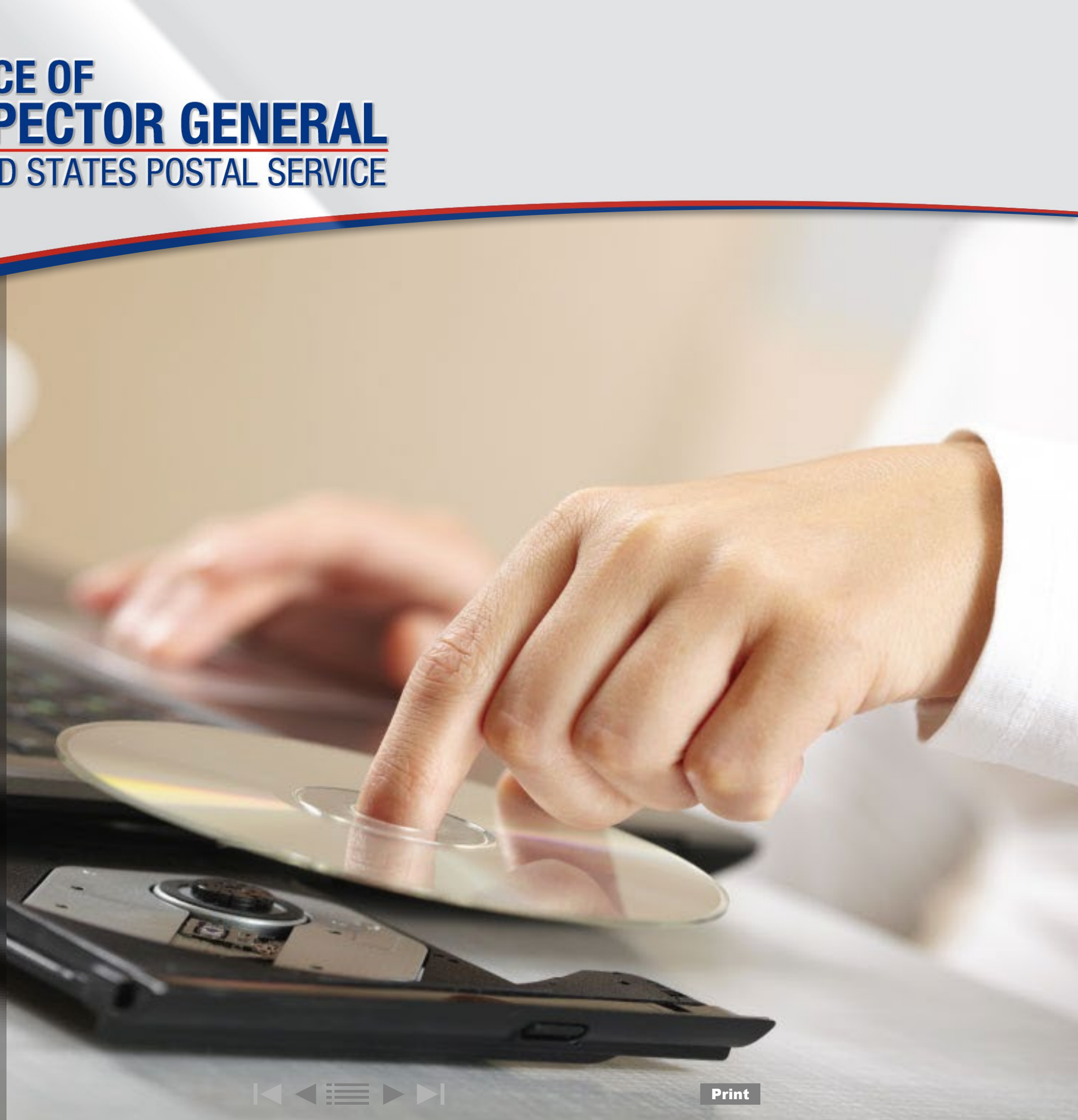
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Software Inventory Management – Greater Boston District

Audit Report

Report Number
IT-AR-15-007

July 13, 2015



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Effective software management practices are not in place to adequately protect and safeguard information resources in the Greater Boston District.

Background

Software management provides processes for managing inventories, license agreements, and monitoring software assets. Effective software management allows organizations to maintain an accurate software inventory to improve accountability, security, and compliance. Reliable software inventories are necessary to effectively test, evaluate, monitor, and manage information system controls.

The U.S. Postal Service Office of Inspector General's Information Technology Security Risk Model identified the Greater Boston District as the highest risk for security events in fiscal year 2014. Having an inventory of authorized and unauthorized software ranks second on the list of the 20 most critical security controls in the industry. To respond effectively to emerging threats and detect unauthorized software, the Postal Service must manage and monitor its software inventories.

Our objective was to evaluate the effectiveness of the Postal Service's software inventory management practices in the Greater Boston District.

What The OIG Found

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 for the software inventory management process including: roles and responsibilities, systems to maintain software inventories, and instructions for detecting and removing unauthorized software. In addition, there is no accurate inventory of software installed at facilities in the Greater Boston District. We identified 186 instances of unauthorized software products on 31 of the 161 computers we reviewed.

This occurred because headquarters management has not issued to districts detailed guidance related to the software inventory management process. Current systems the Postal Service uses to manage its enterprise-wide software inventory are not effective and are fragmented across the organization. Without an accurate inventory of software assets, the Greater Boston District may be using unsecure versions of software, purchasing unnecessary licenses, or violating software license agreements.

What The OIG Recommended

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.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 13, 2015

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

GREGORY S. CRABB
ACTING CHIEF INFORMATION SECURITY OFFICER AND VICE PRESIDENT, DIGITAL SOLUTIONS

RICHARD P. ULUSKI
VICE PRESIDENT, NORTHEAST AREA OPERATIONS

E-Signed by Michael Thompson
ERIFY authenticity with eSign Deskto

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

SUBJECT: Audit Report – Software Inventory Management – Greater Boston District (Report Number IT-AR-15-007)

This report presents the results of our audit of the Software Inventory Management – Greater Boston District (Project Number 14WG015IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Cover
Highlights....1
  Background....1
  What The OIG Found....1
  What The OIG Recommended....1
Transmittal Letter....2
Findings....4
  Introduction....4
  Conclusion....5
  Defining Software Inventory Management Processes....5
  Accuracy of Software Inventory....6
  Other Matters....7
    Engineering Software....7
Recommendations....8
    Management's Comments....8
    Evaluation of Management's Comments....9
Appendices....10
  Appendix A: Additional Information....11
    Background....11
    Objective, Scope, and Methodology....11
    Prior Audit Coverage....12
  Appendix B: Instances of Unauthorized Software....13
  Appendix C: Management's Comments....14
Contact Information....17

Findings

Introduction

This report presents the results of our audit of the U.S. Postal Service's Software Inventory Management – Greater Boston District (Project Number 14WG015IT000). Our audit objective was to evaluate the effectiveness of the Postal Service's software inventory management practices in the Greater Boston District. See Appendix A for additional information about this audit.

Software asset management (SAM) provides processes for strategically tracking and managing software inventories, license agreements, and monitoring software assets. Effective SAM practices allow organizations to maintain an accurate inventory of their software assets and prioritize the use of information technology (IT) resources to improve accountability, security, and compliance.

The SysAdmin, Audit, Networking, and Security (SANS) Institute[1] ranks having an "Inventory of Authorized and Unauthorized Software" second on the list of the 20 most critical security controls. Management must monitor software assets frequently to ensure they are being appropriately managed and are able to detect the installation of unauthorized software.[2]

The Postal Service uses the Infrastructure Toolkit (ITK)[3] application to document all approved software products and has three classifications of software for the Advanced Computing Environment (ACE).[4] See the graphic below for a description of these classifications.

SOFTWARE CLASSIFICATIONS FOR ACE SYSTEMS Click on a category for details.

Source: Postal Service management.

All software products should be listed in the ITK prior to installation on the network. Without effective software management practices, organizations risk running unauthorized software, purchasing unnecessary licenses, and violating software license agreements.

1 The SANS Institute develops, maintains, and makes available, at no cost, the largest collection of research documents about various aspects of information security.
2 Software products that are not approved for installation on the network.
3 A repository of software implemented through the corporation. There are three classifications of software listed in the ITK: approved, restricted (approved use for a certain group of users), or obsolete/rejected.
4 ACE provides a standardized desktop environment for central management, minimizes local administration, and ensures that users have compatible tools.

Postal Service policies and procedures do not clearly define the software inventory management process for the Greater Boston District including roles and responsibilities, guidelines for maintaining software inventories, and removing unauthorized software.

Conclusion

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 identified 186 instances of unauthorized software products on 31 of the 161 computers we reviewed at the Boston and Middlesex Essex (ME) processing and distribution centers (P&DC).[5]

These circumstances occurred because the Enterprise-Wide Software Asset Management Controlling Authority[6] has not issued to districts detailed guidance for the software inventory management process. In addition, systems the Postal Service currently uses to manage the enterprise-wide software inventory at the district level are ineffective and fragmented across the organization. Proper controls over software assets allow organizations to identify systems running vulnerable and malicious software to help prevent attackers from gaining sensitive information and potentially compromising the network. Without appropriate controls and guidance from the controlling authority, the Greater Boston District cannot properly secure its information resources and is at increased risk of unauthorized access and disclosure of sensitive data.

Defining Software Inventory Management Processes

Postal Service policies and procedures do not clearly define the software inventory management process for the Greater Boston District. Specifically, there is no guidance on:

- Employee roles and responsibilities for managing software assets
- Methods and systems used to maintain software inventories
- Detecting and removing unauthorized software

The Enterprise-Wide Software Asset Management Controlling Authority established the TIPA approval process for obtaining authorization for all category three software products requiring local district management. However, this process is not documented in existing policy and was not distributed to Greater Boston District management. District IT personnel did not know how to access the ITK application to identify all existing software products approved for installation on the Postal Service network. In addition, Postal Service policy[7] and management instructions[8] only provide overarching guidance for software asset management and do not clearly define district responsibilities.

The software inventory management process is not clearly defined because the Enterprise-Wide Software Asset Management Controlling Authority did not make establishing a process for districts to follow a priority and relied, instead, on existing software management guidance. Without proper knowledge of and guidance for software asset management, the Greater Boston District is at increased risk of using unsecure software and potentially violating software license agreements.

---

5 We conducted our audit work at the Boston and ME P&DCs and the Salem Main Post Office (MPO); however, we did not identify unauthorized software at the Salem MPO.

6 A joint headquarters responsibility shared by the Postal Service's manager, IT Business Management, in Washington, DC; and the manager, IT Performance Achievement, in Raleigh, NC.

7 Handbook AS-805, *Information Security*, dated May 2014, includes assigning all personnel responsibility for sustaining accurate software inventories, maintaining an enterprise-wide software inventory, and ensuring the enterprise-wide software inventory management process provides appropriate documentation.

8 Management Instruction AS-820-2004-6, *The Advanced Computing Environment*, dated June 2014, provides an overview for the centralized management of ACE infrastructure and a standard software configuration. However, this instruction does not address all classifications of software residing on ACE systems and the various organizational units responsible for managing each software classification.

An accurate inventory of software installed at Greater Boston District facilities does not exist and 186 instances of unauthorized software products were identified across 31 systems.

Accuracy of Software Inventory

An accurate inventory of software installed at facilities in the Greater Boston District does not exist as required by policy.[9] We statistically selected and scanned 161 of 707 devices[10] at the three facilities we visited in the Greater Boston District. From this sample, we identified 186 instances[11] of unauthorized software products installed on 31 systems at two of the facilities and eight software products with inaccurate information in the ITK. The unauthorized software included FoxTab PDF Converter,[12] Price MetÃ©r,[13] and Unity Web Player[14] (see Table 2 for more details on the unauthorized software we identified). Table 1 shows the distribution of the 186 instances of unauthorized software products.

Table 1. Unauthorized Software by Facility

District Facility	Number of Instances of Unauthorized Software	Number of Systems
Boston P&DC	136	22
ME P&DC	50	9
Total	186	31

Source: U.S. Postal Service Office of Inspector General (OIG) GFI LanGuard and Nessus scanning tools.

Based on the sample results, 20 percent of the 161 systems we tested had unauthorized software installed. Given a 95 percent confidence and a plus or minus 7 percent precision level, we concluded that one or more unauthorized software products are installed on 137 of the 707 systems at the three Greater Boston District facilities.

This issue occurred because the Postal Service uses several ineffective methods and systems to manage and maintain its enterprise-wide software inventory, which is fragmented across the organization. Specifically:

- The Enterprise Architecture Committee uses the ITK application to capture all approved software products and versions that can be installed on systems connected to the network. The ITK is a manually intensive application that does not have automated processes for reconciling installed software to authorized listings. In addition, management determined that the ITK would not include certain approved software products, such as component software[15] associated with a main software product, drivers,[16] and Postal Service applications; however, this deviation is not documented in policy.

- IT Enterprise Access Infrastructure, Desktop Computing, manages the standard images approved and centrally deployed on ACE systems. This group also uses the System Center Configuration Manager to identify software installed on workstations; however, there is no automated process to compare this data with data in the ITK.

9 Handbook AS-805, Section 10-4.3.1, General Acquisition Policy, and Section 10-4.7.1, Corporate Software Inventory.
10 We focused our review on [redacted]
11 The 186 instances we identified related to 25 unique software products found on multiple devices.
12 An application used to install a printer on a computer system to convert documents to a pdf format.
13 An application used to identify the lowest prices when conducting online shopping.
14 An application used to build 3-D games with animated characters and graphics allowing users to play games on the web or as standalone players.
15 Software designed to work as a component of a larger application.
16 Software that allows a computer to communicate with hardware or devices. Without drivers, the hardware connected to a computer – such as a video card or printer – would not work.

Postal Service policy does not clearly define whether Engineering systems connected to the Mail Processing Equipment/ Mail Handling Equipment private network and the Postal Service's Managed Network Services must adhere to policy outlined in Handbook AS-805 regarding software inventory policies.

- The IT Performance Achievement, Capacity, and Performance Management Group oversees the configuration management database, which captures all software products installed on servers. However, there are no automated processes to reconcile installed server software to the ITK.

Without maintaining an accurate inventory of software assets, the Greater Boston District risks running unauthorized software products and potentially incurring fines for violating software license agreements. In addition, attackers continuously seek to exploit organizations with vulnerable versions of software.

During our audit, management upgraded 23 of the 31 systems to the ACE III standard build image, which removed unauthorized software products. While removal efforts continue, unauthorized software still remains on eight systems.

Other Matters

Engineering Software

Although not within the scope of this audit, during fieldwork it came to our attention that software policies for evaluating Engineering's Mail Processing Equipment/Mail Handling Equipment (MPE/MHE) are not clearly defined. Specifically, the Corporate Information Security Office (CISO) has not clearly identified the requirements for Engineering systems connected to the Postal Service's Managed Network Services (MNS) network.[17] Handbook AS-805 does not specify whether Engineering systems connected to the MPE/MHE's private network and the Postal Service's MNS must adhere to policy outlined in Handbook AS-805.[18]

As an industry best practice,[19] organizations should use standards to develop a software asset management model that fits their business operations and leverage existing resources to improve software governance. CISO has not prioritized establishing policy to clearly define the software management processes for Engineering systems connected to the Postal Service's MNS.

Without proper knowledge of and control over software asset management, the Postal Service cannot properly secure its information resources and is at increased risk of unauthorized access and disclosure of sensitive data.

17 The Postal Service uses [redacted]
18 Handbook AS-805-G, *Information Security for Mail Processing/Mail Handling Equipment,* dated March 2004, for the private network (10.X.X.X) provides that Engineering will determine the criteria and the use of all software products in the MPE/MHE. However, the handbook does not address MPE/MHE connected to the Postal Service MNS and the software requirements.
19 Gartner, *Improve Software Asset Management Governance With Standards and Best Practice Models*, dated May 2011.

Recommendations

We recommend management update policies to provide specific roles and responsibilities for managing the software inventory process, and provide instructions for detecting and removing unauthorized software to the Greater Boston District.

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

1. Update policies to provide specific roles and responsibilities for managing the software inventory process and provide instructions for detecting and removing unauthorized software to all districts.

2. Develop a process for identifying software products that should be added to the Infrastructure Toolkit and document any deviations.

3. Require district Information Technology personnel to access and review the Infrastructure Toolkit listing of all approved software products and follow the Technology Initiative Prioritization Assessment process prior to software installation.

4. Establish an automated process to reconcile the enterprise-wide inventory and detect unauthorized software on the network.

We recommend the acting vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to coordinate with the Greater Boston District manager to:

5. Remove unauthorized software identified on the Greater Boston District's network.

We recommend the acting chief information security officer and vice president, Digital Solutions:

6. Revise Handbook AS-805, Information Security, to clarify software inventory policies pertaining to Engineering systems connected to the Postal Service's Mail Processing Equipment/Mail Handling Equipment private network and Managed Network Services.

Management's Comments

Management agreed with recommendations 1 through 5 and disagreed with recommendation 6.

Regarding recommendations 1 through 5, management stated they will perform a holistic evaluation of software inventory management policies 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 updates necessary to reflect the changing needs of the organization. Management stated in subsequent communications that, as part of the holistic evaluation, they will clarify the policy regarding roles and responsibilities for identifying and removing unauthorized software on the Postal Service network. Management's target implementation date is December 31, 2016.

Regarding recommendation 6, management stated that they should update Handbook AS-805-G instead of Handbook AS-805. Management stated that they will revise Handbook AS-805-G, Section 3-4, Software, to clarify software inventory policies pertaining to Engineering systems connected to the Postal Service network and managed network services. In subsequent communications, management provided a target implementation date of July 2016.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1 through 5 and corrective actions should resolve the issues identified in the report. The OIG considers management's comments to recommendation 6 to be partially responsive.

Regarding recommendation 6, revising Handbook AS-805-G will partially correct the issue identified in the report. However, engineering equipment residing on the MNS (56.X.X.X) network must follow the policy outlined in Handbook AS-805. Therefore, any policy updates specifying software requirements for Engineering systems connected to the Postal Service's MNS should be added to Handbook AS-805.

The OIG considers recommendations 1, 5, and 6 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.

Appendices

Click on the appendix title to the right to navigate to the section content.

Appendix A: Additional Information 11
Background 11
Objective, Scope, and Methodology 11
Prior Audit Coverage 12
Appendix B: Instances of Unauthorized Software 13
Appendix C: Management's Comments 14

Appendix A: Additional Information

Background

Reliable software inventories are critical to effectively test, evaluate, monitor, and manage information system controls. SAM is considered a best practice that is necessary to appropriately track assets to determine what software programs are running on systems and optimize software across an organization. The Postal Service has an enterprise-wide software inventory to account for district assets and requires appropriate documentation of the software inventory management process.

Greater Boston District IT personnel are responsible for installing ACE software products in the standard build images on district systems, issuing devices to users, and providing hands-on support in the field. The majority of software management functions are centrally managed for ACE systems and governed by national policies.

As the owner of one of the largest civilian networks in the world, the Postal Service has about 125,000 desktop computers and 17,000 laptops. In 2014, the Postal Service's ITK application captured about 1,700 approved software products[20] authorized for use on district systems enterprise-wide. With an environment of this size, it is critical to maintain an accurate inventory of software assets.

Objective, Scope, and Methodology

Our objective was to evaluate the effectiveness of the Postal Service's software inventory management practices in the Greater Boston District. We selected this district for review based on the results of the OIG's 2014 IT Security Risk Model's identification of this district as the highest risk district for security events associated with IT assets.

Our audit focused solely on the results of our findings at three Greater Boston District facilities; however, current software management practices give the majority of software responsibilities to headquarters-level offices, so the Postal Service must make changes nationally rather than locally to address the issues identified in this report. We did not review controls over Engineering systems as part of this audit.

To accomplish our objective, we performed software scans at the Boston and ME P&DCs and the Salem MPO, interviewed personnel to evaluate software asset management practices, and analyzed and compared our results to the Postal Service's authorized software listings. We also evaluated processes for managing software assets, management's monitoring capabilities, and controls in place to detect the installation of unauthorized software on the network.

We performed onsite enumeration scans in October 2014 using Nmap[21] to identify all devices on the network at three Greater Boston District facilities. Our scans identified 1,522 devices connected to the Postal Service's [redacted] We removed devices with the role of printers, switches, routers; and other devices that cannot be scanned for installed software. Next, we selected a random statistical sample of 161 of 707 Windows systems (ACE workstations and laptops) to scan for installed software at the three district facilities.

We performed software scans in October 2014 using GFI LanGuard[22] and Nessus[23] to obtain the software products installed on the 161 systems in our sample. We obtained the software management requirements and current inventory listings of authorized

20 The ITK-approved software listing contains several approved versions of the same software products.
21 A scanning tool for network discovery and security auditing.
22 A network security scanner and patch management tool that can scan, detect, assess, and rectify security vulnerabilities.
23 A vulnerability and configuration assessment product that features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.

software products installed on these systems from Postal Service management, which included the ITK-approved software and ACE versions II and III standard build images. We compared our scan results to the Postal Service's records to determine the accuracy of its software inventories. We analyzed the results and reported them by facility.

We conducted this performance audit from September 2014 through July 2015; however, we suspended the project from November 2014 to February 2015 due to higher priority audit work.

We performed this audit in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on May 28, 2015 and June 2, 2015, and included their comments where appropriate.

We assessed the reliability of computer-processed data by performing automated testing. We assessed the reliability of ITK application data by using scripts in a MySQL database, reviewing existing information about the data, comparing data elements with other sources, and interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

We performed prior audit work for the *Management and Utilization of Software Licenses* (Report Number IT-AR-13-006, dated July 31, 2013). We did not identify monetary impact during this audit.

Appendix B: Instances of Unauthorized Software

Table 2 summarizes unauthorized software installed on systems at the Boston and ME P&DCs. We did not identify unauthorized software at the Salem MPO. The results were identified by the OIG GFI LanGuard and Nessus scanning tools on 31 of the 161 district systems we tested.

Table 2: Instances of Unauthorized Software

	Instances per Facility	
25 Unique Unauthorized Software Products	**Boston**	**ME**
HP SNMP Proxy	17	6
Delete Printer Object	17	6
EINST	17	6
Monitor Logon and Logoff	17	6
RDC	17	6
Windows Management Framework Core	17	6
Keyboard Layout Management Application	11	2
Driver Installer	8	1
Roxio 9	7	1
Adobe Acrobat Connect Add-in	2	0
Adobe AIR	1	0
AppNHost 1.0.5.1	1	0
FoxTab PDF Converter	1	0
Fuze Meeting	1	0
Scan	1	0
Unity Web Player	1	0
Paperport 9	0	1
HPUPD510_PCL6	0	2
Access Control System V5.1.5.4 Client	0	1
Internet Page Accelerator	0	1
Price MetÃ©r (remove only)	0	1
Qt	0	1
Speedial	0	1
Web Bar 2.0.5336.18408	0	1
WebDAV 7.5 For IIS 7.0	0	1
Total Instances	**136**	**50**

Source: OIG GFI LanGuard and Nessus scanning tool results.

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

June 25th, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Software Inventory Management – Greater Boston District (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 recommendations 1-5.

Recommendation [1]:
Update policies to provide specific roles and responsibilities for managing the software inventory process and provide instructions for detecting and removing unauthorized software to all districts.

Recommendation [2]:
Develop a process for identifying software products that should be added to the Infrastructure Toolkit and document any deviations.

Recommendation [3]:
Require district Information Technology personnel to access and review the Infrastructure Toolkit listing of all approved software products and follow the Technology Initiative Prioritization Assessment process prior to software installation.

Recommendation [4]:
Establish an automated process to reconcile the enterprise-wide inventory and detect unauthorized software on the network.

Recommendation [5]:
Remove unauthorized software identified on the Greater Boston District's network.

Management Response/Action Plan:
Management generally 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

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

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

Recommendation 6:
Revise Handbook AS-805, *Information Security*, to clarify software inventory policies pertaining to Engineering systems connected to the Postal Service's Mail Processing Equipment/Mail Handling Equipment private network and Managed Network Services.

Management Response/Action Plan:
Management disagrees with the recommendation. The correct handbook to reference is the Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment (MPE/MHE)* and not Handbook AS-805, *Information Security*. Section 3-4 Software, will be revised to clarify software inventory policies pertaining to Engineering systems connected to the Postal Service's network and managed network services.

[redacted]

Select software status on the left hand bar and it will show current, future, planned and other software versioning and deployment details as well. The ITK only shows software that is administrative .56 software, which has been a major disconnect during audits of MPE/MHE equipment because it is typically non-ace and operates primarily on the .10 network.

Target Implementation Date:
Management is requesting closure of this recommendation upon issuance of the final audit report.

Responsible Officials:
Vice President, Digital Solutions and CISO
Vice President, Engineering Systems

475 L'Enfant Plaza SW
Washington DC 20260-5000
WWW.USPS.COM

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

6/26/2015

Gregory S. Crabb
(A) Vice President, Digital Solutions and CISO

06/25/15

Michael J. Amato
Vice President, Engineering Systems

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

475 L'Enfant Plaza SW
Washington DC 20260-5000
WWW.USPS.COM

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100