VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Mismanagement of the Systems to Drive Performance Project

February 13, 2012
11-02467-87

ACRONYMS AND ABBREVIATIONS

DSS	Decision Support System
OIG	Office of Inspector General
OIT	Office of Information Technology
STDP	Systems to Drive Performance
VHA	Veterans Health Administration

Report Highlights: Review of Alleged Mismanagement of the Systems to Drive Performance Project

Why We Did This Review

VA is implementing the Systems to Drive Performance (STDP) dashboard capability to track cost accounting data that will facilitate senior leadership decision making. We evaluated the merits of allegations that VA did not use an appropriate contract vehicle to develop and implement the STDP, ensure system testing met contract and program requirements, adequately protect sensitive VA information from unauthorized access and disclosure, and ensure STDP applications provide capabilities that are not redundant with existing VA systems.

What We Found

We did not substantiate the allegations regarding an inappropriate STDP contract vehicle, inadequate system testing, and system redundancy. However, we substantiated the remaining allegation that VA did not adequately protect sensitive information from unauthorized access and disclosure. Specifically, we determined that more than 20 system users had inappropriate access to sensitive STDP information. VA's National Data Systems Group did not consistently approve requests for user access to STDP. Further, project managers did not report unauthorized access as a security event, as required by VA policy.

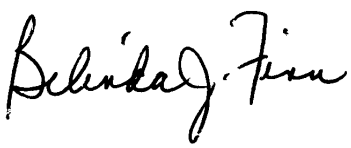
STDP project managers were not fully aware of VA's security requirements for system development and had not formalized user account management procedures. Inadequate Information Security Officer oversight contributed to weaknesses in user account management and failure to report excessive user privileges as security violations. As a result, VA lacked assurance of adequate control and protection of sensitive STDP data.

What We Recommend

We recommend the Assistant Secretary for Information Technology and the Assistant Secretary for Management ensure project managers receive training on project-related information security requirements. The Assistant Secretary for Information Technology should assign Information Security Officers throughout the project to oversee software development efforts. Further, the Assistant Secretary for Management should implement controls to ensure user account management procedures align with established VA policy.

Agency Comments

The Principal Deputy Assistant Secretary for Information Technology and the Assistant Secretary for Management agreed with our findings and recommendations. The OIG will monitor implementation of the corrective action plans.



BELINDA J. FINN
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

We evaluated the merits of an April 2011 VA Office of Inspector General (OIG) Hotline complaint that the Office of Management did not effectively manage the Systems to Drive Performance (STDP) project.

Background

The STPD project aims to provide VA management with "real-time" information to facilitate decisions related to budgets and performance, and to achieve greater value from the allocation of VA resources. The use of STDP financial "dashboards" will make identification of data anomalies easier and allow faster manipulation of data to produce custom reports based on trends or concerns. STDP will consolidate VA patient and financial information from various data sources and display financial cost and accounting data in a graphical format. STDP supports the Office of Management and Budget's Enterprise Wide Cost and Accountability initiative for improved Federal cost management and is one of the VA Secretary's 16 major initiatives for 2011.

The Assistant Secretary for Management is the business owner of the STDP project. The STDP software development group consists of staff members from the Office of Management, the Office of Information Technology (OIT), and the contractor. The development group uses an "Incremental" or "Agile" development approach to develop, test, and implement major software releases. VA expects the Program Management Accountability System to provide near-term visibility for the project and help avoid long-term project failure. Under the Program Management Accountability System, software development projects must incrementally deliver smaller and more frequent releases of system functionality.

Allegation

In April 2011, an anonymous complainant alleged that VA was not appropriately managing the STDP project. Specifically, the complainant alleged that VA did not use an appropriate contract vehicle to procure STDP software development services, ensure STDP testing met contract and program requirements, adequately protect sensitive VA information from unauthorized access and disclosure, and ensure STDP applications provided unique capabilities that were not redundant with existing VA systems.

To determine the merits of the Hotline allegation, we visited offices associated with the STDP project and interviewed project management officials and representatives from OIT and the Office of Management. Appendix A provides details on the scope and methodology for our review. Appendix B provides additional background information pertinent to our review. Appendixes C and D provide comments by the Assistant Secretaries for Management and OIT on a draft of this report.

RESULTS

Finding Inadequate Protection of Sensitive Data

We did not substantiate the allegations regarding an inappropriate STDP contract vehicle, inadequate system testing, and system redundancy. However, we substantiated the remaining allegation that VA did not adequately protect sensitive VA information from unauthorized access and disclosure. Specifically, we determined that more than 20 system users had inappropriate access to sensitive STDP information. VA's National Data Systems Group did not consistently approve requests for user access. Further, project managers did not report unauthorized access as a security event, as required by VA policy.

STDP project managers were not fully aware of VA's security requirements for system development and had not formalized user account management procedures. Inadequate Information Security Officer oversight contributed to weaknesses in user account management and the failure to report the granting of excessive user rights as security violations. As a result, VA lacked assurance of adequate control and protection of sensitive STDP data.

Unsubstantiated Allegations

We did not substantiate the allegations regarding an inappropriate STDP contract vehicle, inadequate system testing, and system redundancy. Specifically,

- **Contract vehicle:** VA's choice of a contract vehicle for the STDP was appropriate. Our review showed that VA is using a hybrid contract for STDP, which entails leveraging a firm-fixed-price portion for hardware and software purchases, and a time-and-materials portion for creation of the dashboards. Per Office of Management and Budget acquisition policy, the use of this hybrid method of contracting is appropriate for short-term software development efforts where estimated development costs are unknown. Specifically, Office of Management and Budget Circular A-11, "Capital Programming Guide," states that it may not be possible to estimate the cost of performing an entire contract with sufficient accuracy to support the use of a fixed price or structured incentive contract. As such, the guide states that it may be desirable to initiate the work with a small, short-duration time-and-materials or cost-plus-fixed-fee contract until development work is complete. STDP project management was unable to predict with sufficient accuracy the effort needed to build the first dashboards for the system. VA's use of a time-and-materials contract for software development provided the flexibility needed to address STDP project uncertainties.

- **STDP testing:** VA properly identified, documented, and corrected functionality defects found during testing, as required by project plans and contract milestones. Test documentation showed correction of a number of defects during successive software releases for the project. For example, system developers remediated problems such as lack of scroll bar functionality, broken reference links to source data, data export errors, and inadequate system performance encountered with the various software releases. VA's use of an incremental approach, making small changes on a frequent basis over a short duration, makes it easier to control development work and ensure that corrections and fixes work effectively. This method is consistent with the contract and project test plan, and meets VA requirements for project management.
- **Redundant functionality:** The STDP dashboard as currently implemented has some overlapping functionality with legacy systems as it uses common data resident within VA's Decision Support System (DSS). According to representatives from VA's Decision Support Office, DSS is the central repository for reporting information related to operational costs for all VA lines of business and provides the underlying data for STDP. However, VA has planned that incremental advancements in STDP development will eventually exceed DSS reporting capabilities. Ultimately, STDP will provide management with readily accessible cost and accountability information not easily compiled with current legacy systems.

Access Control Weaknesses

We substantiated the allegation that VA did not adequately protect sensitive VA information from unauthorized access and disclosure. In February 2011, the STDP training manager submitted a user request to OIT to provide super user permissions (full access) for 20 individuals participating in STDP system testing. Austin Information Technology Center and Corporate Data Center Operations representatives granted system access without approval from VA's National Data Systems Group, which governs access to sensitive Veterans Health Administration (VHA) Core National Data Extract information hosted on VA systems.

In March 2011, OIT populated STDP with VHA Core National Data Extract information, including personally identifiable birth date, age, sex, race, ethnicity, county of residence, zip code, and financial information. More than 20 system users had inappropriate access to the sensitive data hosted in the STDP development environment for 35 days. Project managers initiated actions to downgrade users' system access to "view only" permission when students in a training class discovered the excessive privileges in mid-April 2011. By late April 2011, STDP project management had reviewed all system user accounts and downgraded permission levels for 50 system users in total. Project management migrated STDP from development to production in May 2011. Nonetheless, project management did not report a

potential breach of VA sensitive data because it was unaware of VA policy requiring reporting on this type of security event.

VA has published a range of guidance, outlining requirements for systems security access control. Specifically, VA Handbook 6500, *VA Information Security Program*, requires project authorities for high-impact systems formally to establish logical access controls that enforce the most restrictive set of rights or privileges for users based on their duties. Additionally, VA Handbook 6500 requires that information owners determine access and privileges for users of systems containing sensitive information and mandates that Information Security Officers review all system access requests. Part of VA Handbook 6500, *VA National Rules of Behavior*, requires users to report suspected or identified security events. VA Handbook 6500.02, *Management of Security and Privacy Events*, supplements this guidance by requiring users and system officials to report security events to the VA Network Security and Operations Center. Further, VA Directive 6066, *Protected Health Information*, defines data contained in the National Data Extract information as sensitive personal financial information.

Inadequate Information Security Awareness and Oversight

VA's weaknesses in protecting sensitive STDP data resulted from several factors:

- Project management did not implement formal procedures for granting and reviewing user access to STDP in line with VA guidance. Initial ad hoc procedures used by project management did not consistently require special approvals to grant access to VA sensitive data hosted in STDP. Management followed these ad hoc procedures when creating test user accounts until the release of draft procedures, *STDP Dashboard Access Request SOP*, in March 2011. The draft procedures established requirements for the National Data Systems Group to approve all requests to sensitive VHA Core National Data Extract information hosted in STDP. Program offices used these draft procedures as guidelines for granting user access rights, but did not fully adhere to all requirements outlined in the document. To date, VA has not finalized procedures for granting system access to STDP.
- OIT (Austin Information Technology Center) representatives did not recognize that STDP system users had requested excessive system access rights beyond what they needed for testing purposes. Our review disclosed that the use of confusing acronym codes on access authorization forms made it difficult for authorizing officials to identify excessive system access requests. This led officials to approve the user account requests without first vetting them through the National Data Systems Group as required.

- VA did not consistently assign an Information Security Officer to oversee STDP development. VA policy required assignment of an Information Security Officer to ensure security controls, such as access approval processes, were in place and functioning correctly. Without active Information Security Officer oversight, STDP project management was not fully informed of VA's information security requirements and did not implement sufficient approval processes to protect access to VA sensitive data. The lack of oversight also contributed to management's failure to report security violations upon discovering excessive user rights in the system.

Data Protection Not Assured

Access control weaknesses during STDP project development created opportunities for unauthorized use and disclosure of sensitive VA privacy information hosted in STDP. While we did not discover indications of actual information security breaches and recognize the system is not publicly accessible via the Internet, project management should have reported excessive user permissions as a security event in accordance with VA information security policy.

Until effective controls are in place to prevent future unauthorized access, VA information systems and sensitive veteran financial data will remain vulnerable to the risk of compromised confidentiality, integrity, and availability. VA could better assure STDP information security by taking the following actions:

- Provide project managers with the training needed to gain a thorough understanding of VA's information security requirements.
- Formalize procedures for reviewing and approving STDP access requests with the appropriate levels of user permissions.
- Assign Information Security Officers throughout STDP development and include them in the process of reviewing and approving user access requests.

Recommendations

1. We recommend the Assistant Secretary for Information Technology, in coordination with the Assistant Secretary for Management, ensure that Systems to Drive Performance project managers receive training that specifically addresses all of information security requirements for system development as defined in VA Handbook 6500, *VA Information Security Program*.

2. We recommend the Assistant Secretary for Information Technology assign Information Security Officers to oversee Systems to Drive Performance development activities, ensure proper approval of requests for user access to the system at the appropriate levels, and report information security events in accordance with VA policy.

3. We recommend the Assistant Secretary for Information Technology establish clear, easily distinguishable authorization codes to define levels of user access to Systems to Drive Performance applications and sensitive data.

4. We recommend the Assistant Secretary for Management finalize and implement formal procedures for ensuring Systems to Drive Performance user access control in accordance with VA policy.

Management Comments

The Principal Deputy Assistant Secretary, Office of Information and Technology, concurred with our findings and recommendations. OIT will ensure that employees assigned to the STDP project receive the role-based security training needed to address the issues highlighted in the report. Additionally, an Information Security Officer was assigned to the project in May 2011 to ensure VA's information security requirements are met. Further, the project team, in conjunction with OIT, will review and evaluate authorization codes to ensure they utilize clear and easily distinguishable names.

The Executive in Charge, Office of Management, also concurred with our findings and recommendations. The STDP project team will work with the Information Security Officer to ensure that each team member receives all required training, including VA's Privacy and Security Awareness training, and has signed VA's Rules of Behavior. In December 2011, the project team updated draft standard operating procedures regarding user access. The Office of Information Technology was reviewing the draft procedures prior to review and signature by the Executive in Charge, Office of Management.

OIG Response

Management's comments and corrective action plans are responsive to the recommendations. We will follow up as required on all actions.

Appendix A Scope and Methodology

Our review determined the merits of a VA Hotline allegation that VA has failed to adequately manage the STDP project. We did not evaluate whether STDP functionality met project goals or whether financial dashboards provide sufficient information to facilitate effective decision-making. To accomplish this review, we interviewed VA program officials and staff, examined STDP project documentation, and examined the vendor's contracts with VA. We researched applicable VA Directives and Federal information security requirements, and identified relevant business processes and information system security controls. Additionally, we evaluated VA activities to oversee the user accounts provisioning process, reporting of information security events, and project management practices to ensure compliance with VA policies and procedures.

We conducted our fieldwork at VA's Office of Management and Office of Information Technology in Washington, DC. We performed all fieldwork from April to August 2011.

Reliability of Computer-Processed Data

We did not request computer-processed data for this review. As such, we did not review the accuracy or reliability of data or reports produced by the system. We evaluated the sufficiency and accuracy of information provided in connection with STDP contracts, software development processes, and system security controls.

Compliance With CIGIE Standards

We conducted our review in accordance with *Quality Standards for Inspections* published by the Council of the Inspectors General on Integrity and Efficiency. We planned and performed the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objective.

Appendix B Background

Project History

VA's STDP project supports the Office of Management and Budget's Enterprise Wide Cost Accountability initiative for better cost management within Federal agencies. VA undertook the STDP project to provide a capability to clearly identify, present, and analyze VA financial information to support management decisions. More specifically, STPD aims to provide VA management with "real-time" information to facilitate decisions related to budgets and performance, and to achieve greater value from the allocation of VA resources.

The STDP project makes use of a commercial off-the-shelf product called "QlikView" to rapidly create business intelligence dashboard displays that show existing VA data in a graphical format. The dashboards use data extracts from VA's Decision Support System (DSS), an activity based cost allocation system that estimates cost of providing patient care based on information extracted from payroll and general ledger data. More specifically, DSS provides a mechanism for integrating expenses, workload, and patient utilization to measure quality of care, clinical outcomes, and their financial impact. Developers transfer the data extracts to STDP hardware. Unlike DSS, "QlikView" holds data in resident memory, allowing real-time data manipulation and reporting capability not provided by the legacy system. Additionally, "QlikView" graphical dashboards create custom user-defined reports that simplify interpretation of complex data and offer alternatives to the spreadsheet-style reports generated by DSS.

In August 2010, VA awarded a $2.5 million contract to Healthcare Tech Solutions International to develop and deploy applications in support of the STDP project. The contract included an additional $1 million option year and multiyear provisions for continued support. The contract covered several phases of application development, including the purchase and installation of hardware and software under firm-fixed pricing and the development of five financial dashboards under a time-and-materials component of the contract.

During initial development, STDP was populated with data from non-sensitive DSS sources. In March 2011, VA populated the system with VHA Core National Data Extract information that included patients' personally identifiable information as defined by VA policy. Specifically, extract data contained patient information such as birth date, age, sex, race, ethnicity, county of residence, zip code, and other financial information. The extract also contained social security numbers that were scrambled using a simplistic algorithm that does not meet Federal encryption standards. STDP was migrated from development to an operational state in May 2011.

Appendix C Assistant Secretary for Information Technology Comments

Department of Veterans Affairs

Memorandum

Date: January 23, 2012

From: Principal Deputy Assistant Secretary for Information Technology (005A)

Subj: OIG Draft Report – Review of Alleged Mismanagement of the Systems to Drive Performance Project

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

Thank you for the opportunity to review the subject Office of Inspector General (OIG) draft report. The Office of Information and Technology concurs with OIG's findings and submits the attached written comments for each recommendation.

If you have any questions, feel free to call me at 202-461-6910, or have a member of your staff contact Gary Stevens, Director, Cyber Security (005R2), Office of Information and Technology at 202-632-7538.

(original signed by:)

Stephen W. Warren

Attachment

005 Attachment

Office of Information Technology
Response to draft OIG Report,
"Review of Alleged Mismanagement of the Systems to Drive Performance Project"

OIG Recommendations

1. We recommend the Assistant Secretary for Information Technology, in coordination with the Assistant Secretary for Management, ensure that Systems to Drive Performance project managers receive training that specifically addresses all of information security requirements for system development as defined in VA Handbook 6500, VA Information Security Program.

OIT Comments: Concur. The Office of Information Technology (OIT) will ensure that its employees on the System to Drive Performance (STDP) project receive the necessary role based security training to address the issues highlighted in the report. This training is expected to be completed no later than February 28, 2012. Furthermore, OIT will request that the Program Manager for the STDP project ensure all non-OIT employees also receive the appropriate role based security training by February 28, 2012.

2. We recommend the Assistant Secretary for Information Technology assign Information Security Officers to oversee Systems to Drive Performance development activities, ensure proper approval of requests for user access to the system at the appropriate levels, and report information security events in accordance with VA policy.

OIT Comments: Concur. An information security officer (ISO) was assigned to the STDP project in May 2011, to ensure that VA information security requirements are met. The ISO for STDP is identified in the Security Management and Reporting Tool (SMART). OIT recommends closure of this recommendation.

3. ***We recommend the Assistant Secretary for Information Technology establish clear, easily distinguishable authorization codes to define levels of user access to Systems to Drive Performance applications and sensitive data.***

OIT Comments: Concur. The STDP project team, in conjunction with OIT, will review and evaluate STDP authorization codes to ensure that they utilize clear and easily distinguishable names for Active Directory Groups. The target date for implementation of these codes is by February 15, 2012. The STDP SOP will be revised to include the updated authorization codes and their level of access.

4. We recommend the Assistant Secretary for Management finalize and implement formal procedures for ensuring Systems to Drive Performance user access control in accordance with VA policy.

To be addressed by the Office of Management (Appendix D)

Appendix D Assistant Secretary for Management Comments

Department of Veterans Affairs **Memorandum**

Date: January 27, 2012

From: Executive in Charge, Office of Management, and Chief Financial Officer (004)

Subj: Review of Alleged Mismanagement of the Systems to Drive Performance Project (VAIQ 7189732)

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

1. The Office of Management has reviewed the subject draft report provided on December 22, 2011. We concur with the findings and recommendations.

2. Regarding the allegation that VA did not adequately protect sensitive information from unauthorized access and disclosure, we agree with the finding that additional preventative measures should have been taken regarding security requirements and access control. Although only a small number of employees actually had access to the data for a short period of time prior to the application being placed into production, the data was technically available to users who had been trained to access it. Upon detection of the unauthorized access, STDP management took immediate action to remediate the issue and performed a complete review of all user accounts to preclude unauthorized user access.

3. Responses to the recommendations directed to this office are as follows:

Recommendation 1: Assistant Secretary for Information and Technology (OIT), in coordination with the Assistant Secretary for Management, should ensure that STDP project managers receive training on project-related information security requirements.

Concur. The OM STDP team will work with the OIT ISO for the STDP project to ensure that each member of the project team has received all required training, including VA Privacy & Security Awareness training, and has signed the VA Rules of Behavior. Target Completion Date: Second quarter, FY 2012; contingent on OIT timeframe.

Recommendation 4: Assistant Secretary for Management should finalize and implement formal procedures for ensuring STDP user access controls.

Concur. On December 22, 2011, the STDP project team completed its re-write of the draft user access standard operating procedures. OIT is reviewing the draft prior to OM review and signature. Target Completion Date: February 28, 2012.

4. Thank you for the opportunity to review and comment on this draft report.

(original signed by:)

W. Todd Grams

Appendix E Office of Inspector General Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman, Director Michael Miller Gordon Snyder Felita Traynham

Appendix F Report Distribution

VA Distribution

Office of the Secretary
Veterans Health 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 will be available in the near future on the OIG's Web site at http://www.va.gov/oig/publications/reports-list.asp. This report will remain on the OIG Web site for at least 2 fiscal years.