Department of Veterans Affairs

*Review of
Alleged Lack of Access
Controls for the Project
Management
Accountability System
Dashboard*

ACRONYMS

FY	Fiscal Year
IT	Information Technology
OIG	Office of Inspector General
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
PBO	Project Management Accountability System (PMAS) Business Office
PMAS	Project Management Accountability System
VA	Department of Veterans Affairs

Highlights: Review of Alleged Lack of Access Controls for VA's PMAS Dashboard

Why We Did This Review

The Office of Inspector General received an allegation that the Office of Information and Technology (OI&T) had ineffective access controls over the Project Management Accountability System (PMAS) Dashboard and related project management data and metric reporting information.

What We Found

We substantiated the allegation that PMAS Dashboard access controls were inadequate. OI&T did not configure 17 of the 18 PMAS Dashboard access groups to provide the least needed access privileges even though VA policy required OI&T grant access to VA systems based on the least need (the practice of limiting access to the minimal level that will allow normal performance of duties).

Instead, OI&T designed these 17 groups to have full user access privileges to the PMAS Dashboard data, regardless of individual user need. This occurred because the OI&T director concluded that the PMAS data were not at risk; thus, OI&T should not spend limited funds to develop group access ranging from read only to full access. When requested, OI&T staff could not provide a cost analysis identifying the costs to develop access controls.

In addition, OI&T did not develop user access logs. This prevented OI&T from identifying active users and periodically validating their actions. Thus, OI&T could not effectively manage its risk to data integrity. Without configuring all the PMAS Dashboard groups to restrict user access to the data, VA does not comply with Federal Information Technology security requirements and VA Handbook 6500, and has assumed unnecessary risks to the integrity of its project management data.

What We Recommended

We recommended the Assistant Secretary for Information and Technology create read-only access to PMAS and ensure each user's access is based on the least needed privilege. We also recommended that the Assistant Secretary develop Dashboard access logs and periodically review all users' access to ensure users still have legitimate needs for system access.

Agency Comments

The Assistant Secretary for Information and Technology concurred with our recommendations and provided acceptable corrective action plans. We will monitor their implementation.

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

TABLE OF CONTENTS

RESULTS AND RECOMMENDATIONS

Finding

Project Management Accountability System Dashboard Access Controls Are Inadequate

The Office of Inspector General (OIG) received an anonymous allegation that the Office of Information and Technology (OI&T) had ineffective access controls over the Project Management Accountability System (PMAS) Dashboard and related project management data and metric reporting information.

What We Found

We substantiated the allegation that PMAS Dashboard access controls were inadequate. OI&T did not configure 17 of the 18 PMAS Dashboard access groups to provide the least needed access privileges even though VA policy required OI&T grant access based on the least need (the practice of limiting access to the minimal level that will allow normal performance of duties). Instead, OI&T designed these 17 groups to have full user access privileges to the PMAS dashboard data, regardless of need. This occurred because OI&T thought it would be too costly to develop group access ranging from read-only to full access. Full access would allow users to read, write, modify, and delete data. Without configuring all the PMAS Dashboard access groups to the least needed privilege, VA has assumed unnecessary risks to the integrity of its project management data.

PMAS is an information technology (IT) system that is required to comply with VA Handbook 6500, *Information Security*. The Handbook states VA IT system access should be granted to users based on the least need in order to protect the data in the system and ensure it is not vulnerable to improper modification, disclosure, or destruction. Access privileges must range from read-only to full access depending on the individual needs of the user. Implementing a range of effective access controls would enable OI&T to grant system access to users based on the least need, thereby protecting the PMAS data.

At the time OI&T developed the PMAS Dashboard, the PMAS Business Office (PBO) decided to manage PMAS Dashboard security via Windows domain groups, which control a user's access to the Dashboard. When users need access to specific areas of the PMAS Dashboard, the system administrator adds them to the appropriate group, thereby granting access to an area or feature. Once an individual is granted access to a particular group, he or she has all the rights of that group.

The Business Intelligence Reports group is the only group where users have read-only access to view and print pre-defined reports. Users in this group, such as analysts and senior officials use these reports to help them make informed management decisions. However, if the system administrator

granted any of these same users access to any of the other 17 access groups, they could modify the data that populate the pre-defined reports.

For example, 24 users are members of 2 groups, the Business Intelligence Reports and the Manage Investment group.[1] These 24 users, regardless of their read-only access in the Business Intelligence Reports group, had the ability to manipulate cost and schedule data in the Manage Investment group, potentially altering VA's performance metrics, which are reported on the Office of Management and Budget's (OMB) Federal IT Dashboard. Congress and VA use the performance metrics to make budget-related decisions.

Reason PMAS Dashboard Groups Improperly Configured

OI&T did not see a need to restrict user access privileges except when a user needs to view or print pre-defined reports. The PBO director disclosed that she made the decision because of budget constraints. She stated that it never occurred to her that anyone would want to do anything malicious to the data and was not aware of any malicious activity. She also did not anticipate any interest in the PMAS data, or that anyone would want to verify the data, because she thought the data were for internal use only. The director concluded that the PMAS data were not at risk of being compromised and the PBO should not spend limited financial resources on developing the required read-only access. We requested the costs to develop access controls. However, PBO officials stated they could not separately identify those costs.

The PBO director's decision to limit implementation of the read-only requirement to only the Business Intelligence Reports group and not the other 17 groups created an unmitigated risk to data integrity. In addition, OI&T did not develop user access logs. This prevented OI&T from identifying active users and periodically validating their actions. Thus, OI&T could not effectively manage the risk to data integrity.

OIG previously reported that VA had not implemented the controls needed to monitor system access logs periodically. In our May 2015 Federal Information Security Management Act audit report, we recommended VA enable system audit logs.[2] Without access logs, OI&T cannot adequately monitor users to ensure they have a continued need for PMAS Dashboard access group memberships. In accordance with VA policy, systems must have read-only privileges and system access logs that are reviewed periodically.

---

[1] The Management Investment group users are granted full access to all data contained within that group.
[2] *Federal Information Security Management Act Audit for Fiscal Year 2014*, Report No. 14-01820-355, May 19, 2015.

Conclusion

Access controls are necessary to protect Government information and ensure those systems are not vulnerable to improper data modification, disclosure, or destruction. OI&T officials acknowledged that they chose not to implement read-only access privileges during PMAS Dashboard development with the exception of the Business Intelligence Reports group. Consequently, the PMAS data remained at risk for manipulation. Thus, VA does not comply with Federal IT security requirements and VA Handbook 6500 and has assumed unnecessary risks to the integrity of its project management data.

Recommendations

1. We recommended the Assistant Secretary for Information and Technology create read-only access capability for the Project Management Accountability System.

2. We recommended the Assistant Secretary for Information and Technology assess the current level of each user's access to the Project Management Accountability System Dashboard to ensure each user's access is based on the least privilege needed.

3. We recommended the Assistant Secretary for Information and Technology develop Project Management Accountability System Dashboard access logs.

4. We recommended the Assistant Secretary for Information and Technology periodically review Project Management Accountability System Dashboard access logs to ensure users have a need for system access.

Management Comments

The Assistant Secretary for Information and Technology concurred with our recommendations and provided acceptable corrective action plans. A new dashboard is currently being developed that will store data related to OI&T's new planning, development, and release process. Implementation of recommendations will be included as part of the mandatory requirements for the Veteran-focused Integrated Process Dashboard and the initial estimate target completion date is December 2016.

OIG Response

We consider the corrective actions acceptable and we will monitor their implementation.

Appendix A   Background, Scope, and Methodology

PMAS Dashboard Overview

The PMAS Dashboard IT project was under the purview of PMAS—a performance-based project management discipline intended to improve the rate of success of VA's IT projects. OI&T began developing the PMAS Dashboard in FY 2010 and completed development in FY 2014 at a total cost of approximately $13.5 million, including the costs of the existing access controls. PBO officials could not separately identify the access control costs.

A VA Organizational Tool

VA management uses the PMAS Dashboard as an organizational tool to assist in the governance process ensuring that VA's IT investments achieve:

- Their intended outcomes on time and within budget, meet veterans' needs, and support VA's mission and business objectives

- Appropriate security and privacy protections

- Conformance to legislative mandates and OMB requirements for IT investment management

OI&T uses the PMAS Dashboard to track and report the status of PMAS-managed projects, automate recurring report generation capabilities, centrally store PMAS-related artifacts, and provide automated input for external systems, such as the OMB Federal IT Dashboard.

Scope and Methodology

We reviewed 18 PMAS Dashboard access groups and select users within those groups. To accomplish our review, we:

- Interviewed the PBO director, and the PMAS system administrator to obtain an understanding of how OI&T granted access to the PMAS Dashboard

- Observed a demonstration of the PMAS Dashboard features to include the data users can obtain from the Dashboard and OI&T's process to grant user access to the Dashboard access groups

- Analyzed a current list of PMAS Dashboard access groups to determine completeness and consistency with the PMAS PBO's cited business rules

- Reviewed Federal law and VA policy and guidance related to IT access controls

- Determined whether OI&T used access logs to validate the adequacy of user access and ensure adequate PMAS Dashboard oversight

Data Reliability

We analyzed the access list provided by the PBO and found the initial list to be incomplete because it did not identify users the audit team knew had access to PMAS data. When we questioned the completeness of the list, the PBO simply provided an updated list without explaining the discrepancy

even after we asked. As a result, we limited our findings and conclusions to the users whom we could verify and reported the results accordingly. Thus, we determined the list was sufficiently reliable for the purposes of our findings and conclusions. We did not verify that every user's access was appropriate or evaluate the reliability of PMAS data.[3]

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*.

---

[3] We previously reported that OI&T needs to establish controls for ensuring data reliability in the PMAS Dashboard. *Audit of the Project Management Accountability System Implementation*, Report No. 10-03162-262, August 29, 2011, and *Follow-Up Audit of the Information Technology Project Management Accountability System*, Report No. 13-03324-85, January 22, 2015.

Appendix B   Management Comments

**Department of
Veterans Affairs**   **Memorandum**

Date: April 6, 2016

From: Assistant Secretary for Information and Technology (005)

Subj: OIG Draft Report, Review of Alleged Lack of Access Controls for the Project
Management Accountability System Dashboard (Project No. 2015-02459-R6-0130)

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 Access Controls for the Project Management
Accountability System Dashboard".* The Office of Information and Technology concurs
with the OIG's findings and submits the attached comments for recommendations 1-4.
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

<div style="border:1px solid black; padding:10px;">

**Office of Information and Technology
Comments on OIG Draft Report,**

*Review of Alleged Lack of Access Controls for the Project Management Accountability
System Dashboard (Project Number: 2015-02459-R6-0130)*

</div>

<u>**OIG Recommendation 1:**</u> **We recommended the Assistant Secretary for Information and Technology create read-only access capability for the Project Management Accountability System.**

Comments: Concur. The Office of Information and Technology (OI&T) is undergoing a major transformation of its product planning, development, and release processes to more effectively serve customers and Veterans. As part of this transformation, OI&T will phase out use of the PMAS Dashboard over the next several months.

A new dashboard is currently being developed that will store data related to OI&T's new planning, development and release process. This new dashboard will be called the Veteran-focused Integrated Process (VIP) Dashboard.

OIG Recommendation 1 to create read-only access capability will be included as part of the mandatory requirements for the VIP Dashboard and implemented in that system. The VIP Dashboard will replace the PMAS Dashboard. Development of the VIP Dashboard has just begun; VA's initial estimate for a target completion date is December 2016.

<u>**OIG Recommendation 2:**</u> **We recommended the Assistant Secretary for Information and Technology assess the current level of each user's access to the Project Management Accountability System Dashboard to ensure each user's access is based on the least privilege needed.**

Comments: Concur. The Office of Information and Technology (OI&T) is undergoing a major transformation of its product planning, development, and release processes to more effectively serve customers and Veterans. As part of this transformation, OI&T will phase out use of the PMAS Dashboard over the next several months.

A new dashboard is currently being developed that will store data related to OI&T's new planning, development and release process. This new dashboard will be called the Veteran-focused Integrated Process (VIP) Dashboard.

OIG Recommendation 2 to assess each user's access to ensure it is based on least privilege needed will be included as part of the mandatory requirements for the VIP Dashboard and implemented in that system. The VIP Dashboard will replace the PMAS Dashboard. Development of the VIP Dashboard has just begun; VA's initial estimate for a target completion date is December 2016.

<u>**OIG Recommendation 3:**</u> **We recommended the Assistant Secretary for Information and Technology develop Project Management Accountability System Dashboard access logs.**

Comments: Concur. The Office of Information and Technology (OI&T) is undergoing a major transformation of its product planning, development, and release processes to more effectively serve customers and Veterans. As part of this transformation, OI&T will phase out use of the PMAS Dashboard over the next several months.

A new dashboard is currently being developed that will store data related to OI&T's new planning, development and release process. This new dashboard will be called the Veteran-focused Integrated Process (VIP) Dashboard.

OIG Recommendation 3 to develop dashboard access logs will be included as part of the mandatory requirements for the VIP Dashboard and implemented in that system. The VIP Dashboard will replace the PMAS Dashboard. Development of the VIP Dashboard has just begun; VA's initial estimate for a target completion date is December 2016.

OIG Recommendation 4: We recommended the Assistant Secretary for Information and Technology periodically review Project Management Accountability System Dashboard access logs to ensure users have a need for system access.

Comments: Concur. The Office of Information and Technology (OI&T) is undergoing a major transformation of its product planning, development, and release processes to more effectively serve customers and Veterans. As part of this transformation, OI&T will phase out use of the PMAS Dashboard over the next several months.

A new dashboard is currently being developed that will store data related to OI&T's new planning, development and release process. This new dashboard will be called the Veteran-focused Integrated Process (VIP) Dashboard.

OIG Recommendation 4 to periodically review access logs to ensure users have a need for system access will be included as part of the mandatory requirements for the VIP Dashboard and implemented in that system. The VIP Dashboard will replace the PMAS Dashboard. An independent group within OI&T's Enterprise Program Management Office (EPMO) will review access logs semi-annually and provide recommendations to the VIP Business Office (VBO) for implementation. Development of the VIP Dashboard has just begun; VA's initial estimate for a target completion date is December 2016.

Appendix C OIG Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Mario Carbone, Director Sherry Fincher Heather Jones Brenda Stepps

Appendix D   Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel

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.