OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

AUDIT REPORT

Wireless Local Area Network Deployment and Security Practices

April 24, 2014

Report Number IT-AR-14-005

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

HIGHLIGHTS

April 24, 2014

Wireless Local Area Network Deployment and Security Practices

Report Number IT-AR-14-005

BACKGROUND:

The U.S. Postal Service is committed to providing a high quality, secure, and cost-effective telecommunication infrastructure that includes a wireless local area network. This network helps link about 32,000 facilities and enable communication among hundreds of thousands of employees and systems. The Postal Service is expanding its wireless infrastructure to provide mobile connectivity in delivery units to support new applications and enhance its competitiveness in the package delivery business.

Wireless technology offers multiple benefits such as increased mobility and ease of use; however, wireless networks are easy to compromise if improperly installed, increasing the risk that the confidentiality, integrity, and availability of information systems and data will be compromised. Attackers who gain unauthorized access to wireless networks can obtain sensitive information, conduct fraudulent activities, harm networks and systems, and disrupt operations.

Our objectives were to determine whether the Postal Service has effective security policies and controls in place to detect unauthorized use of and access to its wireless network, and whether the expansion plans for its wireless infrastructure follow established policy and security standards. The vice president, Information Technology, requested this audit.

WHAT THE OIG FOUND:

We determined the Postal Service implemented adequate security policies and controls that effectively detect unauthorized use of and access to its wireless network. Specifically, the Postal Service has configured its wireless controller devices and access points to continuously monitor and detect unauthorized access.

Our wireless network discovery scans at all five facilities we reviewed did not identify any wireless access points that we considered a threat to the network, such as those installed without the network administrator's consent.

In addition, the current expansion plans for the wireless infrastructure follow established policy and security standards, and security procedures in place are effective to ensure new wireless technologies are authorized, evaluated, and assessed prior to deployment.

WHAT THE OIG RECOMMENDED:

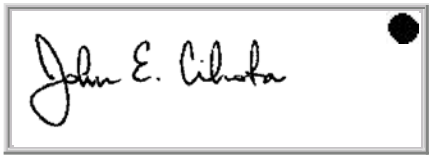
Because the Postal Service has effective security policies and controls for managing its wireless network infrastructure and technology, we are not making any recommendations.

Link to review the entire report

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

April 24, 2014

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



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

SUBJECT: Audit Report – Wireless Local Area Network Deployment and Security Practices (Report Number IT-AR-14-005)

This report presents the results of our audit of the U.S. Postal Service's Wireless Local Area Network Deployment and Security Practices (Project Number 13BG021IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Sean D. Balduff, acting 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 audit of the U.S. Postal Service's Wireless Local Area Network (WLAN) Deployment and Security Practices (Project Number 13BG021IT000). Our objectives were to determine whether the Postal Service has effective security policies and controls to detect unauthorized use of and access to its wireless networks and to determine whether the approved expansion plan for its wireless infrastructure follows established policy and security standards. The vice president, Information Technology, requested we review the Postal Service's WLAN. See Appendix A for additional information about this audit.

The Postal Service has an extensive data and voice telecommunication infrastructure that links about 32,000 facilities and enables communication among hundreds of thousands of employees and systems. This infrastructure includes communication networks and organization-wide computing systems. The communication networks include WLAN, local area networks (LAN), Internet,[1] Intranet,[2] Extranet,[3] Virtual Private Networks (VPN),[4] and all landline and wireless voice and data communication services.

To enhance its competitiveness in the package delivery business, the Postal Service implemented the Delivery Unit Infrastructure Technology (DUIT) Program.[5] This program expands wireless network capabilities at delivery units to provide mobile connectivity for several applications currently scheduled for deployment. Under this program, the Postal Service will install 18,857 wireless access points (AP)[6] at 11,857 delivery units. The expansion will provide key technologies necessary for successful implementation of Delivery, Results, Innovation, Value and Efficiency (DRIVE) Initiative 43, Build a World-Class Packaging Platform, and DRIVE Initiative 20, Achieve 100 Percent Product Visibility.

Conclusion

The Postal Service has effective security policies and controls that detect unauthorized access to its wireless network,[7] and the current expansion plans for its wireless infrastructure follow established policy and security standards.[8] To provide network and data security against unauthorized access and attacks,[9] the Postal Service

[1] A worldwide system of computer networks.
[2] A private network contained within an organization and only accessible by the organization's employees.
[3] A private network that shares part of an organization's information or operations with suppliers, customers, or vendors.
[4] VPN encrypts data sent through the network.
[5] Decision Analysis Report, DUIT Program, October 9, 2013.
[6] A device that allows wireless devices to connect to a network.
[7] Handbook AS-805, *Information Security*, Section 11, Network Security, dated May 2013.
[8] Handbook AS-805, Section 11, and Handbook AS-805-D, *Information Security Network Connectivity Process,* dated September 2009.
[9] A network attack occurs when an attacker or hacker uses certain methods or technologies to use, corrupt, or steal data for malicious purposes.

implemented standardized configurations for its wireless network APs. To improve wireless network monitoring, the Postal Service implemented a [redacted] that detects unauthorized access, unauthorized configuration changes, and other security incidents. Finally, to protect the network infrastructure, the Postal Service has effective security policies in place to ensure new wireless technology is authorized, evaluated, and assessed before deployment.

Effective security controls increase the probability the Postal Service will detect and prevent unauthorized access to its network that could impair the confidentiality, integrity, and availability of information systems and data.

Wireless Local Area Network Security Policies and Controls

Our audit determined that controls over the wireless network and technology were generally in place and effective. Specifically:

- Wireless networks and APs are configured to monitor and detect unauthorized use and access. The Postal Service uses a [redacted] to centrally manage and configure its wireless network and [redacted]. Integrated configuration templates are used to apply common and best-practice configuration settings for encryption, authentication, authorization, and accounting.

- We conducted wireless network scans at five facilities[13] to detect rogue APs.[14] We identified [redacted] out of [redacted] total APs that were not on the approved inventory list.[15] After further analysis, we discovered that [redacted] of the unknown APs were [redacted]. We validated that the [redacted] were [redacted] an approved Postal Service AP and did not pose a security threat. We analyzed the remaining [redacted] unknown APs and determined they were not rogue APs. For example, these APs included mobile hotspots[18] and the APs of surrounding businesses. Therefore, they did not pose a risk to the network infrastructure. See Table 1 for details of this analysis.

[redacted] Raleigh, NC, Processing and Distribution Center (P&DC); [redacted] St. Paul, MN, P&DC; Minneapolis, MN, P&DC, and the [redacted].

Any wireless AP that has been installed on a network's wired infrastructure without the consent of the network administrator or owner.

[15] Inventory listing of all APs connected to the Postal Service network as of November 25, 2013.

[16] A secondary Wi-Fi hotspot created within a physical AP.

[17] The ability of a computer application or product to continue to function well when its size or volume is changed to meet a user's needs.

[18] A portable cellular data modem that is combined with a Wi-Fi router.

- The Postal Service employs continuous monitoring technology and procedures to ensure the wireless network is secure. This technology includes [redacted]. Larger Postal Service facilities have dedicated APs configured for wireless intrusion detection. Smaller facilities employ APs that [redacted] his technology scans and analyzes the wireless network to detect unauthorized access and identify incidents for investigation and resolution by Telecommunication Services.[19]

- Based on limited testing of completed sites,[20] we determined that Telecommunication Services ensured wireless technologies installed as part of the DUIT Program were authorized, evaluated, and assessed prior to deployment and were in compliance with established security policies and procedures. As of February 11, 2014, wireless installation was completed for 2,769 of 11,857 delivery units in the program This installation supports several applications scheduled for deployment:

  - o [redacted]
  - o [redacted]
  - o [redacted]

Telecommunication Services implemented the WLAN tracking database to manage the wireless infrastructure expansion under the DUIT Program. The database contains the deployment status for each application as well as site survey data[24] for individual sites, which allows Telecommunication Services to track the progress of each individual program. See Table 2 for the DUIT Program status.

Recommendations

Security controls over the Postal Service wireless network infrastructure are in place and effective; therefore, we are issuing this report without any recommendations. The Postal Service informally reviewed a draft of this report and had no comments or concerns.

[19] A part of the Enterprise Access Infrastructure group, which manages all access to information technology infrastructure, provides operational support, and provides deployment and strategic direction for the Postal Service.
[20] Selected sites were post offices located in Arlington, WA; Menomonee Falls, WI; Long Point, TX; North Shepherd, TX; and Watsonville, CA.
[21] An overhead camera-based solution that provides hands-free scanning, image capture, and revenue protection functionality at larger delivery units.
[22] DSS consists of an Advanced Computing Environment (ACE) laptop paired with a ring scanner and Bluetooth headset used at smaller delivery units.
[23] A mobile device used to process simple transactions for customers in the lobby rather than at the retail counter.
[24] A wireless site survey is part of the review and approval process. Site surveys are performed to obtain maximum benefits of the wireless devices and maintain appropriate security. The survey results are used to place APs, offer channel sections, etcetera.

Appendix A: Additional Information

Background

Wireless networks allow organizations to extend their LANs to support a mobile workforce. Devices with wireless capabilities such as laptops and smart phones are able to communicate and use computing resources without physically connecting to a network. WLANs are groups of wireless networking devices within a limited geographic area that exchange data through radio communications. WLANs are an extension of the existing wired network and must permit secure, encrypted, authorized communication with access to data, communication, and business services as if connected to the LAN.

WLANs must:

- Maintain accessibility to resources while employees are not connected to a wired network.
- Secure the enterprise from unauthorized, unsecured, or rogue APs.
- Extend the full benefits of integrated network services[25] to nomadic users.[26]
- Segment authorized users and block unauthorized users.
- Easily deploy, operate, and manage central or remote APs.
- Contain wireless threats, enforce security policy compliance, and safeguard information through enhanced security services such as WLAN Intrusion Prevention Systems and Intrusion Detection Systems.
- Simultaneously track thousands of Wi-Fi and active Radio Frequency Identification[27] devices from directly within the WLAN infrastructure for critical applications (location services).
- Provide customers, vendors, and partners with easy access to wired and wireless LANs (guest access).

One of the primary components of a WLAN is an AP that transmits and receives data. These APs allow wireless devices to connect to a wired network using Wi-Fi or related standards, and can serve as the interconnecting point between the WLAN and a fixed wired network. In contrast, a rogue AP is any Wi-Fi access point installed on a network but not authorized for operation on that network, and not under network administrator management. Rogue APs do not conform to WLAN security policies and can allow

[25] Integrated network services support data, voice, and different networking protocols.
[26] Nomadic users are computer users who can freely move in an environment without carrying a computing device, using the devices present in the environment.
[27] A technology that incorporates the use of electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum to uniquely identify an object.

anyone with a Wi-Fi device to connect to a network, bypassing the normal security policies.

Telecommunication Services is responsible for managing the Postal Service network. Network administrators and engineers own all network components and oversee all connections to the network. Telecommunication Services uses the [redacted] for network security, deployment, management, and control issues. This solution integrates [redacted] to automate wireless network planning, configuration, and management functions.

Another tool in the unified wireless network solution is the [redacted] which allows Telecommunication Services to monitor network activity and provide real-time reporting for network statistics and alarms.[29]

Objectives, Scope, and Methodology

Our audit objectives were to determine whether the Postal Service has effective security policies and controls in place to detect unauthorized use and access to its wireless networks, and to determine whether the current approved expansion plan for its wireless infrastructure follows established policy and security standards. To accomplish our objectives, we:

- Interviewed Postal Service officials in Telecommunication Services and members of the Computer Incident Response Team (CIRT)[30] to identify policies and procedures for managing, configuring, and monitoring a wireless network infrastructure and its components.

- Judgmentally selected five facilities at which to conduct wireless network scans to detect unauthorized APs and devices. We conducted the scans using the [redacted].[31] The five facilities we selected were the:

  - Raleigh, NC, P&DC.
  - [redacted].
  - St. Paul, MN, P&DC.
  - Minneapolis, MN, P&DC.
  - [redacted].

[redacted]

An event is an occurrence or detection of some condition in and around the network. An alarm is a [redacted] response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), the [redacted] raises an alarm until the resulting condition no longer occurs.

[30] CIRT is responsible for providing an immediate and effective response to computer security incidents as they occur.

[redacted]

- Obtained an inventory of approved wireless APs and compared data for each of our sampled facilities.

- Identified and analyzed [redacted] unknown APs that were not on the approved inventory list and verified that they were not a threat to the Postal Service network.

- Reviewed standard configuration settings for wireless APs and workgroup bridge.[32]

- Reviewed the [redacted] wireless network security incidents[33] investigated by the CIRT that occurred between October 1, 2013, and February 18, 2014; and verified procedures for monitoring, detecting, and documenting security incidents.

- Obtained documentation for the 2,796 sites completed under the wireless infrastructure expansion project. Selected the five completed sites[34] under the DUIT-PASS Phase 2 and verified that wireless technologies were authorized, evaluated, and assessed prior to deployment.

We conducted this performance audit from August 2013 through April 2014, 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 objectives.

We assessed the reliability of wireless networks inventory data by performing scans of wireless networks, reviewing and analyzing the resultant data, and interviewing knowledgeable officials. We determined that the data were sufficiently reliable for the purposes of this report.

[32] A small stand-alone unit that can provide a wireless infrastructure connection for ethernet-enabled devices.

[redacted]

Arlington, WA; Menomonee Falls, WI; Long Point, TX; North Shepherd, TX; and Watsonville, CA.

Prior Audit Coverage

The U.S. Postal Service Office of Inspector General (OIG) did not identify any prior audits or reviews related to the objective of this audit.

Appendix B: Wireless Scan Analysis

Table 1. [redacted]

Facility	Postal Service Approved APs	OIG Scanned APs	Postal Service Virtual APs	Total Authorized APs	Total Unknown APs
Raleigh P&DC					
[redacted]					
St. Paul P&DC					
Minneapolis P&DC					
[redacted]					
Totals					

Source: Wireless network scans conducted October through December 2013, and Telecommunication Services AP Inventory listing.

Our scans identified [redacted] APs at the five facilities. This total includes [redacted] approved APs and [redacted] that were not in inventory. Based on further analysis of the [redacted] APs, we identified [redacted] APs that increased the total authorized APs to [redacted]. Our final analysis determined that none of the remaining [redacted] APs we discovered were attached to the network; therefore, we did not identify any rogue APs that were a threat to the network.

Table 2. Status of Delivery Unit Wireless Capability Deployment

Status of AP Installations	Programs [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Totals	Percentage
Cancelled	54	73	10		25	162	2.8%
Completed	539	1,163	5	50	1,012	2,769	48.0%
Exception		19				19	0.3%
In Progress		15	4		1	20	0.3%
New		1,891	323			2,214	38.4%
On Hold		28	68			96	1.7%
Pending		15	1			16	0.3%
Rescheduled		27	13			40	0.7%
Scheduled		371	56			427	7.4%
Totals	593	3,602	480	50	1,038	5,763	100.0%
Percentage	10.3%	62.5%	8.3%	0.9%	18.0%	100.0%	

Source: *WLAN Project Tracking Report* dated February 11, 2014.

According to the DUIT program, 18,857 wireless APs will be installed in delivery units to support the [redacted] applications. This connectivity is capable of supporting multiple devices at the same time and providing adequate bandwidth for the applications listed. These APs will be centrally managed and supported, and designed to allow only Postal Service devices to connect to the network infrastructure. Once AP installation is complete under the DUIT program, any future applications that need wireless capability will have it.