VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Incomplete Installation of Encryption Software Licenses

October 11, 2012
12-01903-04

ACRONYMS AND ABBREVIATIONS

IT	Information Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
PMAS	Project Management Accountability System
SD&E	Service Delivery and Engineering
VA	Veterans Affairs

Report Highlights: Review of VA's Alleged Incomplete Installation of Encryption Software Licenses

Why We Did This Audit

OIG received a hotline allegation that the Office of Information Technology (OIT) had not installed and activated all of the 300,000 Guardian Edge encryption software licenses purchased in 2006 at a cost of about $3.7 million.

What We Found

We substantiated the allegation and found that OIT had not installed and activated an additional 100,000 licenses purchased in 2011. As of July 2012, OIT officials stated they had installed and activated only a small portion, about 65,000 (16 percent), of the total 400,000 licenses procured.

OIT did not install and activate all of the licenses due to inadequate planning and management of the project. Specifically, OIT did not allow time to test the software to ensure compatibility with VA computers, ensure sufficient human resources were available to install the encryption software on VA computers, and adequately monitor the project to ensure encryption of all VA laptop and desktop computers.

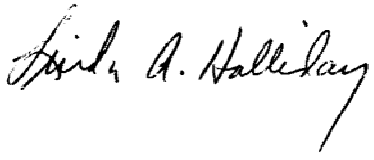
As such, 335,000 (84 percent) of the total 400,000 licenses procured, totaling about $5.1 million in questioned costs, remain unused as of 2012. Given changes in VA technology since 2006, the Department lacks assurance the remaining software licenses are compatible to meet encryption needs in the current computer environment. Further, because OIT has not installed all 400,000 encryption software licenses on VA laptop and desktop computers, veterans' personally identifiable information remains at risk of inadvertent or fraudulent access or use.

What We Recommend

We recommended the Assistant Secretary for Information Technology complete the assessment of the encryption software project to determine whether the software is compatible with VA's operating systems and still meets the Department's needs. Based on the assessment, OIT should terminate the project or develop a plan, including adequate human resources and project monitoring, to ensure installation and activation of the remaining encryption software licenses.

Agency Comments

The Assistant Secretary for Information Technology concurred with our finding and recommendations and provided an appropriate action plan. We will follow up on the implementation of corrective actions.



LINDA A. HALLIDAY
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Objective

We evaluated the merits of a VA Office of Inspector General (OIG) Hotline complaint that the Office of Information Technology (OIT) had not installed and activated all of the 300,000 Guardian Edge encryption software licenses purchased in 2006 at a cost of about $3.7 million.

Background

In May 2006, a stolen hard drive initiated a heightened and immediate concern by VA for the protection of personally identifiable information. Specifically, an unencrypted external hard drive of a VA laptop was stolen from the home of a VA employee. The hard drive contained personally identifiable information for 26 million veterans. VA initiated notifications to the veterans at an expense of approximately $20 million for credit monitoring and mailings. In August 2006, the VA Secretary mandated that OIT upgrade all VA lap and desktop computers with enhanced data security encryption software.

Allegation

In October 2011, we received an anonymous Hotline complaint that OIT had not installed and activated all of the 300,000 Guardian Edge encryption software licenses purchased. According to the complainant, OIT purchased the licenses in 2006 for about $3.7 million from Systems Made Simple. The complainant alleged that VA had used the software to encrypt only 40,000 of some 450,000 lap and desktop computers.

Prior Reviews

Our annual Federal Information Security Management Act reviews have repeatedly identified the need for VA to address information security weaknesses, including inadequate implementation and enforcement of oversight controls over access to information systems. Such weaknesses place sensitive information at risk of unauthorized access, loss, or fraudulent use.

Appendix A provides additional background information on our review. Appendix B provides details on our review scope and methodology. Appendix C provides potential monetary benefits and Appendix D includes comments by the Assistant Secretary for Information Technology.

RESULTS AND RECOMMENDATIONS

Finding Incomplete Encryption Software Installation

We substantiated the allegation that OIT had not installed and activated all of the 300,000 encryption software licenses purchased in 2006. Additionally, we found that OIT had not installed and activated an additional 100,000 licenses purchased in 2011. As of July 2012, OIT officials stated they had only installed and activated approximately 65,000 (16 percent) of the total 400,000 licenses procured.

OIT did not use all of the licenses due to inadequate planning and management of the encryption software project. Specifically, prior to acquisition, OIT officials did not allow time to test the software on VA laptop and desktop computers; OIT lacked sufficient human resources and did not monitor the project to ensure complete installation and activation of the software licenses. As a result, 335,000 licenses, totaling about $5.1 million in questioned costs, remained inactive. OIT acknowledged that VA laptop and desktop computers remain unencrypted. As a result, veterans' data remained at risk due to unencrypted computers.

Incomplete Installation and Activation

OIT had not installed and activated all of the 300,000 encryption software licenses purchased in 2006 and the additional 100,000 purchased in 2011, spending about $5.9 million for licenses and maintenance agreements. Details of VA purchases follow.

- In August 2006, VA purchased 300,000 Guardian Edge encryption software licenses and maintenance agreements for $2.4 million.
- Between 2007 and 2011, VA spent another $1.2 million to continue the maintenance agreements for the 300,000 licenses.
- In April 2011, VA purchased an additional 100,000 licenses and maintenance agreements totaling approximately $2.3 million, which included a 2-year extended maintenance agreement on the original 300,000 licenses.

The Clinger Cohen Act of 1996 requires the Chief Information Officer to ensure information technology programs are monitored and evaluated. The Chief Information Officer is also required to advise the head of the agency on whether to continue, modify, or terminate projects. Moreover, human resources should be sufficient for the successful performance of information technology programs.

In August 2006, the VA Secretary mandated that OIT encrypt all laptops by September 2006. According to OIT officials, they managed to encrypt about 25,000 to 30,000 laptops by September 2006. OIT did not maintain

inventory records dating back to 2006, so we were unable to verify the actual number of VA laptops encrypted. After the laptop installation in September 2006, OIT attempted to install the encryption software on VA's desktop computers, but encountered incompatibility issues between the different makes and models of VA desktop computers and the encryption software. OIT discontinued installation of the encryption software until OIT could upgrade and standardize VA's computer equipment.

As of July 2012, OIT had only activated 65,000 (16 percent) of 400,000 encryption software licenses and had not identified plans to install and activate the remaining 335,000. OIT officials stated the 65,000—which could include duplicate counts when computers are turned off, reimaged, then turned on again or when computers are upgraded and not scrubbed—represent the number of computers that had logged into the Guardian Edge/Symantec server within the previous 90 days.

As of August 2012, OIT was still assessing whether the encryption software would be compatible with existing operating systems and meet the Department's needs. At the time of our review, OIT could not provide us reasonable assurance that it would install and activate the remaining encryption software licenses.

Why Not Installed and Activated

Over a 6-year period, OIT has not installed and activated the encryption software licenses due to inadequate planning and management of the project. Specifically, OIT did not make time to test the encryption software to ensure compatibility with VA computers. It lacked sufficient human resources and did not monitor the project to ensure complete installation and activation of the encryption software licenses.

- **Lack of Software Testing—**OIT officials stated that, in 2006, they did not test the encryption software prior to the acquisition because they only had about 30 days to install and activate the encryption software licenses on all laptops after contract award. OIT decided not to move forward with activation of the software licenses on desktop computers until VA could upgrade the computer equipment with operating systems compatible with the encryption software.
- **Insufficient Human Resources—**OIT officials stated that, although they had over 5,000 people in their organization, they struggled with coordinating the encryption software implementation due to competing priorities. For example, in 2009, OIT needed human resources to transition from Windows XP to Windows 7. Similarly, in March 2012, OIT could not allocate sufficient resources to the software installation because VA had embarked upon a cultural transformation with implementation of the Continuous Readiness in Information Security Program—an integrated approach to protecting sensitive information from inappropriate exposure or loss.

- **Lack of Project Monitoring**—The Service Delivery and Engineering (SD&E) department was responsible for ensuring the encryption software implementation. SD&E officials indicated that they used the Technical Information Program to monitor the encryption software project. However, these officials could not provide specifics about the Technical Information Program, nor how SD&E used it to ensure installation and activation of the software licenses. Additionally, OIT officials could not provide evidence of any other oversight and monitoring activities from 2006 through 2009.

From 2009 through 2011, SD&E did not enforce the oversight process in place—Project Management Accountability System (PMAS)—to ensure installation of all of the encryption software or pausing or terminating the project. According to the project manager, OIT should have established the project in PMAS. Had SD&E established the project in PMAS, it would have better ensured complete installation and activation of software licenses, available human resources to do the work, and transparency so that OIT leadership and project management could have clearly identified cost, schedule, quality, scope, and resource information. According to an SD&E official, previous project managers did not use PMAS because they did not fully understand the PMAS requirements.

Moreover, rather than open a new project in PMAS for monitoring, OIT planned to incorporate the encryption software into the Windows 7 upgrade, which would enable the licenses to automatically install and activate. However, requirements for the Windows 7 project indicated that the installation and activation of the encryption software was optional; therefore, there was no assurance that the encryption software would have been installed and activated with the deployment of Windows 7. By initiating the project in PMAS, OIT may have had a better handle on tracking project status, including pausing or terminating the project.

Conclusion

Because of inadequate project planning and management, 335,000 licenses, totaling about $5.1 million in questioned costs, remained unused. OIT officials acknowledged that they had fallen short with the installation and activation of the licenses, purchased in 2006 and 2011, and that some VA computers remain unencrypted. Consequently, veterans' data remained at risk of tampering, fraud, and inappropriate disclosure. As of August 2012, OIT was assessing whether the encryption software was compatible with the Department's current operating systems and could not provide reasonable assurance that it would use the remaining software to encrypt VA computers.

Recommendations

1. We recommended the Assistant Secretary for Information Technology complete the software encryption project assessment to determine whether to continue or terminate the project.

2. We recommended the Assistant Secretary for Information Technology, if it is determined to continue the project, develop a plan that includes sufficient human resources and monitoring to install and activate all of the purchased encryption software licenses.

Management Comments and OIG Response

The Assistant Secretary for Information Technology concurred with our finding and recommendations. OIT completed its assessment of the encryption software and found the software to be compatible with the Department's current operating systems. As such, OIT developed a plan to deploy Windows 7, which will include the encryption software, by September 2013. Additionally, OIT asserts that the necessary human resources and monitoring tools are now in place to complete the Windows 7 deployment plan.

The implementation plan is acceptable, and we are closing Recommendation 1 based on OIT's response to Recommendation 1 and actions to be taken in Recommendation 2. We will follow up on the planned actions to deploy Windows 7 until they are completed. Appendix D contains the full text of the Assistant Secretary for Information Technology comments.

Appendix A Background

OIT Purpose and Components

The Office of Information Technology (OIT) is the steward of the Department's information technology (IT) assets and resources. OIT provides strategy and technical direction, guidance, and policy to ensure that IT resources are appropriately acquired and managed for the Department. The Assistant Secretary for Information Technology, or Chief Information Officer, is the single leadership authority for IT. The Chief Information Officer is the principal advisor to the Secretary on all matters relating to the management of VA's IT.

Within OIT, the Service Delivery and Engineering (SD&E) component is responsible for all computers within the organization including the operational and maintenance activities associated with VA's IT environment. For example, this OIT component is responsible for overseeing and managing VA's regional data centers and the IT network, conducting production monitoring for all information systems, and managing the delivery of operations services to all VA geographic locations. Field Operations, a division of the Service Delivery and Engineering component, is responsible for the actual implementation of the encryption software.

Encryption Software Purchase

In August 2006, VA awarded a $4 million contract to Systems Made Simple for 300,000 Guardian Edge encryption software licenses, maintenance, training, and other optional services, such as additional training, to include contractor travel for onsite consultation for deployment assistance. Systems Made Simple, acquired by Symantec Corporation in 2010, was a service-disabled, veteran-owned business that delivered leading IT solutions to Fortune 500 customers and Federal agencies, including the Environmental Protection Agency and General Services Administration. In 2011, VA purchased an additional 100,000 licenses and maintenance, totaling approximately $2.3 million, from Symantec Corporation. This purchase also included a 2-year extended maintenance agreement on the original 300,000 licenses purchased in August 2006.

Appendix B Scope and Methodology

We conducted our work from March through July 2012. Our focus for this review was on OIT's 2006 implementation of 300,000 encryption software licenses on VA computers. We also considered whether OIT implemented an additional 100,000 licenses procured in 2011.

Methodology

To conduct our review, we examined applicable VA criteria and compared it with Federal IT best business practices and standards to determine whether they were parallel. We also reviewed the Guardian Edge contract and financial documentation to obtain the cost per license, the total number of licenses, the total amount spent on maintenance agreements, and the option years exercised.

We extracted license and maintenance contract data as illustrated in Tables 1 and 2, and calculated questioned costs from 2006 through 2011 for unused licenses in Table 3.

Table 1

License Contract Data						
Purchase Year	**Licenses**		**License Purchase Costs[2]**	**Maintenance Costs[1]**		**Number of Years**
	Purchased	**Unused**		**2006-2011[3]**	**2011[4]**	
2006	300,000	235,000[1]	$ 7.00	$1.00	$1.17	5
2011	100,000	100,000	19.79	N/A	$0.00	2

Source: VA OIG based on documentation provided by OIT
[1]Based on Guardian Edge/Symantec server connection scans within the last 90 days.
[2]Cost per license.
[3]Maintenance fee $1.00 per license charged every year for 5 years.
[4]Maintenance fee $1.17 per license charged for 2 years for the 2006 license purchase.

Table 2

Total License and Maintenance Costs (in millions)							
License Costs	**Costs By Year**						**Total Costs**
	2006	**2007**	**2008**	**2009**	**2010**	**2011**	
Purchase[1]	$2.100	$0.000	$0.000	$0.000	$0.000	$1.979	$4.079
Annual Maintenance[2]	0.300	0.300	0.300	0.300	0.300	0.351	1.851
Total	**$2.400**	**$0.300**	**$0.300**	**$0.300**	**$0.300**	**$2.330**	**$5.930**

Source: VA OIG based on documentation provided by OIT
[1]Total licenses multiplied by purchase costs.
[2]Total licenses multiplied by maintenance costs.

Table 3

Unused License and Maintenance Costs (in millions)							
Unused License Costs	**Questioned Costs By Year**						**Total Costs**
	2006	**2007**	**2008**	**2009**	**2010**	**2011**	
Purchase[1]	$1.645	$0.000	$0.000	$0.000	$0.000	$1.979	$3.624
Annual Maintenance[2]	0.235	0.235	0.235	0.235	0.235	0.275	1.450
Total	$1.880	$0.235	$0.235	$0.235	$0.235	**$2.254**	**$5.074**

Source: VA OIG based on documentation provided by OIT
[1]Unused licenses multiplied by purchase costs.
[2]Unused licenses multiplied by maintenance costs.

We attempted to obtain costs associated with the data breach notifications and settlements, but OIT does not track these costs. We also attempted to obtain inventory records to identify the number of laptops and desktops VA maintains. However, OIT could not provide this data.

We interviewed the complainant to obtain an understanding of the allegation. We also met with key VA officials to learn about the encryption software and plans to deploy the unused software.

Data Reliability

We did not receive computer-processed data for this review. As such, we could not review the accuracy or reliability of such data.

Government Standards

We conducted this review in accordance with the *Quality Standards for Inspection and Evaluation* published by the Council of 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 C Potential Monetary Benefits in Accordance With Inspector General Act Amendments

Recommendation	Explanation of Benefits	Better Use of Funds	Questioned Costs
1–2	Lack of planning, management, and monitoring of the encryption software project.	$0	$5.1 million
	Total	**$0**	**$5.1 million**

Appendix D Assistant Secretary for Information Technology Comments

Department of Veterans Affairs

Memorandum

Date: September 28, 2012

From: Assistant Secretary for Information Technology (005)

Subj: OIG Draft Report, Review of Alleged Incomplete Implementation of Encryption

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

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

If you have any questions, please contact my office.

Roger W. Baker

Attachment

OIG Recommendations

1. We recommend the Assistant Secretary for Information Technology complete the software encryption project assessment to determine whether to continue or terminate the project.

OIT Response: Concur. OIT's assessment of the encryption software has been completed. The software was found to be compatible with the Department's current operating systems. OIT leadership supports the continued use of the current Symantec Full Disk Encryption software to encrypt every desktop and laptop computer. With VA data residing on these devices, it is vital to protect that data.

2. We recommend the Assistant Secretary for Information Technology, if it is determined to continue the project, develop a plan that includes sufficient human resources and monitoring to install and activate all of the purchased encryption software licenses.

OIT Response: Concur. OIT has the appropriate human resources and monitoring tools in place to install and activate all of the purchased encryption software licenses. The Encryption/Win 7 deployment plan is as follows:

a. Win 7 deployments started on June 1, 2011. Over 23,000 machines are currently on Win 7 and encrypted.

b. Clinical deployment will begin after October 1, 2012.

c. VBA deployment will begin after September 24, 2012.

d. The rate of deployment will be approximately 2% per week, with expected completion of September 30, 2013.

OIT Technical Comments to OIG Findings in the Draft Report -

None.

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	Mario Carbone, Director Curtis Hill John Houston Heather Jones Crystal Markovic

Appendix F 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 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.