OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Hardware Inventory Management– Greater Boston District

Audit Report

Report Number
IT-AR-15-004

March 25, 2015

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Management does not have an accurate inventory of hardware assets connected to the Postal Service network.

Background

An effective asset management process actively manages all hardware devices on a network, so that only authorized devices have network access, and allows for quick response to security events. Asset management consists of maintaining inventory, tracking assets, and updating records.

The U.S. Postal Service Office of Inspector General's (OIG) Information Technology (IT) Security Risk Model identified the Greater Boston District as the district with the highest risk for security events associated with information technology assets in Quarter 1, fiscal year 2014. Security events include adware, spyware, and computer viruses. If hardware affected by any of these events is not quickly physically located, postal operations may be disrupted. To respond effectively to security events, management must be able to physically locate assets. In 2014, the Greater Boston District managed about 12,000 information technology assets.

Our objective was to determine whether the Greater Boston District has an accurate inventory and processes to manage hardware assets connected to the Postal Service network.

What The OIG Found

Management does not have an accurate inventory of hardware assets connected to the Postal Service network. Specifically, management could not physically locate 49 of the 182 (27 percent) active systems sampled at the three facilities we visited. In addition, 33 network assets or 18 percent of our sample that we physically located had inaccurate and incomplete data in the Asset Inventory Management System. We also determined the inventory list of sensitive property (such as laptops, computers, and switches) is not reconciled with physical assets.

These circumstances occurred primarily because the Postal Service does not have a process to effectively track all IT assets and enforce existing policy. We estimated about $3.9 million for incomplete data in the Asset Inventory Management System and assets potentially at risk. Management needs an accurate and complete inventory to physically locate and disconnect a compromised or unauthorized device attached to the Postal Service network.

What The OIG Recommended

We recommended the Postal Service implement validation controls to the Asset Inventory Management System application and procedures to verify assets are authorized for connectivity before adding to the system. We also recommended management implement a scheduled inventory verification process for sensitive property and complete plans to prevent unauthorized devices from gaining access to the network.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 25, 2015

MEMORANDUM FOR: JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

RICHARD P. ULUSKI
VICE PRESIDENT, AREA OPERATIONS,
NORTHEAST AREA

E-Signed by Kimberly Benoit
VERIFY authenticity with eSign Desktc

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Audit Report – Hardware Inventory Management –
Greater Boston District (Report Number IT-AR-15-004)

This report presents the results of our audit of the U.S. Postal Service's Hardware Inventory Management – Greater Boston District (Project Number 14WG014IT000).

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

Table of Contents

Findings

Management could not physically locate 49 of the 182 (27 percent) active systems sampled at the three facilities we visited.

Introduction

This report presents the results of our audit of the U.S. Postal Service's Hardware Inventory Management - Greater Boston District (Project Number 14WG014IT000). Our objective was to determine whether the Greater Boston District has an accurate inventory and processes to manage hardware assets connected to the Postal Service network. See Appendix A for additional information about this audit.

Asset management is the process of tracking and managing the physical components of computers and network devices from acquisition through disposal. According to the SysAdmin, Audit, Networking, and Security (SANS) Institute,[1] "Inventory of Authorized and Unauthorized Devices" ranked first on the list of the 20 most critical security controls.

The goal of hardware asset management is to account for all hardware assets on the information technology (IT) infrastructure and to provide comprehensive inventory visibility. Specifically, this process should actively manage inventory by tracking assets and updating records to ensure that only authorized hardware devices have network access. Proper asset management results in effective maintenance and timely troubleshooting of network problems.

The U.S. Postal Service Office of Inspector General's (OIG) IT Security Risk Model identified the Greater Boston District as the highest risk district for security events associated with IT assets in Quarter 1, fiscal year 2014. Security events include adware,[2] spyware,[3] Trojans,[4] viruses,[5] and worms.[6] If hardware infected by any of these events is not quickly physically located, postal operations would be disrupted. In 2014, the Boston District managed about 12,000 IT assets.

According to the Enterprise Information Repository,[7] the Asset Inventory Management System (AIMS) is the official central repository for tracking IT assets. AIMS allows users to interactively query the asset database using a variety of search results to review, analyze, and maintain the Postal Service's network and non-network asset inventory.

Conclusion

Management did not have an accurate inventory of hardware assets connected to the Postal Service network in the Greater Boston District. Specifically, management could not physically locate 49 of the 182 active systems (27 percent) sampled at the three sites we visited. In addition, 33 network assets (18 percent) that we physically located had inaccurate and incomplete data in AIMS. Further, we found that network devices are entered into AIMS without verifying the devices are authorized for connection to the network. Finally, we determined management does not reconcile the sensitive property inventory listing (such as laptops, computers, and switches) with physical assets at the district level to ensure accountability. We estimated about $3.9 million for incomplete data in AIMS and assets potentially at risk.

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 that can track and view a user's personal information and provide it to third parties without the user's authorization or knowledge.
3 Software that conducts activities on a computer without the user's consent, including collecting personal information on a user.
4 Software programs that appear to be harmless but contain hidden code designed to exploit or damage a system. Hackers can transmit them through email messages, or use them to modify or destroy data or obtain confidential information.
5 Computer programs or scripts that attempt to spread from one file to another on a single computer and/or from one computer to another without the knowledge or consent of the computer user.
6 Specific types of viruses that spread across many computers through network connections, creating copies of themselves on the infected computers.
7 The Postal Service's database of record that maintains information about existing applications, toolsets, and data.

Thirty desktop computers were assigned to retired, former, or transferred employees who no longer controlled the assets.

Retired assets removed from the network were still documented as active in AIMS.

These conditions occurred because management has not developed standard operating procedures for documenting the physical location of these assets. Additionally, the Postal Service does not use an official centralized asset inventory management system to manage all IT assets connected to the network and enforce existing policy.[8] Furthermore, the Postal Service has not implemented a process to verify the existence of sensitive assets that are valued below the capital asset threshold. As a result, an unauthorized device could compromise operations or could be added to the network without detection. Similarly, sensitive assets could be lost or stolen without detection.

Management of Information Technology Assets

Management did not have an accurate inventory of hardware assets connected to the Postal Service network in the Greater Boston District. This occurred because the Postal Service has not developed a process to effectively track all IT assets. Without an accurate and complete inventory management system, the Postal Service may have difficulty promptly locating and disconnecting a compromised or unauthorized device attached to its network. This could limit the Postal Service's ability to troubleshoot and respond quickly to security events.

Hardware Not Physically Located

Based on our enumeration[9] scans, we sampled 182 assets connected to the Postal Service network at the three district facilities we visited. Management could not physically locate 49 of the 182 assets, and 18 of the 49 were not documented in any asset management system.

When management cannot physically locate network devices, it can be difficult to promptly respond to issues and recover operations. If a device were compromised, an attacker could install malware, steal information, corrupt data, and disrupt operations before management could physically locate and disconnect the device.

Inaccurate Asset Inventory

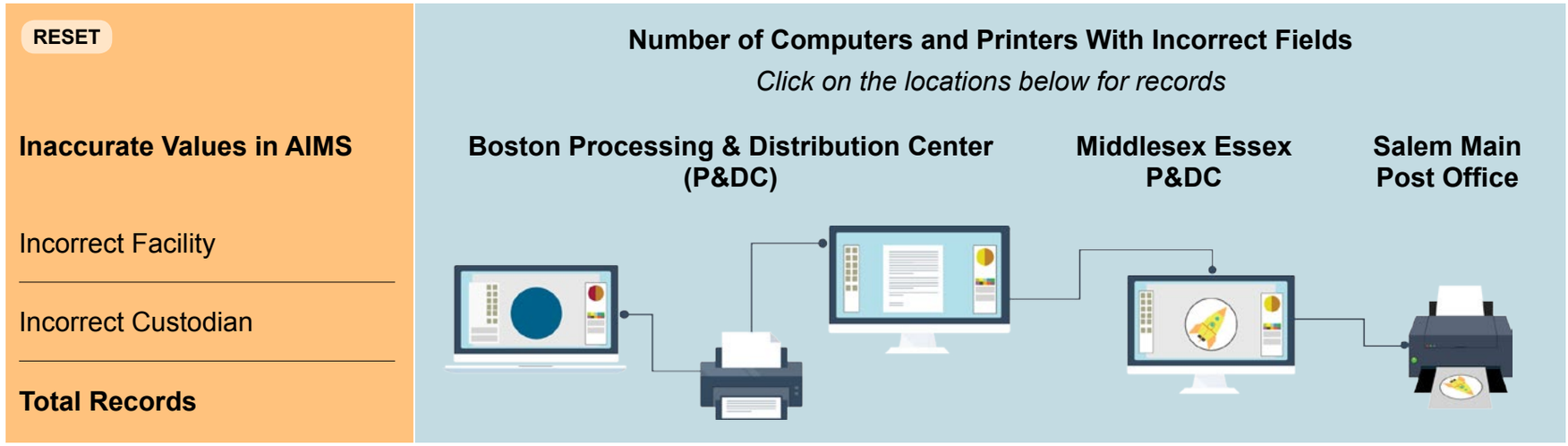
From our sample of 182 assets, we identified 33 with inaccurate and incomplete data recorded in AIMS. For example:

- We identified 30 desktop computers assigned to retired, former, or transferred employees who no longer controlled the assets.
- A computer and a printer connected to the network in the Greater Boston District were documented in AIMS as physically located in other cities.[10]
- We identified three active assets on the network that were [redacted].
- Retired assets removed from the network were still documented as active in AIMS.

Figure 1 summarizes the number of computers and printers with inaccurate data records that we identified in AIMS for the three facilities selected.

8 Handbook AS-805, *Information Security*, Section 10-4.7.2: Individual Information Resource Inventories, March 2014.
9 The method used to discover devices on the network.
10 According to AIMS, the computer was assigned to a facility in Oak Park, IL, and the printer was assigned to a facility in Los Angeles, CA.

Figure 1. Inaccurate Inventory Records



Source: AIMS.

These vulnerabilities occurred because there are no validation controls for more than 15 data sources uploaded into AIMS, nor a process to verify accuracy and completion of inventory records for hardware assets connected to the network. In addition, management stated that users are not consistently updating inventory records when assets are retired.

The lack of validation controls can cause duplicate or incomplete records in the inventory listing. Management needs accurate information to make sound financial and operational decisions. An inaccurate inventory system exposes the Postal Service to the loss or theft of its assets because it can be difficult to identify and physically locate a compromised device [redacted]

Asset Inventory Management System Data Analysis

Based on our analysis of extracts from the AIMS database, the Greater Boston District's asset records are incomplete. For example, 933 of 5,269 computers (17.7 percent) were missing serial number information.

Table 1 summarizes the number of computers, printers, and network devices with incomplete data records that we identified in AIMS for the Greater Boston District.

Table 1. Asset Records With Missing Information – Greater Boston District

	Type of Asset (Number of Records Reviewed)						
	Computers (5,269)		Printers (2,204)		Network Devices[11] (5,042)		Percentage of All Assets Reviewed[12]
Field Values Missing in AIMS							
Serial Number	933	17.7%	0	0.0%	3,675	72.9%	36.8%
Custodian	1,745	33.1%	558	25.3%	5,004	99.2%	58.4%
Manufacturer	2,163	41.1%	0	0.0%	3,754	74.5%	47.3%
Make/Model	2,162	41.0%	0	0.0%	3,708	73.5%	47.0%
Cost	2,279	43.3%	1,341	60.8%	5,042	100.0%	69.2%
Location	43	0.8%	80	3.6%	283	5.6%	3.0%

Source: AIMS.

As a result of our audit, management has re-established an automated process that updates the AIMS with newly discovered network devices. However, these network devices are added to AIMS without verifying the assets are authorized to be connected to the network.

The lack of asset accountability prevents responsible personnel from ensuring inventories are accurate and authorized. Consequently, an unauthorized device could be inadvertently added to the AIMS database. Although an asset can be discovered, it can be difficult to determine if the asset is authorized.

Inventory Verification and Reconciliation

Management did not verify the existence of sensitive property[13] against an official asset inventory management system at the district level, as required.[14] This is because management only performs asset verification for capital assets [redacted] and for sensitive property at headquarters facilities. Management has not established a process in the Greater Boston District to verify that all infrastructure components exist, as required by policy.[15]

Without proper knowledge and control of all the assets connected to the network, IT staff cannot properly secure those assets. In addition, an organization's systems are more vulnerable to loss, theft or attack when it lacks an accurate inventory. If an unauthorized person were to obtain a computer or network device, he or she may be able to access sensitive information, such as configuration files, passwords, or personally identifiable information, and could possibly disrupt mail operations.

11 Network devices include routers and switches connected to the network.
12 We computed this percentage by totaling the number of missing field values per category and dividing that number by the total number of assets (12,515) – computers (5,269), printers (2,204), and network devices (5,042) – in the Greater Boston District.
13 Property considered especially vulnerable to theft or loss, such as computers, digital cameras, camcorders, projectors, and other valuable portable equipment.
14 Handbook AS-701, *Material Management*, Section 541.26: Verification and Physical Inventory, January 2014.
15 Handbook AS-805, Section 11.3.2: Maintaining Network Asset Control, March 2014.

Network Authentication

Asset inventory control includes processes and tools to detect and manage all devices accessing the network. Organizations use tools to authenticate and authorize network assets. The Greater Boston District has not employed adequate asset inventory controls to [redacted].[16] Adequate controls have not been employed because management did not make it a priority to implement network access controls enterprise-wide.

Without asset inventory controls, an attacker or trusted user could attach an unauthorized device to the Postal Service network without detection. In addition, management may not be able to promptly address a security event originating from an unauthorized device if asset inventory controls are lacking.

16 [redacted].

Recommendations

We recommend management implement validation controls to the Asset Inventory Management System application to improve data integrity. We also recommend management implement a scheduled inventory verification process for sensitive property and complete plans to prevent unauthorized devices from gaining access to the network.

We recommend the vice president, Information Technology, direct the program manager, Asset Inventory Management System, to:

1. Implement validation controls to the Asset Inventory Management System application to improve data integrity.

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

2. Implement procedures to verify assets are authorized for network connectivity before Asset Inventory Management System records are added or modified.

3. Complete plans to implement controls to prevent unauthorized network devices from gaining access to the Greater Boston District network.

We recommend the vice president, area operations for the Northeast Area, direct the district manager, Greater Boston District, to:

4. Implement a scheduled inventory verification process to verify the existence of sensitive property at regular intervals, as required.

Management's Comments

Management agreed with recommendations 1, 3, and 4; and partially agreed with recommendation 2.

Regarding recommendation 1, management agreed that additional validation controls would provide improved data integrity to the AIMS application. The Postal Service will upgrade existing controls and develop new controls to help ensure the timely delivery of accurate and current tracking data to the AIMS system. Management's target implementation date is July 1, 2015.

Regarding recommendation 2, management stated that the Postal Service adds computers and printers to AIMS with the required field values via direct feed from the vendor; however, direct vendor feeds to AIMS is not available for telecommunications equipment. Management extracts data on telecommunications equipment from the network based on a point-in-time scan and extract. The Postal Service will develop a process to improve the quality of the data fed into AIMS to ensure that the system updates reflect the best data available about Postal Service assets. Management's target implementation date is July 1, 2015.

Regarding recommendation 3, management stated that they have already begun the corrective action to prevent access by unauthorized network devices by implementing CISCO ISE (Identity Service Engine). The implementation enables real-time device management on the network, including blocking capability to unauthorized devices. The capability is currently implemented at headquarters and the Raleigh, NC, campus. The last phase of implementation will be at the field sites and will require upgraded equipment. Management's target implementation date is September 30, 2017.

Regarding recommendation 4, management stated that they will issue a policy regarding inventorying hardware at specific intervals and against the AIMS application. Management's target implementation date is July 1, 2015.

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

Evaluation of Management's Comments

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

The OIG considers recommendations 2 and 3 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

Background

Asset management is the process of tracking and managing the physical components of computers and computer networks, from acquisition through disposal. The objectives of inventory control and asset management procedures include maintaining uniform accountability for assets. The primary responsibility for controlling assets rests with the officials to whom equipment is assigned. The material accountability officers are responsible for performing scheduled inventory verification for sensitive property and capital assets at headquarter facilities. The district material accountability officers perform inventory verification for capital assets only.

The Postal Service has about 125,000 desktop computers, 17,000 laptops, and 85,000 printers. The Greater Boston District has about 5,000 network devices, 5,000 desktop and laptop computers, and 2,000 printers. With this many devices, keeping an accurate inventory is critical.

Objective, Scope, and Methodology

Our objective was to determine whether the Greater Boston District has an accurate inventory and processes to manage hardware assets connected to the Postal Service network. To accomplish our objective, we performed enumeration scans at the Boston Processing and Distribution Center (P&DC), the Middlesex Essex P&DC, and the Salem Main Post Office; interviewed personnel; and analyzed and compared our results to the Postal Service inventory.

We performed on-site enumeration scans in October 2014 using Nmap[17] to obtain the inventory of devices on the Postal Service network. Our scans identified 1,522 assets connected to the Postal Service's 56.x.x.x network. As a result, we randomly selected 182 assets for our sample. We obtained an inventory listing of assets connected to the network in the Greater Boston District from AIMS, performed physical inventory reviews of select assets between October and November of 2014, and compared our results to the AIMS inventory. We analyzed the results and reported them by network devices, computers, and printers.

We conducted this performance audit from September 2014 through March 2015, 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 February 23, 2015, and included their comments where appropriate.

We assessed the reliability of AIMS data by performing electronic testing of required data elements, reviewing existing information about the data and the system that produced them, and interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

17 Scanning tool for network discovery and security auditing.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
Capital District Vulnerability Assessment	IT-AR-15-001	12/12/2014	None

Report Results: Our report determined that security controls in the Capital District did not adequately protect Postal Service infrastructure and data from unauthorized access or corruption. Specifically, we identified configuration vulnerabilities that included areas of non-compliance related to operating systems, intrusion protection, accounts, passwords, and logging. Further, administrators did not install the latest patch updates on systems and allowed remote access to network devices using unsecure communications that weaken network security. We made ten recommendations. Management agreed with nine of the recommendations and partially agreed with the other.

Appendix B: Management's Comments

RICHARD P. ULUSKI
VICE PRESIDENT, AREA OPERATIONS
NORTHEAST AREA

UNITED STATES POSTAL SERVICE

March 13, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Hardware Inventory Management – Greater Boston District
Report Number IT-AR-15-DRAFT

Northeast Area management agrees with each finding in the audit report.

Recommendation 4:
Implement a scheduled inventory verification process to verify the existence of sensitive property at regular intervals, as required.

Management Response
The Northeast Area agrees with the recommendation and will direct all Northeast Area Districts to fully implement the national Information Technology policy regarding inventory verification to verify the existence of sensitive property at regular intervals, as required.

Target Implementation Date:
Date established by national Information Technology policy.

Responsible Management Official:
Manager, Enterprise Access Infrastructure

Richard P. Uluski

cc: Manager, Corporate Audit Response Management

6 GRIFFIN ROAD NORTH
WINDSOR, CT 06006-7010
WWW.USPS.COM

JOHN T. EDGAR
VICE PRESIDENT
INFORMATION TECHNOLOGY

UNITED STATES POSTAL SERVICE

March 12, 2015

Lori Lau Dillard
Director, Audit Operations

SUBJECT: Hardware Inventory Management – Greater Boston District (Report Number IT-AR-15-DRAFT)

Recommendation [1]:
We recommend the vice president, Information Technology, direct the program manager, Asset Inventory Management System, to implement validation controls to the Asset Inventory Management System application to improve data integrity.

Management Response:
Management agrees that additional validation controls would provide improved data integrity to the AIMS system. The issues with data integrity in AIMS are rooted in the quality of the data provided to AIMS by the major feeder systems and on the reliance on the local hardware recipients to maintain that data through timely and accurate status and change reporting. To address this condition, existing controls will be updated and new controls will be developed to help ensure the timely delivery of accurate and current tracking data to the AIMS system. This will enhance the monitoring and tracking capabilities for physical assets.

Target Implementation Date:
July 1, 2015

Responsible Management Official:
Manager, Enterprise Access Infrastructure

Recommendation [2]:
We recommend the vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to implement procedures to verify assets are authorized for network connectivity before Asset Inventory Management System records are added or modified.

Management Response:
Management agrees in part with this finding. Today, computers and printers are added to the AIMS system via a direct file feed from the vendor (currently HP). This file arrives with the necessary data to populate all required fields with initial values. This is not the case for telecommunications equipment. In this case, direct vendor feeds are not available to AIMS. Data on telecommunications equipment is extracted from the network based on a point in time scan and extract. In this case, telecommunications equipment data integrity is based solely on what is connected to the network at the time of the scan. To address this, the process will be

improved or developed to improve the quality of the data feeding into AIMS. This action will ensure that AIMS updates reflect the best data available about Postal assets.

Target Implementation Date:
July 1, 2015

Responsible Management Official:
Manager, Enterprise Access Infrastructure

Recommendation [3]:
We recommend the vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to complete plans to implement controls to prevent unauthorized network devices from gaining access to the Greater Boston District network.

Management Response:
Management agrees with this finding. The corrective action to prevent access by unauthorized network devices has already begun. The solution centers on the [redacted] will enable real time device management on the network, including a tiered blocking capability for any devices found to be questionable or unauthorized. This capability is currently implemented in the Raleigh RITSC campus and in USPS Headquarters. Implementation is currently in-progress at the Eagan and San Mateo data centers, with the Merrifield and Bolger sites scheduled. Implementation for Field sites will be the last phase and will include mandatory upgrades of wireless LAN capabilities and switching.

Target Implementation Date:
September 30, 2017

Responsible Management Official:
Manager, Enterprise Access Infrastructure

Recommendation [4]:
We recommend the vice president, area operations for the Northeast Area, direct the district manager, Greater Boston District, to implement a scheduled inventory verification process to verify the existence of sensitive property at regular intervals, as required.

Management Response:
Management agrees with this finding. A policy will be issued regarding inventorying hardware at specific intervals and validating against the Asset Inventory Management System.

Target Implementation Date:
July 1, 2015

Responsible Management Official:
Manager, Enterprise Access Infrastructure

John T. Edgar
Vice President, Information Technology

cc: Mgr, Corporate Audit Response Management

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