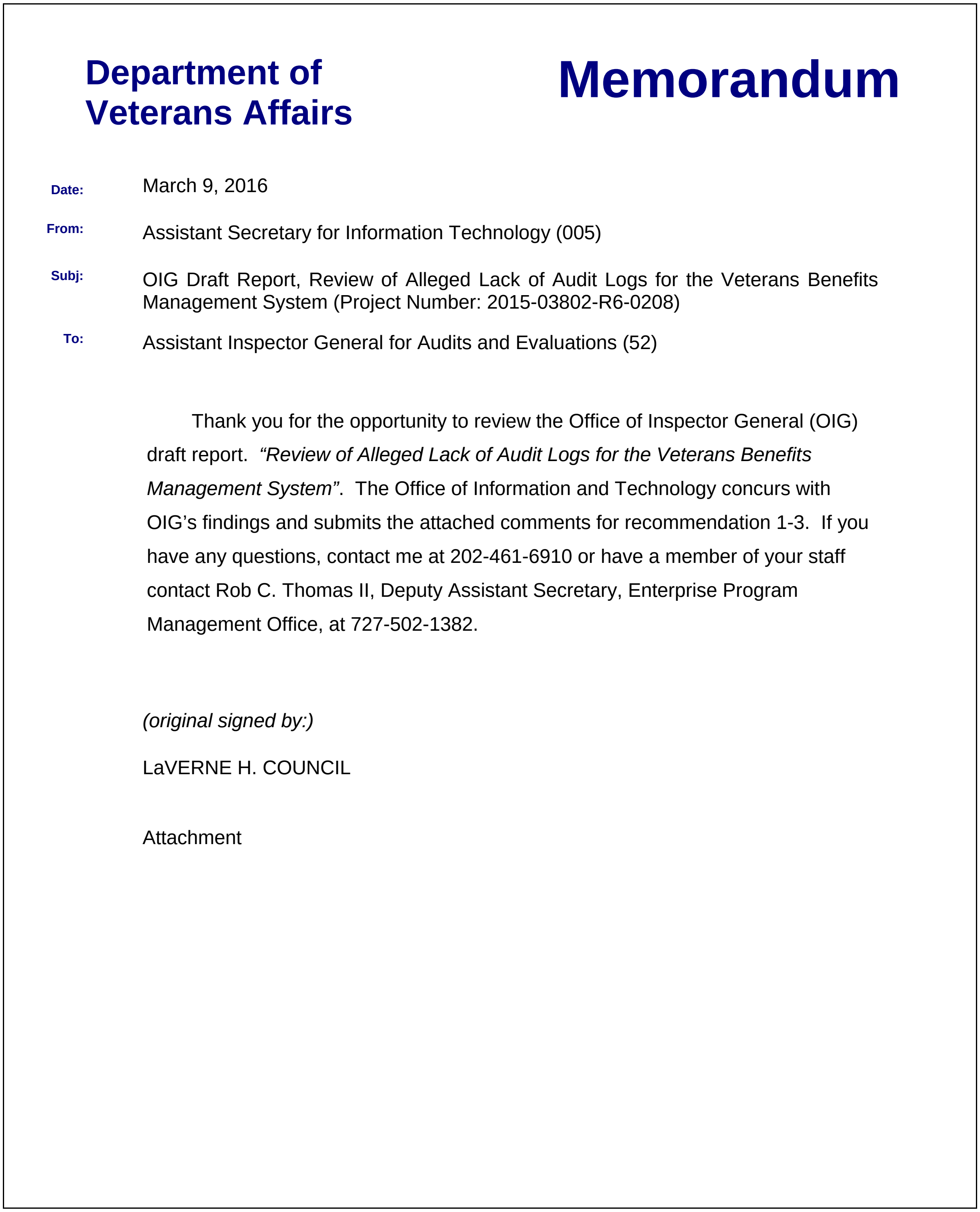
Recommendation 2: We recommended the Assistant Secretary for Information and Technology integrate audit logs into the Veterans Benefits Management System based on the requirements provided by the Acting Under Secretary for Benefits.

VBA Response: VBA defers to the Office of Information and Technology.

Recommendation 3: We recommended the Acting Under Secretary for Benefits test the newly integrated audit logs to ensure that the logs capture all potential security violations.

VBA Response: Concur. VBA will test any changes to security logs to ensure they better reflect attribution of the VBA business application used that resulted in a security violation. Subsequent to release of the enhanced functionality, VBA will also monitor the logs in coordination with ISOs to ensure no additional issues are identified after deployment. VBA anticipates completion of post-deployment audit log testing and monitoring within three months of deployment.

Appendix C Management Comments – Assistant Secretary for Information and Technology



Department of Veterans Affairs

Memorandum

Date: March 9, 2016

From: Assistant Secretary for Information Technology (005)

Subj: OIG Draft Report, Review of Alleged Lack of Audit Logs for the Veterans Benefits Management System (Project Number: 2015-03802-R6-0208)

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

Thank you for the opportunity to review the Office of Inspector General (OIG) draft report. *"Review of Alleged Lack of Audit Logs for the Veterans Benefits Management System"*. The Office of Information and Technology concurs with OIG's findings and submits the attached comments for recommendation 1-3. If you have any questions, contact me at 202-461-6910 or have a member of your staff contact Rob C. Thomas II, Deputy Assistant Secretary, Enterprise Program Management Office, at 727-502-1382.

(original signed by:)

LaVERNE H. COUNCIL

Attachment

005 Attachment

Office of Information and Technology
Comments on OIG Report,
Review of Alleged Lack of Audit Logs for the Veterans Benefits Management System

OIG Recommendation 1: We recommended the Acting Under Secretary for Benefits develop and provide the Office of Information and Technology with system requirements for integrating audit logs containing the data security officers need to intervene in potential security violations into the Veterans Benefits Management System.

> **Comments**: OI&T defers to the Veterans Benefits Administration as the owner of this recommendation.

OIG Recommendation 2: We recommended the Assistant Secretary for Information and Technology integrate audit logs into the Veterans Benefits Management System based on the requirements provided by the Acting Under Secretary for Benefits.

> **Comments:** Concur. OI&T will assist VBA, and other users as necessary, to conduct regression tests with VBMS users to determine when sensitivity checks are not performed and/or user actions are not correctly recorded in the audit logs. The regression tests will produce business requirements to address auditing needs. VBA will prioritize these business requirements for inclusion in a future VBMS release. Once the requirements are added to the scope of a release, VBMS OI&T will work with the Benefits Gateway Services (BGS) to implement the business requirements by making changes to either the VBMS application of the BGS web services. VBA will submit the requirements to OI&T on July 31, 2016, and the next available VBMS release will be December 31, 2016, which will include the integration of audit logs.

OIG Recommendation 3: We recommended the Acting Under Secretary for Benefits test the newly integrated audit logs to ensure that the logs capture all potential security violations.

> **Comments**: OI&T defers to the Veterans Benefits Administration as the owner of this recommendation.

Appendix D Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Mario M. Carbone, Director Jehri Lawson Sean Lupton Larrynnee Pierre

Appendix E Report Distribution

VA Distribution

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

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government 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

This report is available on our Web site at www.va.gov/oig.