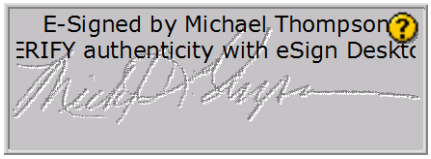
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 14, 2015

MEMORANDUM FOR: JUDITH A. ADAMS
ACTING VICE PRESIDENT, INFORMATION TECHNOLOGY



FROM: Michael L. Thompson
Acting Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Management Alert – Management of Unauthorized Software (Report Number IT-MA-15-003)

This management alert presents the results of our review of the U.S. Postal Service's Management of Unauthorized Software (Project Number 14WG015IT001).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Aron Alexander, director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Introduction

We are issuing this management alert to provide U.S. Postal Service management with insight regarding unauthorized software on the Postal Service network (Project Number 14WG015IT001). Our objective was to determine whether the Postal Service identifies and removes unauthorized software on its network nationwide. During our *Software Inventory Management – Greater Boston District* audit (Project Number 14WG015IT000) we identified an issue with nationwide impact. This management alert responds to ineffective practices for identifying and removing unauthorized software. In addition, in July 2013, the U.S. Postal Service Office of Inspector General (OIG) issued an audit report[1] stating that the Postal Service did not manage software in accordance with policy.

Software assets include all information technology (IT) programs, applications, operating systems, and related resources. Management must procure and maintain all software installed on Postal Service IT resources in accordance with agency policies and procedures. Postal Service policy requires listing all approved software within the Infrastructure Toolkit (ITK).[2] Management should remove from the Postal Service Computing Environment any software that is not listed in the ITK or approved and maintained by IT management.

Controls over inventory of authorized and unauthorized software ranks second on the list of the 20 most critical security controls in the industry.[3] To respond effectively to emerging threats and detect unauthorized software, the Postal Service must manage and monitor its software inventories.

Conclusion

The Postal Service identifies unauthorized software on its network enterprise-wide bi-annually, rather than quarterly, as required.[4] Even when unauthorized software is identified, the Postal Service does not remove unauthorized products as required because management did not assign responsibility for removal of this software. While we recognize that management has taken steps to periodically identify unauthorized software, they must do so more frequently and take further action to remove these unauthorized products. Without appropriate controls in place, unauthorized software on the Postal Service network could expose the organization to vulnerable versions of software, penalties for violating software license agreements, and cyber-attacks. Frequently monitoring and quickly removing unauthorized software can minimize the

[1] *Management and Utilization of Software Licenses* (Report Number IT-AR-13-006, dated July 31, 2013).
[2] A repository of software implemented through the corporation. There are three classifications of software in the ITK: approved, restricted (approved use for a certain group of users), and obsolete/rejected.
[3] Ranking is according to the SysAdmin, Audit, Networking, and Security Institute, This organization is responsible for developing, maintaining, and making available, at no cost, the largest collection of research documents about various aspects of information security.
[4] Handbook AS-805*, Information Security*, Section 10-3.1, Software Safeguards; and Section 10-3.4.3, Prohibited Software, dated May 2014.

damage of a system compromise. We determined that Postal Service assets valued at about $33 million were at risk due to unauthorized software remaining on the network.

Unauthorized Software

Twice a year management identified unauthorized software enterprise-wide, but they are required to monitor and identify unauthorized software quarterly.[5] Furthermore, they have not taken steps to remove these unauthorized products from the Postal Service network. Specifically, the Enterprise-Wide Software Asset Management Controlling Authority did not require Desktop Computing to remove unauthorized software products. Desktop Computing currently monitors unauthorized software activity by:

- Conducting network scanning using the System Center Configuration Manager (SCCM)[6] to identify installed software on Advanced Computing Environment (ACE)[7] systems.

- Performing manual comparisons to the ITK to determine whether installed software products are authorized.

- Generating *Unauthorized Software Activity* reports,[8] which are not released to management or district personnel.

- Issuing security warning screen banners on systems that include unauthorized software.

In March 2015, we reviewed the *Unauthorized Software Activity* report that Desktop Computing generates and identified 2,355[9] software products that appear to be unauthorized and do not have a business purpose. Examples of products that do not appear to have a business purpose include the Coupon Printer for Windows[10] (nine instances), 100 Electric Blues Guitar Licks[11] (one instance), Masque World-Class Poker[12] (one instance), Rosetta Stone Home School[13] (one instance), My Family Tree[14] (one instance) and Turbo Tax software[15] (48 instances) installed on systems across the network.

---

[5] Handbook AS-805, Section 10-3.1, Software Safeguards; and Section 10-3.4.3, Prohibited Software.
[6] A set of enterprise tools that can be used for hardware and software inventories, security updates, software distribution, operating system deployment, and more.
[7] ACE provides a standardized desktop environment for central management, minimizes local administration, and ensures that users have compatible tools.
[8] Desktop Computing generates the *Unauthorized Software Activity* reports [redacted]
[9] Desktop Computing provided the *Unauthorized Software Activity* report dated March 2015, listing 10,004 unauthorized software products. We removed 2,521 duplicate software products leaving a total of 7,483 products. Based on our analysis of the 7,483 software products, 2,355 did not appear to have a legitimate business need.
[10] Allows access to coupons from thousands of websites across the Internet.
[11] Provides links to guitar lessons.
[12] A poker collection that allows you to play a variety of poker games.
[13] A research-proven, technology-based approach that helps home school students in pre-kindergarten build foundational reading skills.
[14] My Family Tree software creates highly detailed genealogical trees.
[15] Turbo Tax software asks the users questions that affect their tax situations and fills in tax forms behind the scenes.

These circumstances occurred because management has not assigned an appropriate authority to ensure identification and removal of unauthorized software from the network. Without appropriate controls in place, the Postal Service is potentially at risk of running unsecure versions of software and violating software license agreements. Unauthorized software on the Postal Service network could expose the organization to cyber-attacks resulting in data breaches. We determined that Postal Service assets valued at about $33 million were at risk due to unauthorized software remaining on the network.

Recommendations

We recommend the acting vice president, Information Technology, direct the managers, Enterprise Access Infrastructure and Enterprise Architecture, to:

1. Assign responsibility for identifying and reviewing unauthorized software products on the network and, if applicable, remove these products or add them to the approved software listing.

We recommend the acting vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to:

2. Assign personnel to coordinate with district Information Technology staff on a quarterly basis to monitor, identify, and remove unauthorized software from the network.

Management's Comments

Management agreed with the finding and the recommendations in the report.

Regarding recommendations 1 and 2, management stated they will perform a holistic evaluation of software inventory management practices and processes in the IT organization. In addition, Enterprise Access Infrastructure will coordinate with Desktop Computing and Solutions Development and Support to evaluate current software inventory management practices and perform the necessary updates to better reflect the changing needs of the organization. The target implementation date is December 31, 2016.

See Appendix A for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report and corrective actions should resolve the issues identified in the report.

The OIG considers all recommendations significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
Software Inventory Management – Greater Boston District	IT-AR-15-007	7/13/2015	None
Report Results: Our report determined that effective software management practices are not in place to adequately protect and safeguard information resources in the Greater Boston District. Specifically, there are no clearly defined policies and procedures governing the software inventory management process. We recommended the Postal Service update its software inventory management process, identify software to add to its approved listing, and require district information technology personnel to follow approved software processes prior to software installation. We also recommended management establish an automated process to reconcile software inventories and coordinate with district staff to remove unauthorized software. Management agreed with five of our six recommendations.			
Management and Utilization of Software Licenses	IT-AR-13-006	7/31/2013	None
Report Results: Our report determined the Postal Service is not managing and using software in accordance with policy and software license agreements. Specifically, management does not have a reliable enterprise-wide software inventory, a process for periodically monitoring usage of all software on the network, and procedures in place to periodically conduct network scans. We recommended the Postal Service establish a controlling authority to govern software assets enterprise-wide to include creating and maintaining an enterprise-wide software inventory list, using the full capability of existing software monitoring tools to monitor compliance with software license agreements, revising policy to require periodic scans of workstations, and conducting scans to identify unauthorized software running on the Postal Service network. Management agreed with our recommendations.			

Appendix A. Management's Comments

Judith A. Adams
(A) Vice President
Information Technology

UNITED STATES POSTAL SERVICE

June 25th, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Management of Unauthorized Software (IT-AR-15-DRAFT)

Overall, Postal Service management agrees with the recommendations outlined in this Office of Inspector General's (OIG) audit report. Postal Service management recognizes the need for effective software management to maintain an accurate software inventory and to improve accountability, security, and compliance. Postal Service management will holistically evaluate the software inventory management policies and processes to address both recommendations.

Recommendation [1]:
Assign responsibility for identifying and removing unauthorized software products identified on the network enterprise-wide.

Recommendation [2]:
Assign personnel to coordinate with district Information Technology staff on a quarterly basis to monitor, identify, and remove unauthorized software from the network.

Management Response/Action Plan:
Management agrees with the recommendations above. Management will perform a holistic evaluation of software inventory management policies and processes in the IT organization. Enterprise Access Infrastructure will coordinate with Desktop Computing and Solutions Development and Support to evaluate the current software inventory management practices and update to better reflect the changing needs of the organization.

Target Implementation Date:
December 31, 2016

Responsible Officials:
Manager, Enterprise Access Infrastructure, Information Technology
Manager, Desktop Computing
Manager, Solutions Development and Support

475 L'Enfant Plaza SW
Washington DC 20260-5000
www.usps.com

Page 1 of 2

Judith A. Adams
(A) Vice President
Information Technology

Judith A. Adams
(A) Vice President, Information Technology

cc: *Sally K. Haring, Manager, Corporate Audit Response Management*

475 L'Enfant Plaza SW
Washington DC 20260-5000
www.usps.com