OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

South Florida District Vulnerability Assessment

Audit Report

October 22, 2013

Report Number IT-AR-14-001

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

HIGHLIGHTS

October 22, 2013

South Florida District Vulnerability Assessment

Report Number IT-AR-14-001

BACKGROUND:

The U.S. Postal Service Office of Inspector General's risk modeling identified the South Florida District as the (b)(3):39 USC 410 (c)(2) based on collected data showing malicious software programs on district computer systems. These security incidents can damage information system hardware and software and affect the integrity, confidentiality, and availability of data.

The South Florida District serves more than 14 million customers, delivers mail to more than 3.1 million homes, and generates annual revenue of about $1.1 billion. Districts are responsible for adhering to U.S. Postal Service policies for maintaining and securing their information systems. The (b)(3):39 USC 410 (c)(2) Service Center is responsible for updating all South Florida District information systems, including installing security updates. Engineering personnel in (b)(3):39 USC 410 manage the applications supporting the mail processing environment in the district.

Our objective was to review security controls in the South Florida District to determine whether the infrastructure adequately protects Postal Service data.

WHAT THE OIG FOUND:

Security controls in the South Florida District did not adequately protect Postal Service data and infrastructure against potential corruption and unauthorized access. Of (b) Internet addresses that operated as servers, databases, and workstations at three mail processing plants, we found significant security control weaknesses on (b) of them. Administrators did not consistently install security updates (patches) and configure all operating systems and databases as required by policy.

In addition, servers used to (b)(3):39 (b)(3):39 in the mail were configured with an (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) Further, management did not ensure that all South Florida District personnel with access to computer resources completed required annual security awareness training.

These vulnerabilities could impact the security of information resources and the operation of critical mail processing equipment.

WHAT THE OIG RECOMMENDED:

We recommended management implement vendor recommendations for patching and Postal Service configuration standards, correctly configure the (b)(3):39 USC 410 (c)(2) and ensure personnel with access to Postal Service resources receive annual security awareness training.

Link to review the entire report

October 22, 2013

MEMORANDUM FOR: JAMES P. COCHRANE
ACTING CHIEF INFORMATION OFFICER AND
EXECUTIVE VICE PRESIDENT

JEFFREY C. WILLIAMSON
CHIEF HUMAN RESOURCES OFFICER AND
EXECUTIVE VICE PRESIDENT

MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

FROM: John E. Cihota
Deputy Assistant Inspector General
for Financial and Systems Accountability

SUBJECT: Audit Report – South Florida District Vulnerability Assessment (Report Number IT-AR-14-001)

This report presents the results of our audit of the U.S. Postal Service's South Florida District Vulnerability Assessment (Project Number 13WG003IT000).

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

Attachment

cc: Corporate Audit and Response Management

TABLE OF CONTENTS

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's South Florida District Vulnerability Assessment (Project Number 13WG003IT000). Our objective was to review security controls in the Postal Service's South Florida District to determine whether the infrastructure adequately protects Postal Service data. See Appendix A for additional information about this audit.

The U.S. Postal Service Office of Inspector General (OIG) prepares quarterly Information Technology (IT) Security Risk Models to provide stakeholders with a holistic view of security in their respective areas of responsibility. The model is an evaluation of data retrieved from the [redacted] identifying instances of security events[2] occurring on information systems at the district level. The Consolidated IT Security Risk Model for fiscal year (FY) 2012, Quarters (Q) 2-4,[3] and FY 2013, Q1 identified the South Florida District as the [redacted] regarding the number of security events. The South Florida District currently serves more than 14 million customers, delivering mail to more than 3.1 million homes, businesses, and Post Office boxes.

The security events identified include instances of adware,[4] spyware,[5] Trojans,[6] viruses,[7] and worms[8] on information resources at South Florida District facilities. Left uncorrected, these security events can damage information system hardware and software; impact the confidentiality, integrity, and availability of sensitive data; or cause complete system compromise of critical applications needed to process the mail.

---

[1] The [redacted] obtains security event data from antivirus solutions residing on computers at Postal Service district facilities. The data are used to prepare the risk models.

[2] The security events to generate these quarterly risk models are reported to the [redacted] and are malicious software programs obtained from antivirus solutions hosted on computers at Postal Service district facilities.

[3] The FY 2012 Q1 data was not used due to the security event activity only capturing a partial data set from December 7-31, 2011, based on hardware changes.

[4] Adware is advertising display software that requires users to view advertisements when the program is running and usually requires an active Internet connection to view advertisements through a web browser. This software can track and view a user's personal information, providing it to third parties without the user's authorization or knowledge.

[5] Spyware is software that conducts activities on a computer without the user's consent to include collecting personal information on a user. This software can degrade a computer's performance and violate a user's personal privacy.

[6] Trojans are software programs that appear to be harmless but contain hidden code designed to exploit or damage a system. They can be transmitted through email messages, modifying or destroying data and obtaining confidential information.

[7] Viruses are 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. They can be transmitted as attachments to an email message or in a downloaded file, causing damage to hardware, software, or data.

[8] Worms are specific types of viruses that spread across many computers through network connections, creating copies of itself in the computer's memory. These can occur without user interaction and have the ability to consume network or local resources and cause denial-of-service attacks.

Conclusion

Security controls surrounding the Postal Service's South Florida District do not adequately protect Postal Service infrastructure and data against potential unauthorized access or corruption. We identified (b) Internet Protocol (IP) addresses[9] at (b)(3):39 South Florida District facilities reviewed.[10] We selected (b) IP addresses for review based on their role as servers, databases, and workstations.[11] We identified an aggregate[12] of (b) critical and high-risk vulnerabilities on (b)(3):39 and (b)(3):39 USC 410 servers. In addition, we identified an aggregate of (b) database server high-risk vulnerabilities. These vulnerabilities are higher than expected compared to similar assessments performed at other Postal Service data centers and facilities.[13]

Administrators did not consistently patch (install approved security updates) and configure server operating systems and (b)(3):39 USC 410 (c)(2) with operating system security requirements. The Advanced Computing Environment (ACE)[14] workstations contained (b)(3):39 USC 410 (c)(2) vulnerabilities. (b)(3):39 USC 410 (c)(2)[15] contained an (b)(3):39 USC 410 (c)(2) Finally, only two of 1,244 ACE account holders received the required annual computer security awareness training. Implementing effective security controls increases the Postal Service's ability to detect and prevent a compromise that might impact the confidentiality, integrity, and availability of information resources and the continued operation of critical mail processing equipment.

Because of the significant number of vulnerabilities in the South Florida District infrastructure, we provided our raw results to system administrators for further assessment and corrective action. Contrary to our normal procedures, due to the number of vulnerabilities identified, we did not filter out false positives[16] or determine the root cause of each critical and high-risk vulnerability. We recognize that some of the identified vulnerabilities may be false positives and communicated our approach with the responsible managers and system administrators. Management agreed that further

---

[9] A numeric address assigned to a device on a computer network that uses the IP for communication.

[10] (b)(3):39 USC 410 (c)(2)
(b)(3):39 USC 410 (c)(2)

[11] We selected (b) IP addresses for review; however, we were unable to conduct vulnerability assessment scans on (b)(IP addresses.

[12] Some vulnerabilities may exist on multiple systems/applications.

[13] The *SAP Human Capital Management System Security Assessment* report (Report Number IT-AR-12-005, dated March 19, 2012) identified (b)(critical and high-risk operating system vulnerabilities on (b servers using the OIG (b)(3):39 scanning tool and (b)(3):39 database server high-risk vulnerabilities on five servers using the OIG AppDetective scanning tool. The *Web Server Security Assessment* report (Report Number IT-AR-13-004, dated March 4, 2013) identified (b) critical and high-risk operating system vulnerabilities on (b) servers using the OIG (b)(3):39 scanning tool.

[14] The Postal Service uses ACE to simplify, standardize, and efficiently manage its IT environment. ACE information systems are centrally managed and supported. Only approved standardized software packages are authorized.

[15] (b)(3):39 USC 410 (c)(2)
(b)(3):39 USC 410 (c)(2)

[16] A false positive is an alert although the reported problem may not actually exist. Vulnerability scanners use matching algorithms to detect known vulnerability signatures. In some situations, the scanner may encounter indicators of a security problem but without clear proof.

assessment and corrective action were needed. We will monitor the actions taken by management to address these vulnerabilities.

Operating System Vulnerabilities

System administrators in (b)(3):39 USC 410 (c)(2)[17] did not consistently patch and configure operating systems as required by policy.[18] None of the 11 (b)(3):39 USC 410 (c)(2) or three (b)[19] mail processing servers or workstations examined were current with recommended patches. Additionally, 15 (b)(3):39 USC 410 (c)(2) and three (b)(3):39 USC 410 (c)(2) servers did not meet standard configuration requirements based on Postal Service policy.[21]

Our review of the 11 (b)(3):39 USC 410 (c)(2) mail processing servers and workstations noted in Table 1 identified an aggregate[22] of (b) critical and high-risk patch vulnerabilities. This includes such vulnerabilities as (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) The (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) could allow an attacker to remotely execute malicious code when the user, running the vulnerable application, opens a file from an unsecured location. Correcting these vulnerabilities would assist in ensuring critical mail processing applications function as intended.

---

[17] Although the systems reside in the South Florida District, system administrators located in (b)(3):39 USC 410 (c)(2) manage the administration of all information systems supporting the mail processing environment residing in the district.

[18] Handbook AS-805, *Information Security*, (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

[19] We performed (b)(3):39 USC 410 (c)(2) vulnerability assessment scans on (b)(3):39 USC 410 (c)(2) servers (b)(3):39 USC 410 (c)(2) servers, and (b)(3):39 USC 410 (c)(2) workstations. However, we were unable to assess patching vulnerabilities on (b)(3):39 USC 410 (c)(2) servers and workstations. Results from (b)(3):39 USC 410 (c)(2) information systems, ACE workstations, were inconclusive due to the (b)(3):39 USC 410 (c)(2) blocking access to the scanning tools used by the OIG, one server did not provide sufficient privileges, and two servers did not provide user access from the network to conduct scanning.

[20] We performed (b)(3):39 USC 410 (c)(2) vulnerability assessment scans on (b)(3):39 USC 410 (c)(2) servers and workstations and (b)(3):39 USC 410 (c)(2) servers identifying configuration and compliance-related vulnerabilities.

[21] Handbook AS-805, (b)(3):39 USC 410 (c)(2)

[22] This total represents the number of single instances, by application, of identified vulnerabilities. Some vulnerabilities may exist on multiple systems/applications.

[23] (b)(3):39 USC 410 (c)(2)

[24] (b)(3):39 USC 410 (c)(2) (b)(3):39 U

[25] (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) This vulnerability could allow memory to be overwritten and the security manager to be bypassed, leading to application crashes and arbitrary code execution.

Table 1. Critical and High-Risk Vulnerabilities – (b)(3):39 USC 410 (c)(2)

Mail Processing System/Application	Number of Servers/ Workstations	Number of Vulnerabilities by System/Application
Server		
(b)(3):39 USC 410 (c)(2)	2	32
	1	17
	4	36
	3	187
Workstation		
(b)(3):39 USC 410 (c)(2)	1	95
Total	**11**	**367**

Source: OIG (b)(3):39 scanning tool results.

Our review of the three (b) mail processing servers noted in Table 2 identified an aggregate of (b) critical and high-risk patch vulnerabilities on three (b)(3):39 servers. For example, the (b)(3):39 USC 410 (c)(2) vulnerability could allow remote attackers to execute malicious code. See Tables 5 and 6, respectively, in Appendix C for more details on (b)(3):39 USC 410 (c)(2) vulnerabilities on each server.

Table 2. Critical and High-Risk Vulnerabilities – Linux Patches

Mail Processing System/Application	Number of Servers	Number of Vulnerabilities by System/Application
(b)(3):39 USC 410 (c)(2)	3	32

Source: OIG (b)(3):39 scanning tool results.

(b)(3):39 USC 410 (c)(2)

Our review of 20 configuration and compliance checks[32] on (b)(3):39 USC 410 (c)(2) mail processing servers and workstations noted in Table 3 identified an aggregate of 66 critical and high-risk vulnerabilities such as (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

Table 3. Critical and High-Risk Configuration and Compliance Vulnerabilities — (b)(3):39 USC 410 (c)(2)

Mail Processing System/Application	Number of Servers/ Workstations	Number of Vulnerabilities by System/Application
Server		
(b)(3):39 USC 410 (c)(2)	2	9
	2	18
	4	7
	2	5
	3	15
Workstation		
(b)(3):39 USC 410 (c)(2)	1	3
	1	9
Total	**15**	**66**[33]

Sources: OIG (b)(3):39 USC 410 (c)(2) scanning tool results.

Our review of 18 configuration and compliance checks[34] on three (b)(3):39 mail processing servers noted in Table 4 identified 13 critical and high-risk vulnerabilities such as (b)(3):39 USC 410 (c)(2)

Table 4. Critical and High-Risk Configuration and Compliance Vulnerabilities — (b)(3):39 USC

Mail Processing System/Application	Number of Servers	Number of Vulnerabilities by System/Application
(b)(3):39 USC 410 (c)(2)	3	13[35]

Sources: OIG (b)(3):39 USC 410 (c)(2) scanning tool results.

[32] The 20 configuration and compliance checks consisted of the categories of password management, audit policy, (b)(3):39 USC 410 (c)(

[33] This total represents the number of single instances, by application, of identified vulnerabilities. Some vulnerabilities may exist on multiple systems/applications.

[34] The 18 configuration and compliance checks consisted of the categories of (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

[35] This total represents the number of single instances, by application, of identified vulnerabilities. Some vulnerabilities may exist on multiple systems/applications.

These operating system vulnerabilities existed because:

- Some administrators were not aware of the current Postal Service hardening (security) standards, used legacy policies, or did not have access to the current standards.

- Administrators did not verify that patching and configuration of all information systems conform to standards to ensure appropriate IT security.

- Some information systems are running a (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) Thus, management made a business decision to continue to use the (b)(3):39 USC 410 (c)(2) based on higher priorities. Management informed us that network firewalls are in place, and they limit access to these information systems as a mitigating control.

- (b)(3):39 USC vendor recommended patches were installed automatically using (b)(3):39 USC (b)(3):39 USC 410 (c)(2) patching tool; however, administrators did not perform manual updates for patches not applied by the tool.

- One information system required the installation of a certain level of service pack before applying vendor recommended patches; however, the information system was (b)(3):39 USC 410 (c)(2)

- Some information system vendor recommended patches were identified since their last patch cycle.

- Management made a business decision not to (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) of some information systems. Installing these patches on (b)(3):39 USC 410 (c)(2) would not be (b)(3):39 USC 410 (c)(2) These systems must be compatible to support the mail processing environment. However, management is working to (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) environment for these information systems.

According to Postal Service policy,[37] servers directly connecting the MPE/MHE (b)(3):39 USC (b)(3):39 USC 410 (c)(2) must be hardened to the standards approved by the manager, Corporate Information Security Office (CISO). The servers examined during our audit reside on the Postal Service (b)(3):39 USC 410 (c)(2) therefore, we relied upon the hardening standards approved by CISO in conducting the vulnerability assessment.

[36] WSUS enables IT administrators to manage and implement the latest Microsoft product updates to computers that are running the (b)(3):39 operating system.
[37] Handbook AS-805-G, *Information Security for Mail Processing/Mail Handling Equipment (MPE/MHE)*, (b)(3):39 US (b)(3):39 USC 410 (c)(2)

In addition, the vulnerability assessment scans were conducted (b)(3):39 the Postal Service's (b)(3):39 USC 410 (c)(2) and, as a result, the vulnerabilities reported are (b)(3):39 USC 410 (c) (b)(3):39 USC 410 (c)(2) There is still a (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) However, since this network access is not (b)(3):39 USC 410 (c)(2) the exposure is significantly reduced.

Based on our audit, management took corrective action to reimage the ACE workstation identified in our FY 2012 Consolidated IT Security Risk Model that did not have the approved (b)(3):39 software installed. Management also applied some vendor recommended operating system patches.

(b)(3):39 USC 410 (c)(2) Vulnerabilities

Database administrators did not ensure (b)(3):39 USC 410 (c)(2) servers were patched, configured, and in compliance with Postal Service policy[38] and industry best practice.[39] We identified (b)(3):39 USC 410 (c)(2) on five (b)(3):39 USC 410 (c)(2) servers. For example, these servers were (b)(3):39 USC 410 (c)(2) (b)(3):39 dating back to (b)(3):39 USC 410 (c) Compliance related vulnerabilities we detected included (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

These operating system vulnerabilities existed because management determined that the (b)(3):39 USC 410 (c)(2) legacy system hosting four of the (b)(3):39 USC 410 (c)(2) servers is running (b)(3):39 USC and upgrading to newer versions of (b)(3):39 USC 410 (c)(2) on the database servers. As a result, management made a business decision (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

Unsecured (b)(3):39 USC could allow a person or malware to read, change, or delete files, accidentally or maliciously. See Table 7 in Appendix D for more details on (b)(3):39 USC 410 (c) (b)(3):39 USC server patching, configuration, and compliance high-risk vulnerabilities. To mitigate the risk, management plans to migrate the (b)(3):39 USC database servers from the (b)(3):39 USC 410 system to the (b)(3):39 USC 410 (c)(2)[41] which is compatible with newer versions of (b)(3):39 and will allow current vendor recommended patches to be applied.

---

[38] Handbook AS-805, (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

[39] (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

[40] (b)(3):39 USC 410 (c)(2) the correct planned route with the mail class and destination for each mailpiece.

[41] (b)(3):39 USC 410 (c)(2) collects data from all mail processing equipment in a facility allowing managers to balance equipment and staffing to workloads improving productivity.

(b)(3):39 USC 410 (c)(2) Vulnerabilities

Administrators did not ensure two (b)(3):39 machines were configured according to policy.[42] Specifically, two (b)(3):39 machines contained an anonymous (b)(3):39 USC 410 (c)(2) configured with (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) The account must allow users to interact with the web server to obtain a quick status of (b)(3):39 USC 410 (c)(2) in emergency situations (b)(3):39 USC 410 (c)(2) The current (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) that connects to the application's web server. Management is uncertain why (b)(3):39 USC 410 (c)(2) (b)(3):39 USC because the responsible programmers are no longer on the program. As a result, users (b)(3):39 USC 410 (c)(2)

Management agreed to (b)(3):39 USC 410 (c)(2) The CISO initiated a Computer Incident Response Team ticket to address the (b)(3):39 USC 410 (c)(2) (b)(3):39 USC

Security Awareness Training

Management did not ensure that all South Florida District personnel with access to Postal Service IT resources completed annual security awareness training.[43] During FY 2012, only two of 1,244 employees[44] (less than 1 percent) with an active ACE logon ID assigned to the (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) received security awareness training. This occurred because South Florida District management did not receive official notification that the *IT Security in a Wired World* training course was the required annual security awareness training implemented and approved by the CISO to meet this requirement. Before FY 2013, the Postal Service's Strategic Training Initiatives (STI)[45] mandating annual training requirements also did not include an information security course for completion by Postal Service personnel. CISO initiated the process to include the newly developed *IT Security: Our Shared Responsibility* training course in the FY 2013 STI to address this issue.

Postal Service executive management did not ensure that bargaining unit employees with access to Postal Service IT resources completed annual security awareness training as required by policy. While non-bargaining unit employees[46] were to complete the newly developed FY 2013 STI *IT Security: Our Shared Responsibility* training course, management did not require bargaining unit employees to take this course

---

[42] Handbook AS-805 (b)(3):39 USC 410 (c)(2)

[43] Handbook AS-805, (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

[44] Of 1,244 employees, 1,067 were bargaining unit employees. They are classified as career or non-career employees represented by a labor organization (union) that negotiates with management for wages, hours, and other terms and conditions of employment.

[45] STIs are an annual legal and regulatory compliance for training and guarantee that the field locations have funding available for training.

[46] Career non-bargaining positions are typically administrative, managerial, and technical. They are represented by management associations, which do not have collective bargaining rights.

because of the need to fund the workhours associated with this training. As a result, untrained users may not be aware of actions they can take to protect the Postal Service's data and resources, increasing the risk of users engaging in inappropriate web browsing, file exchanging, email viewing, or not reporting suspected incidents of security policy violations.

Two recent audit reports[47] identified continuing weaknesses in security awareness training nationwide. The *Security Awareness Training Program* audit report indicated the CISO information security awareness training program has not been effectively implemented across the agency. Only 3,878 of the more than 340,000 users (about 1 percent) nationwide completed the required initial and annual information security awareness training in FY 2011.

Based on this audit, we are asking management to revisit and address prior recommendations to clearly define the users required to take the mandatory information security awareness training and ensure these users receive the necessary computer security awareness training.

Additionally, based on this audit, the South Florida District initiated efforts to ensure bargaining and non-bargaining unit employees with computer access assigned to facilities within this district complete the *IT Security in a Wired World* training course. On October 26, 2012, management issued emails to the South Florida District Leadership Cluster managers instructing them to ensure all personnel with computer access completed the mandatory *IT Security in a Wired World* training course for FY 2013 in the Learning Management System (LMS).[48] This effort was to educate computer users on best practices in safeguarding Postal Service computer systems by September 30, 2013.

Recommendations

We recommend the vice president, Engineering Systems, direct the manager, Engineering Software Management, to:

1. Provide system administrators access to current hardening standards policies.

2. Conduct a thorough review of vendor recommendations for patching and Postal Service standards for configuration to ensure appropriate measures are taken to correct the significant number of identified vulnerabilities.

3. Develop a technical refresh plan for the engineering infrastructure that addresses (b)(3):39 USC 410 (c)(2)

[47] *Remote Access Controls* (Report Number IT-AR-11-008, dated September 14, 2011) and *Security Awareness Training Program* (Report Number IT-AR-12-008, dated June 25, 2012).
[48] LMS is the official repository for conducting training and tracking mechanism for course completion by Postal Service personnel.

4. Configure and patch operating systems according to Handbook AS-805, *Information Security,* requirements.

5. Review information system configurations in accordance with policy to ensure information systems remain configured according to security standards.

6. Configure and patch all database servers to ensure compliance with appropriate hardening standards for their configuration.

7. Determine the (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) and configure (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

We recommend the acting chief information officer and executive vice president, in coordination with the chief human resources officer and executive vice president:

8. Ensure all personnel with access to Postal Service resources receive annual security awareness training or provide a waiver for all personnel considered exempt from training.

Management's Comments

Management neither agreed nor disagreed with the findings but agreed with recommendations 1 through 3 and 5 through 7. In addition, management disagreed with recommendation 4 and neither agreed nor disagreed with recommendation 8. Management also stated that the report failed to filter out all false positives when conducting vulnerability assessment scans which inflated the actual number of identified vulnerabilities. Management agreed that some of the identified vulnerabilities are known and they accept the risks due to business decisions.

Specifically, for recommendations 1 and 2, management stated they will provide the latest hardening standards to all current system administrators and reinforce the process by communicating the standards to them. Management also will continue to evaluate vendor recommendations for patching and make a business decision on installing patches based on a risk benefit analysis. Management noted that their January 2012 Engineering Patch Management Process evaluates each upgrade to determine the impact to the system and mail processing operations. The target completion date for both recommendations was September 30, 2013.

To address recommendation 3, management stated they will develop a technical refresh plan for engineering infrastructure (b)(3):39 USC 410 (c)(2) (b)(3):39 based on a risk benefit analysis approach. The target completion date is November 30, 2013. Management also noted that, prior to the audit, they engaged suppliers of their processing equipment to determine the cost and benefit of upgrading (b)(3):39 USC 410 (c)(2) In many instances, the mail processing

equipment application software and hardware upgrades (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) and required for thousands of information systems.

In response to recommendation 4, management agreed to configure and patch operating systems according to Handbook AS-805-G for mail processing equipment. They added that the report only referenced compliance with Handbook AS-805, and the report vulnerabilities were based on vulnerability assessment scans conducted (b)(3):39 USC 410 (c)(2) and did not reflect an actual vulnerability from external threats. Management stated that Handbook AS-805-G provides specific guidance for the MPE and MHE residing inside Postal Service secure firewalls. They will continue to configure and patch operating systems according to Handbook AS-805-G for the computer systems and network ranges that manage, monitor, and control mail processing functions.

Regarding recommendations 5 and 6, management stated they will continue evaluating information system configurations to ensure they remain configured according to appropriate security standards. Further, management will continue to patch and configure (b)(3):39 USC 410 (c)(2) servers based on the specific application and perform a risk benefit analysis.

Regarding recommendation 7, management noted that, during the audit (on August 20, 2013) they removed (b)(3):39 USC 410 (c)(2) from the (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) and configured (b)(3):39 USC 410 (c)(2) accordingly. Therefore, management stated they have implemented this recommendation and are in compliance.

In response to recommendation 8, management agreed to enhance its process by issuing written annual requirements for security awareness training. Management added that Handbook AS-805 currently provides a mandatory security training requirement for all active ACE users. For FY 2013, management issued a requirement for all Postal Career Executive Service, Executive and Administrative Schedule, and OIG employees to view and acknowledge the current security awareness course in LMS. Management provided bargaining unit employees with ACE IDs with awareness training when hired through Link articles, Security Alerts, and screen banner information on a routine basis. Management noted that CISO will enhance its process by issuing written annual requirements for security awareness training and tracking based on the functional area and target population starting in FY 2014. The target completion date was October 1, 2013.

See Appendix E for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and corrective actions should resolve the issues identified in the report. Based on management's response, we agree to close recommendation 7 upon issuance of this report.

Regarding recommendations 1 and 2, we agree with management that the various processes they are implementing should resolve the issues identified. Providing all current system administrators with access to the latest hardening standards and thoroughly evaluating vendor recommendations for patching will address the significant number of report vulnerabilities and ensure that management appropriately patches and configures information systems according to security standards. We encourage management to prepare a waiver that (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) on the mail processing environment.

Regarding recommendation 3, we agree with management that developing a technical refresh plan for the Engineering infrastructure could reduce (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) The technical refresh plan also could work toward mitigating future occurrences of some of the significant vulnerabilities identified during the audit.

Regarding recommendation 4, we agree with management that, contrary to normal procedures, we did not filter out false positives based on the significant number of vulnerabilities in South Florida District infrastructure when compared to similar assessments performed at other Postal Service data centers and facilities. We recognized that some of the identified vulnerabilities may be false positives and communicated our approach to the responsible managers and system administrators and in the report body. We also provided our raw results to system administrators for further assessment and corrective action. Management agreed that further assessment and corrective action were needed.

Additionally, Handbook AS-805-G states that servers directly connecting the MPE/MHE private network to the (b)(3):39 USC 410 (c)(2) must be hardened to the standards approved by the manager, Corporate Information Security. The servers examined during our audit reside on the MNS (b)(3):39 USC 410 (c)(network; therefore, we used the hardening standards approved by CISO (Handbook AS-805) in conducting the vulnerability assessment.

Regarding recommendations 5 and 6, we agree with management continuing to evaluate information system configurations to ensure they remain configured according to security standards and ensuring that they patch and configure (b)(3):39 USC 410 (c)(2) servers according to policy. We encourage management to work with the CISO in ensuring that

the security guidance in Handbook AS-805-G fully meets Postal Service policy for private networks that connect to the Postal Service's larger intranet.

The OIG considers recommendations 3, 7, and 8 significant and, therefore, requires OIG concurrence before closure. Management completed corrective action for recommendation 7 so that recommendation can be closed in the audit tracking system. Consequently, the OIG requests written confirmation when corrective actions are completed for recommendations 3 and 8. 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.

Appendix A: Additional Information

Background

The Postal Service provides customer service and manages its operations, including mail processing and distribution, in seven geographical areas and 67 districts. The South Florida District, located in the Southern Area, serves more than 14 million customers, delivering mail to more than 3.1 million homes, businesses, and post office boxes. The South Florida District mail processing facilities generate annual operating revenue of about $1.1 billion. The South Florida District has five mail processing plants, three of which were within our review:

- (b)(3):39 USC 410 (c)(2)
-
-

Districts must adhere to Postal Service policies in maintaining and securing their information systems. This responsibility includes local district IT personnel managing network infrastructure and information systems within these three facilities. They handle requests for all website access, oversee setting up user workstations received from the (b)(3):39 USC 410 (c)(2) Service Center and perform migrations to transfer user data from one machine to another.

The (b)(3):39 USC 410 (c)(2) Service Center is responsible for updating all South Florida District information systems, including installing system patches, updating system configuration, monitoring antivirus scan results, and seeking support from local district IT staff when needed. Engineering personnel in (b)(3):39 USC 410 (c)(2) manage the administration of all applications supporting the mail processing environment residing in the South Florida District.

Objective, Scope, and Methodology

Our objective was to review security controls in the Postal Service's South Florida District to determine whether the infrastructure adequately protects Postal Service data. To accomplish our objective, we prepared the FY 2012 Consolidated IT Security Risk Model trending security events. The model identified the South Florida District as the (b)(3):39 USC 410 (c)(2) We

presented the IT Security Risk Model results to South Florida District management and evaluated their process for securing and managing their information resources.

We performed an (b)(3):39 USC 410 (c)(2) using (b)(3):39 USC 410 (c)(2) during our survey to evaluate the South Florida District's entire information systems environment residing within the (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 After excluding network devices and printers, we identified (b)(3):39 USC 41 IP addresses within these facilities.

We evaluated unique hardware codes[51] known to host potentially vulnerable operating systems, and identified (b) of the (b)(3):39 IP addresses for review. Using data from our FY 2012 IT Security Risk Model, we also selected (b) ACE workstations, (b) within each facility, that had the highest number of security events. Therefore, our judgmental sample comprised (b) IP addresses for information systems at the three selected facilities.

Based on the survey results, we attempted to perform a vulnerability assessment to identify patch[52] and configuration related vulnerabilities using (b)(3):39 USC 410 (c)(and (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) scanning tools on the (b) IP addresses. (b) of the (b) IP addresses contained (b)(3):39 USC 410 (c)(2) servers, which required the (b)(3):39 USC 410 (c) scanning tool. However, we did not evaluate (b) IP addresses (b)(3):39 USC 410 (c)(2)
(b)(3):39 USC 410 (c)(2)
(b)(3):39 We performed vulnerability assessment scans on 19 (b)(3):39 information systems and three (b)(3):39 information systems residing at the (b)(3):39 USC 410 (c)(2)
(b)(3):39 USC 410 (c)(2)

Our scan results for five of 19 (b)(3):39 USC 410 (c)(2) information systems, ACE workstations, were inconclusive for assessing patch vulnerabilities due to the (b) [6] blocking access to the scanning tools used by the OIG. Implementing the (b) provides enhanced security over ACE workstations to monitor network traffic to prevent unauthorized access, which was effective when the OIG attempted to access these workstations.

---

[49] (b)(3):39 USC 410 (c)(2)
[50] (b)(3):39 USC 410 (c)(2)
[51] (b)(3):39 USC 410 (c)(2)
(b)(3):39 USC 410 (c)(2)

[52] Install updates released by software vendors.
[53] A vulnerability and configuration assessment product that features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.
[54] A network security scanner and patch management tool that can scan, detect, assess, and rectify security vulnerabilities.
[55] A network-based discovery and vulnerability scanner that discovers database applications within the infrastructure and assesses their security controls. It scans databases for vulnerabilities, configuration issues, weak passwords, missing patches, access controls, and other issues that could compromise the system or its data.
[56] (b)(3):39 USC 410 (c)(2)
(b)(3):39 USC 410 (c)(2)

We interviewed appropriate personnel[57] to determine whether all South Florida District system users with access to Postal Service resources at the three facilities completed annual security awareness training for FY 2012. The South Florida District Human Resources Office and CISO provided employee records of all assigned personnel, provided LMS security awareness training reports, and identified active ACE logon IDs for employees assigned to each facility. The audit team analyzed the information and performed 100 percent testing of the data in a MySQL[58] database. We used the results to identify all South Florida District personnel with access to Postal Service resources that received annual security awareness training at the three selected facilities.

We conducted this performance audit from October 2012 through October 2013 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 August 1, 2013, and included their comments where appropriate.

We assessed the reliability of computer-processed data by performing automated testing. We assessed the reliability of South Florida District employee records, LMS training records, and CISO ACE logon ID data by performing 100 percent testing of the data using scripts in a MySQL database. We determined the data were sufficiently reliable for the purposes of this report.

[57] Personnel included South Florida District management, Human Resources Office, LMS executives, and the CISO.
[58] MySQL is a free, downloadable version of the world's most popular open source database.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
Security Awareness Training Program	IT-AR-12-008	6/25/2012	None
Report Results:			
(b)(3):39 USC 410 (c)(2)			
Remote Access Controls	IT-AR-11-008	9/14/2011	None
Report Results:			
(b)(3):39 USC 410 (c)(2)			

Appendix B: Other Impacts

Recommendation	Impact Category	Amount
1, 3, 4, 5, and 6	IT Security[59]	None

[59] Computer software, networks, and data that are vulnerable or at risk of loss because of fraud, inappropriate or unauthorized disclosure of sensitive data, or disruption of critical Postal Service operations and services.

Appendix C: (b)(3):39 USC 410 (c)(2) Patching Vulnerabilities

Table 5 summarizes all (b)(3):39 USC 410 (c)(2) system patching critical and high-risk vulnerabilities for the South Florida District (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) The results were provided by the OIG (b)(3):39 USC 410 (c)(2) scanning tool on 11 (b)(3):39 USC 410 (c)(2) servers and workstations tested.

Table 5. (b)(3):39 USC 410 (c)(2) Vulnerabilities

Device	Number of Vulnerabilities[60]		
	Critical	High	Total
Server			
(b)(3):39 USC 410 (c)(2)	6	25	31
	6	26	32
	13	4	17
	15	20	35
	15	20	35
	15	20	35
	16	20	36
	25	162	187
	14	86	100
	14	86	100
Workstation			
(b)(3):39 USC 410 (c)(2)	16	79	95
Total	**155**	**548**	**703**

Source: OIG (b)(3):39 scanning tool results.

Table 6 summarizes (b)(3):39 USC 410 (c)(2) system patching critical and high-risk vulnerabilities for the South Florida District (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) The results were provided by the OIG (b)(3):39 USC 410 (c)(2) scanning tool on three (b)(3):39 USC information systems tested.

[60] The (b)(3):39 USC 410 (c)(2) provides the severity levels of information system vulnerabilities, associated impact, and remediation activities.
[61] Our vulnerability assessment scans identified applications associated with more than one system; therefore, we used numeric values to identify applications with several information systems.

Table 6. Vulnerabilities – (b)(3):39 USC 410 (c)(2)

Server	Number of Vulnerabilities		
	Critical	High	Total
(b)(3):39 USC 410 (c)(2)	4	28	32
	3	28	31
	4	28	32
Total	**11**	**84**	**95**

Source: OIG (b)(3):39 scanning tool results.

Appendix D: (b)(3):39 USC 410 (c)(2) Vulnerabilities

Table 7 summarizes (b)(3):39 USC 410 (c)(2) patching, configuration, and compliance high-risk vulnerabilities for the South Florida District (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2) The results were provided by the OIG (b)(3):39 USC 410 (c)(2) scanning tool on five (b)(3):39 USC 410 (c)(2) supporting the (b)(3):39 USC 410 and (b)(3):39 USC 410 (applications.

Table 7. Vulnerabilities – (b)(3):39 USC 410 (Databases

Application	Number of High-risk Vulnerabilities
(b)(3):39 USC 410 (c)(2)	111
	122
	122
	124
	123
Total	**602**

Source: OIG (b)(3):39 USC 4 scanning tool results.

Appendix E: Management's Comments

UNITED STATES POSTAL SERVICE

August 22, 2013

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Draft Audit Report – South Florida District Vulnerability Assessment (Report Number IT-AR-13-DRAFT)

Thank you for the opportunity to review and comment on the subject draft audit report. The Postal Service considers matters of computer security seriously. We are in agreement with some of the recommendations and responded accordingly in the attachment.

The subject report and this response contain information related to potential security vulnerabilities that, if released, could be exploited and cause substantial harm to the U.S. Postal Service. The manager, Corporate Information Security will determine what portions of the report should be considered as classified, restricted, and exempt from disclosure under the Freedom of Information Act.

If you have any questions or comments regarding this response please contact John Keegan, at (703) 280-7230.

Ellis A. Burgoyne
Chief Information Officer
and Executive Vice President

Jeffrey C. Williamson
Chief Human Resource Officer
and Executive Vice President

Michael J. Amato
Vice President, Engineering Systems

Attachement

cc: Ms. Brennan
Mr. Edgar
Ms.Feindt
Mr. Keegan
Ms. Fernandez
Corporate Audit and Response Management

South Florida District Vulnerability Assessment
Report Number IT-AR-13-DRAFT, Project Number 13WG003IT000
Page -2-

General Comments

The report fails to filter out all false positives which showed up on system scans, which inflates the actual number of vulnerabilities. Additionally, some of the vulnerabilities are known and accepted risks due to business decisions:

- 2 of 5 (b)(3):3 updates were in fact installed and completed, but not registered by the scanning tool used for this audit.
- The remaining 3 of 5 Operating System updates were not identified as being necessary by (b)(3):39 USC 41 update tool.
- The (b)(3):39 USC updates identified as missing were (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (c)(2)

The report only references compliance with Handbook AS-805 standards. In March of 2004, a separate standard Handbook AS-805G was established specifically for mail processing equipment (MPE) and mail handling equipment (MHE) that reside inside the Postal Service's secure firewalls. The fact that most of the equipment is in a closed intranet mitigates the risk of malware threats. The report findings were based on tests run within the USPS firewall and does not reflect the actual vulnerability from external threats.

Recommendations
We recommend the vice president, Engineering Systems, direct the manager, Engineering Software Management, to:

1. Provide system administrators access to current hardening standards policies

Management Response: Management agrees with this recommendation and will provide the hardening standards to all current system administrators. These standards are included in all of our core contracts with suppliers. This process will be reinforced by communicating it to all system administrators.

Target Implementation Date: September 30, 2013

Responsible Official: (b)(6)

2. Conduct a thorough review of vendor recommendations for patching and Postal Service standards for configuration to ensure appropriate measures are taken to correct the significant number of identified vulnerabilities.

Management Response: Management agrees with this recommendation and will continue to evaluate vendor recommendations for patching and make a business decision based on a risk benefit analysis. The current patch management process established is used to constantly evaluate any upgrades. As indicated in the January 2012 Engineering Patch Management Process, each upgrade gets evaluated to determine the impact to the system. Due to the complex interaction of the operating system and the integrated machine control application, patches must be carefully tested. If patches are approved, an implementation and deployment plan are developed to minimize the cost and impact to mail processing operations.

Target Implementation Date: September 30, 2013

Responsible Official: (b)(6)

3. Develop a technical refresh plan for the Engineering infrastructure that addresses (b)(3):39 (b)(3):39 USC 410 (c)(2)

Management Response: Management agrees with this recommendation and will continue the development of a refresh plan for the infrastructure to address any (b)(3):39 USC 410 (c)(2) (b)(3):3 The plan will be based on risk benefit analysis. A comprehensive list of the plan for all systems is maintained by our Software Process Management group.

Prior to this audit, Engineering Systems has engaged the suppliers of all our processing equipment to determine the cost and benefit of upgrading our operating systems to the current platforms. Many instances require a costly hardware upgrade to thousands of computers. Given the current financial state of the Postal Service, we objectively determine if the cost justifies the benefit.

Engineering Systems proactively evaluates the security concerns regarding (b)(3):39 USC 410 (c) (b)(3):39 USC 4 at the processing centers. In January 2013, a (b)(3):39 U risk analysis was performed. The analysis projected minimal cost associated with a malware infection compared to the high cost of the application software and hardware upgrades of MPE.

Target Implementation Date: November 30, 2013

Responsible Official: (b)(6)

4. Configure and patch operating systems according to Handbook AS-805, *Information Security*, requirements.

Management Response: Management disagrees with this recommendation. We will continue to configure and patch operating systems according to the Handbook AS-805G for the computer systems and networks that manage, monitor, and control mail processing functions; collect workload statistics from the MPE/MHE environment; and transmit control data or production statistics between the MPE/MHE environment and other Postal Service information systems.

Target Implementation Date: Not applicable

Responsible Official: (b)(6)

5. Review information system configurations in accordance with policy to ensure information systems remain configured according to security standards.

Management Response: In accordance with Handbook AS-805G, Management agrees and will continue to evaluate information system configurations and ensure the units remain configured according to the appropriate security standards.

Target Implementation Date: On-going

Responsible Official: (b)(6)

6. Configure and patch all database servers to ensure compliance with appropriate hardening standards for their configuration.

Management Response: Management agrees with this recommendation and will continue to configure and patch the data base servers based on the specific application and a risk benefit analysis.

Target Implementation Date: On-going

Responsible Official: John Keegan

7. Determine the minimum privileges necessary for the (b)(3):39 USC 410 (c)(2) (b)(3):39 USC 410 (to function and configure (b)(3):39 USC 4 accordingly.

Management Response: Management agrees with this recommendation and has already implemented the necessary correction. The change removes the administrative privileges from the (b)(3):39 USC 410 (c)(2)

Target Implementation Date: August 20, 2013

Responsible Official: (b)(6)

We recommend the chief information officer and executive vice president, in coordination with the chief human resources officer and executive vice president:

8. Ensure all personnel with access to Postal Service resources receive annual security awareness training or provide a waiver for all personnel considered exempt from training.

Management Response: Currently AS-805 has a mandatory security training requirement for all active ACE users. For 2013 a requirement was issued for all PCES, EAS, and OIG employees to view and acknowledge the current Security Awareness course in the Learning Management System. Bargaining unit employees having ACE IDs are provided security awareness training when hired, through Link articles, Security Alerts, and screen Banner information on a routine basis.

CISO will enhance its process by issuing written annual requirements for the Security Awareness training and tracking based on functional area and target populations. This new process will commence with FY2014.

Target Implementation Date: October 1, 2013

Responsible Official: (b)(6)