



# Department of Homeland Security Office of Inspector General

## Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices

(Redacted)





Homeland  
Security

July 29, 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the actions taken by the Transportation Security Administration (TSA) to implement effective controls to ensure that sensitive information processed by its wireless network and systems is protected from potential exploits. This report is based on a review of internal policies and procedures, interviews with TSA management officials and personnel within the Office of Information Technology and the Federal Air Marshal Service, physical security assessments, vulnerability assessments, direct observations, and a review of applicable documentation.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "Frank W. Deffer".

Frank W. Deffer

Assistant Inspector General, IT Audits

# Table of Contents/Abbreviations

---

Executive Summary .....	1
Background .....	2
Results of Audit .....	6
Actions Taken To Secure TSA’s Wireless Network, Systems, and Devices .....	6
Missing Security Patches Weaken Wireless Security .....	12
Recommendations .....	16
Management Comments and OIG Analysis .....	16
DHS’ Baseline Configuration Controls Have Not Been Fully Implemented on All Wireless Devices and Supporting Infrastructure Systems .....	17
Recommendations .....	20
Management Comments and OIG Analysis .....	20

## Appendices

Appendix A: Purpose, Scope, and Methodology .....	22
Appendix B: Management Comments to the Draft Report .....	25
Appendix C: Examples of TSA Headquarters High-Risk Vulnerabilities .....	28
Appendix D: Examples of FAMS High-Risk Vulnerabilities .....	29
Appendix E: Major Contributors to this Report .....	30
Appendix F: Report Distribution .....	31

## Abbreviations

BES	BlackBerry Enterprise Server
DHS	Department of Homeland Security
DOS	denial-of-service
EAP	Extensible Authentication Protocol
FAMS	Federal Air Marshal Service
FAMSNet	FAMS Network
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
LAN	local area network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PDA	personal digital assistant
PKI	Public Key Infrastructure

# Table of Contents/Abbreviations

---

RADIUS	Remote Authentication Dial-In User Service
SP	Special Publication
SQL	Structured Query Language
TLS	Transport Layer Security
TSA	Transportation Security Administration
TSA Net	TSA Network
WLAN	wireless local area network

# OIG

*Department of Homeland Security  
Office of Inspector General*

---

## **Executive Summary**

Our audit focused on whether the Transportation Security Administration (TSA) has implemented effective controls to ensure that sensitive information processed on its wireless network and BlackBerry devices is protected from potential exploits. It included TSA headquarters' wireless network components and devices, as well as the wireless devices and support infrastructure used by the Federal Air Marshal Service. We used specialized scanning hardware and software to determine whether any rogue access points or unauthorized wireless networks or devices were in use at selected facilities. Further, we conducted scans to detect signal leakage from wireless access points outside TSA headquarters' office buildings.

Overall, TSA has implemented effective physical and logical security controls to protect its wireless network and devices. We did not detect any high-risk vulnerabilities on its wireless network infrastructure or rogue or unauthorized wireless networks or devices attributed to TSA or the Federal Air Marshal Service. Although we identified signal leakage from TSA's wireless network, we determined that this was not a security risk because of the mitigating controls implemented. However, we identified high-risk vulnerabilities involving patch and configuration controls. Improvements are needed to enhance the security of wireless components to fully comply with the department's information security policies and better protect TSA's and Federal Air Marshal Service's wireless infrastructure against potential risks, threats, and exploits.

We are making four recommendations in our report to the TSA Chief Information Officer. Management concurred with all of the recommendations and has already begun implementing them. The

---

response from the Administrator, TSA, is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

## **Background**

Because wireless networks and devices offer connectivity without the physical restrictions associated with wired infrastructures, the use of wireless technology has grown more popular. Wireless networks and devices can offer many benefits to government agencies, such as expanded network accessibility that promotes increased flexibility for the federal workforce. Further, remote accessibility may allow federal employees to perform critical functions and maintain government continuity of operations in the event of an emergency situation or natural disaster. However, wireless networks and devices also present significant security challenges, including cyber threats, weak physical controls of wireless infrastructure and devices, and unauthorized (i.e., rogue) deployments of wireless access points.<sup>1</sup>

The National Institute of Standards and Technology (NIST) identified several potential threats and attack types that may be used to compromise a wireless network. Figure 1 summarizes the potential threats identified, with brief descriptions of each.

---

<sup>1</sup> A “rogue” access point is one that is accessible to an organization’s employees but is not managed as part of the approved network. Most rogue access points are installed by employees and not managed by system administrators.

**Figure 1: Potential Threats to Wireless Networks**

Potential Threat Types	Attack Type <sup>2</sup>	Brief Description
Eavesdropping	Passive	An attacker will monitor wireless data transmissions between devices for message content, such as authentication credentials or passwords.
Traffic Analysis	Passive	An attacker can gain intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.
Denial-of-Service (DOS)	Active	An attacker prevents or prohibits the normal use or management of a wireless local area network (WLAN).
Masquerading	Active	An attacker impersonates an authorized user to gain access to certain unauthorized privileges.
Message Replay	Active	An attacker monitors transmissions (passive attack) and retransmits messages posing as the legitimate user.
Message Modification	Active	An attacker alters a legitimate message by deleting, adding to, changing, or reordering the message.

Source: NIST Special Publication (SP) 800-48, Revision 1, p. 3-1.

Wireless systems include local area networks (LANs), personal area networks, laptop computers, cellular phones, and other devices, such as wireless headphones and other handheld devices.<sup>3</sup> The most common transmission standards used for wireless devices are the Institute of Electrical and Electronics Engineers (IEEE) 802.11 (802.11x) standards and 802.15 Bluetooth technologies.<sup>4</sup>

Wireless networks increase the reach of conventional wired networks by using radio wave signals to transmit data to wireless-enabled devices, such as laptop computers, smartphones, and personal digital assistants (PDA). For example, a WLAN can be formed by establishing connections through

---

<sup>2</sup> According to NIST, a passive attack occurs when an unauthorized party gains access to an asset and does not modify its content or actively attack or disrupt a WLAN. An active attack occurs when an unauthorized party modifies a message, data stream, or file.

<sup>3</sup> A personal area network is the interconnection of information technology (IT) devices within the range of an individual person.

<sup>4</sup> The 802.11x wireless standard can include but is not limited to all 802.11 standards, such as 802.11a/b/g/n. The range of 802.11n devices can reach up to 1,400 feet.

---

a wireless access point or via ad hoc networks to other 802.11x-compatible devices, such as laptop computers, smartphones, and PDAs. Handheld devices and other smartphones may have special features, such as data storage, access to electronic mail and corporate enterprise applications, voice and text messaging, and internet browsing through cellular services or 802.11x technologies. Today, most laptop computers and printers are equipped with both 802.11x and Bluetooth functionality built-in.

The Bluetooth communication protocol is used primarily for wireless connectivity between several types of devices, including smartphones, laptops, printers, and headsets. Bluetooth is defined as an open standard designed for short-range radio frequency communication, most commonly about 30 feet. Bluetooth technology is often used to create wireless personal area networks between two or more devices, commonly referred to as ad hoc or peer-to-peer networks.

In June 2004, we reported that the Department of Homeland Security (DHS) had not implemented effective controls to protect its wireless networks and devices and prevent unauthorized access points from connecting to its networks.<sup>5</sup> Specifically, we determined that intrusion detection systems were not installed to monitor wireless activity. In addition, we identified two rogue wireless access points at a component's facility, non-DHS wireless signals broadcasting beyond the physical boundaries at DHS component facilities, and Bluetooth enabled on three government-issued laptop computers. In August 2005, we identified another unauthorized wireless access point at a component.<sup>6</sup> The weaknesses reported were indicators that DHS had not implemented strong controls to ensure that only legitimate users can access network resources.

As part of its Wireless Infrastructure Project, TSA's Office of Information Technology began implementing wireless connectivity in 2007. The project consists of two phases designed to provide wireless accessibility to TSA personnel at its headquarters and approximately 400 commercial airports across the country. As part of the first phase, TSA has deployed a wireless

---

<sup>5</sup> *Inadequate Security Controls Increase Risks to DHS Wireless Networks* (OIG-04-27), June 2004.

<sup>6</sup> *Improved Security Required for U.S. Coast Guard Networks* (OIG-05-30), August 2005.



---

infrastructure at its headquarters facility, which provides personnel with access to the TSA Network (TSANet).<sup>7</sup> Wireless connectivity is available in TSA headquarters' conference rooms, training rooms, and other common areas. TSA has also issued its personnel, including airport staff, with BlackBerry devices for mobile communications and data accessibility. The devices are supported using a centrally managed BlackBerry Enterprise Server (BES) infrastructure.<sup>8</sup> The second phase of the project, which consists of providing wireless network connectivity at airport locations, has not yet been implemented.

The Federal Air Marshal Service (FAMS), a separate organization within TSA, does not maintain a wireless network. However, FAMS personnel rely extensively on their [REDACTED] devices as a primary means of communication in carrying out their mission and national security responsibilities to help secure and protect the United States' aviation system, including aircraft, airports, passengers, and crew, from criminal and terrorist attacks. FAMS personnel require secure mobile communications, including Bluetooth capabilities, to perform their mission. These devices are supported by FAMS' own centrally managed [REDACTED] backbone infrastructure under the FAMS Network (FAMSNet).<sup>9</sup> Microsoft Windows 2003 servers host the [REDACTED] application used to administer the [REDACTED] devices FAMS personnel use.

As part of our audit, we used laptops equipped with wireless scanning software to identify any unauthorized networks that could be attributed to TSA and verify the signal coverage for access points outside of TSA headquarters. Our laptops were equipped with AirMagnet Wi-Fi Analyzer Pro to detect wireless networks and capture identification and authentication information, including service set identifier, media access control address, authentication protocol, and signal strength. We scanned for 802.11x signals at selected TSA and FAMS facilities in both the Washington, DC, metropolitan area and field offices. We then analyzed

---

<sup>7</sup> TSANet provides wide area network backbone connectivity between all TSA locations and field offices. Additionally, TSANet provides Domain Name Service, virtual private network, and wireless access services.

<sup>8</sup> A BES is software that is hosted (typically) by a Microsoft Windows Server 2003 or 2008 and used to administer BlackBerry device deployment and security. Depending on the infrastructure, a Microsoft Structured Query Language (SQL) database may be used to support functionality.

<sup>9</sup> FAMSNet facilitates internet access as well as internal access to FAMS' information systems.

---

the recorded data to determine the presence of TSA wireless access points and other unauthorized networks or devices.

We also evaluated the effectiveness of controls implemented on TSANet, as well as the TSA BES system and FAMS [REDACTED] infrastructure under FAMSNet, using Tenable Nessus scanning software to identify any security vulnerabilities. TSANet and the TSA BES system are managed by TSA's Office of Information Technology and hosted at TSA headquarters. The FAMSNet [REDACTED] infrastructure is managed by FAMS personnel and hosted at FAMS' primary data center. The TSA and FAMS [REDACTED] systems provide a two-way communications link between a user's [REDACTED] account and the user's assigned [REDACTED] device.

Since both TSA and FAMS are using a current [REDACTED] software that allows security controls to be centrally managed from the server, we obtained and analyzed [REDACTED] policy settings for both TSA and FAMS devices to determine if controls were implemented according to DHS policy. When applied, the server's security settings propagate down and become mandatory for all [REDACTED] smartphones. Additionally, we evaluated physical security controls related to building and system access, perimeter security, media access and storage, facility emergencies, visitor access, and environmental controls.

## **Results of Audit**

### **Actions Taken To Secure TSA's Wireless Network, Systems, and Devices**

TSA has implemented policies, processes, and mitigating physical and system controls to protect its WLAN, supporting infrastructure, and devices from potential exploits. We did not identify any high-risk vulnerabilities on TSA's WLAN infrastructure, or any rogue or unauthorized wireless devices. In addition, an intrusion detection system has been implemented to monitor wireless activity. Further, FAMS has actively worked to secure its infrastructure from the risks associated with wireless and Bluetooth devices.

---

## **Controls Implemented To Mitigate Signal Leakage Identified at TSA Headquarters**

We conducted wireless scans to verify access point signal coverage outside TSA headquarters' office buildings. We used the AirMagnet Wi-Fi Analyzer Pro to conduct testing and walked throughout TSA headquarters to determine the use and assess the security implemented on the wireless access points.<sup>10</sup> Based on our scans, we identified 51 wireless access points that were positively attributed to TSA, 7 of which were confirmed as nonoperational. Confirmation was conducted via physical proximity to the devices, as well as the media access control address identified by the scans, to the externally facing side of each access point provided by headquarters.

We were able to identify signal leakage around two buildings at TSA headquarters. However, because of mitigating controls, such as a hidden service set identifier, requirement for the specific client, strong Federal Information Processing Standards 140-2 certified encryption, and a TSA-controlled and -issued digital certificate required on both user laptops and the authentication server, we determined that this leakage is not a security risk.

## **TSA Is Complying With Wireless Standards and Policies**

During the audit, we determined that both TSA and FAMS are adhering to DHS and NIST 802.11 wireless and Bluetooth standards to secure their wireless infrastructure and devices. TSA has also developed its own IT security policies and procedures regarding the operation and management of its wireless services and devices. TSA's policies for 802.11x and Bluetooth devices outline the minimum technical metrics for the development and use of the technologies, as well as the technical standards.<sup>11</sup> In

---

<sup>10</sup> The AirMagnet Wi-Fi Analyzer Pro automatically detects and alerts users to wireless intrusions, penetration attempts, and hacking strategies, including rogue devices, devices sending unencrypted data, and other potentially damaging security configurations.

<sup>11</sup> TSA's wireless policy is defined in its Information Technology Security Division SPA TS-003; Bluetooth policy is defined in SPA TS-004.

---

addition, TSA has developed guidance for the acceptable use of its BlackBerry smartphones. The guidance addresses help desk processes that cover incident management (i.e., broken or nonfunctional handheld units, lost or stolen handheld units, deactivation process, suspension of handheld service, and reassignment process) and request management (i.e., BlackBerry handheld requests and additional equipment requests).

In addition, TSA has implemented strong authentication and encryption methods to secure its WLAN to maintain the integrity and confidentiality of DHS' data. DHS requires that strong authentication methods be employed to protect wireless networks and devices. Specifically, the policy cites Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)<sup>12</sup> and the use of an enterprise Remote Authentication Dial-In User Service (RADIUS)<sup>13</sup> as a strong authentication method. Further, TSA has implemented the Wireless Fidelity Protected Access 2 Enterprise, which includes EAP-TLS architecture and a RADIUS Public Key Infrastructure (PKI) digital certificate authority to provide secure wireless communications to TSANet. Additionally, TSA has incorporated the required NIST Federal Information Processing Standards 140-2 approved cryptographic module, Advanced Encryption Standard, to help ensure the confidentiality of its wireless communications.

To protect its handheld devices, TSA instituted its BES in a centrally managed architecture that supports the implementation of standard security policies on all TSA BlackBerry smartphones. TSA also implemented a local device security policy that requires the user to authenticate with a password to access the handheld device. In addition, TSA implemented a security measure that erases application data after ■ failed logon attempts and has disabled the camera and video recording functionality to reduce

---

<sup>12</sup> According to NIST, EAP is an access authentication framework that was originally developed to support peer authentication before granting the peer access to the network. The TLS protocol is used to establish a protective tunnel where two parties can execute authentication methods.

<sup>13</sup> RADIUS is an internet-based protocol that facilitates the centralized management of authentication, authorization, and accounting data.

---

potential security concerns in sensitive areas. Further, TSA encrypts the data stored on its BlackBerry devices, as well as data transmitted to and from the devices.

FAMS has implemented password protection similar to that instituted by TSA headquarters, [REDACTED]. However, [REDACTED]. FAMS has set its devices to erase application data after [REDACTED] failed logon attempts and also implemented encryption to aid in securing data-in-transit, as well as data-at-rest, data sent and received, and data stored, [REDACTED]. [REDACTED].

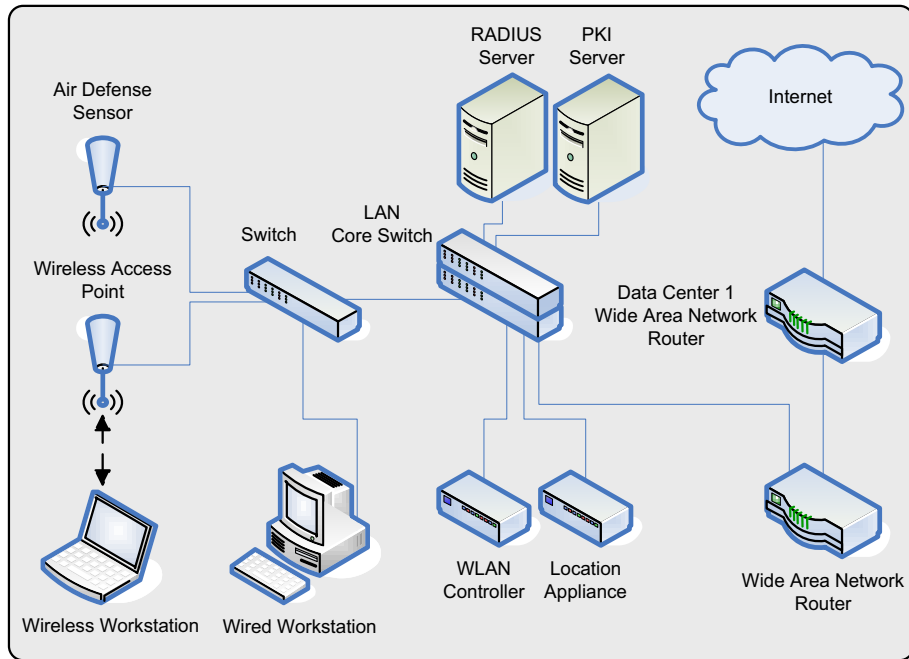
Further, TSA has implemented a wireless intrusion detection system, Air Defense, to protect its WLAN from potential malicious activities or threats.<sup>14</sup> According to DHS policy, a wireless intrusion detection system should incorporate remote sensors that monitor the airwaves and report findings to a wireless intrusion detection system management appliance.<sup>15</sup> These systems scan the airwaves to detect malicious activities such as installation of unauthorized devices, access point outages, wireless client device hijacking, DOS attacks, unauthorized ad hoc or peer-to-peer networks, and other WLAN-specific vulnerabilities. In addition, wireless intrusion detection system sensors may provide triangulation information that assists administrators in identifying attacker location. Figure 2 shows a high-level view of TSA's WLAN architecture.

---

<sup>14</sup> Air Defense is a wireless intrusion detection system that can monitor and detect rogue wireless access points, unauthorized access, and wireless threats, and determine whether use complies with policy.

<sup>15</sup> DHS' *Sensitive System Policy Handbook 4300A*, Attachment Q1 – *Sensitive Wireless Systems*.

**Figure 2: TSA'S WLAN Architecture**

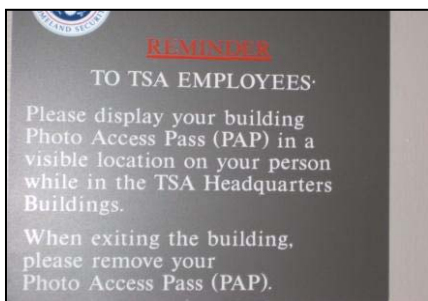


Source: Derived from TSA's Wireless Infrastructure System Design Document.

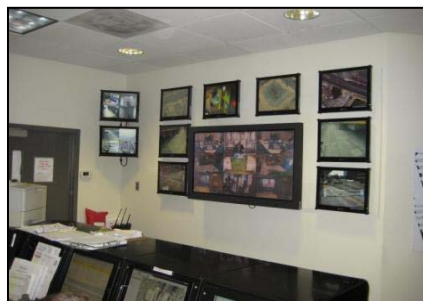
### **Adequate Physical Security Controls Have Been Implemented**

TSA has implemented adequate physical security controls at the facilities where wireless infrastructure and inventory is located. We performed physical security assessments at selected TSA and FAMS facilities. We did not identify any significant deficiencies during these assessments. Figure 3 shows examples of strong physical security countermeasures that have been implemented at TSA headquarters.

### Figure 3: Examples of Physical Security Controls



**Photo Identification Reminder**



**Video Surveillance Monitoring Station**



**Server Room Security Camera**



**Security Booth at TSA Headquarters**

Furthermore, we identified that TSA:

- Conducted annual site security assessments at selected domestic and international airports. Specifically, TSA performed physical and logical security reviews, including wireless scans to identify any unauthorized (i.e., “rogue”) access points, at several airports each year. Based on our reviews of TSA’s fiscal year 2009–2010 site security reports, no rogue wireless access points were identified.
- Performed site surveys prior to implementing its wireless infrastructure project at headquarters. Site assessments were conducted at TSA headquarters in November 2007 to identify wireless infrastructure requirements, define the physical design, and test for potential signal leakage.

- 
- Authorized TSANet and FAMSNet to operate in October and April 2010, respectively. Our quality review of the security authorization packages did not reveal any significant deficiencies. Each system was authorized according to applicable DHS, Office of Management and Budget, and NIST guidance.

### **Conclusion**

In addition to the steps taken, we identified further actions that TSA can take to ensure that the sensitive data processed by its wireless components is better protected from potential threats and exploits. As discussed in the following sections, we identified high-risk patch management vulnerabilities on the three systems tested.<sup>16</sup> TSA's existing patch management process can be improved to ensure that security patches are timely deployed to address system vulnerabilities identified. In addition, we determined that TSA has not fully implemented DHS' baseline configuration settings on all of its wireless devices and supporting infrastructure. Our recommendations will enable TSA to better protect its wireless network, systems, and devices from potential exploits and address the risks and security challenges associated with the use of wireless technology.

### **Missing Security Patches Weaken Wireless Security**

TSA and FAMS must improve patch and configuration management processes on their servers and routers to ensure that controls implemented on the wireless network cannot be circumvented. We reviewed the communication protocols, patch management processes, and configuration controls implemented on TSA and FAMS wireless infrastructures to determine the effectiveness of controls implemented. We used Tenable Nessus to conduct patching vulnerability assessments of the supporting

---

<sup>16</sup> The three systems tested were FAMSNet, the End-User Computing system, and TSA's BES.



infrastructure and client devices at TSA headquarters and at FAMS facilities in Virginia.<sup>17</sup>

Our vulnerability scans at TSA headquarters included a sample of 243 user laptops, the BES infrastructure servers, and their supporting SQL server, all of which enable BlackBerry operations. We also performed vulnerability assessments on the FAMS BES server cluster. FAMS' user laptops were not scanned for security vulnerabilities because they do not offer wireless connectivity to FAMSNet.

### **TSA Headquarters Vulnerability Assessments**

At TSA headquarters, we identified [REDACTED] vulnerabilities on Microsoft Windows XP laptops and the BES supporting BlackBerry devices. The vulnerabilities identified were classified as high-, medium-, and low-risk. The level of risk assigned was based on the severity of damage the vulnerabilities could inflict on a host computer. Figure 4 shows the number of unique high-, medium-, and low-risk vulnerabilities identified by system type.

**Figure 4: Unique Vulnerabilities by System Type at TSA HQ**

	High	Medium	Low	Total
TSA Headquarters Laptops	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
BES Supporting Infrastructure	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Totals	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Our scans identified a total of [REDACTED] unique vulnerabilities. Because medium- and low-risk vulnerabilities do not pose significant threats, our analysis of the results focused on the [REDACTED] unique high-risk vulnerabilities. Overall, our scans identified [REDACTED] instances of high-risk vulnerabilities on TSA headquarters' laptops and [REDACTED] instances of high-risk vulnerabilities on the BES. Unless

<sup>17</sup> Tenable Nessus (Professional Feed) is an up-to-date remote vulnerability software scanning tool for Windows, Linux, Berkeley Software Distribution, Solaris, Apple, and other systems. It is multithreaded, plug-in based, and currently performs more than a thousand remote security checks.

---

addressed immediately, each instance of vulnerability provides an attacker with the potential opportunity to exploit a system.

Of the 243 laptops scanned, only [REDACTED] contained high-risk vulnerabilities; the remaining [REDACTED] had medium- and low-risk vulnerabilities. Some vulnerabilities identified on TSA headquarters' [REDACTED]. [REDACTED] BES that were scanned contained high-risk vulnerabilities. Many of the vulnerabilities we identified on headquarters' systems include those for [REDACTED]. Other vulnerabilities involved [REDACTED]. These vulnerabilities include [REDACTED]. Appendix C lists examples of unique high-risk vulnerabilities identified and the potential threats.

Security and software patches are issued to add or update features and mitigate security vulnerabilities. Applying patches can reduce the number of vulnerabilities that may affect a system's security posture. Currently, TSA downloads and tests Microsoft critical patches [REDACTED] as part of its continuous patching process. After testing is complete and TSA personnel approve the patches, the software updates are pushed out immediately to all TSA workstations. Further, all third-party patch updates are pushed out using Altiris on an as-needed basis, after receiving approval from TSA personnel. The results of our vulnerability assessments revealed that [REDACTED].

DHS requires components to reduce security vulnerabilities through testing and management, promptly installing patches, and



---

[REDACTED]

We discussed the vulnerabilities identified and provided TSA headquarters and FAMS system personnel with our analyses of the technical results. TSA headquarters and FAMS system personnel reviewed our analyses and have begun taking actions to mitigate the vulnerabilities.

**Recommendations**

We recommend that the TSA Chief Information Officer:

**Recommendation #1:** Revise the patch management process to ensure that security patches are deployed timely to mitigate the vulnerabilities identified and better secure headquarters wireless systems.

**Recommendation #2:** Revise the patch management process to ensure that security patches are deployed timely to mitigate the vulnerabilities identified and better secure the FAMS [REDACTED].

**Management Comments and OIG Analysis**

TSA concurred with recommendation 1. Immediately prior to our audit, TSA had just completed a major transition of its Managed Services contract. As part of this transition, the environments used to test the software changes on TSA systems were unavailable and a backlog of software changes, including patches, resulted. The TSA Testing Environment is now available for end user assets (desktops) and will soon be available for enterprise level devices (servers). The backlog of patches on end user assets is being actively worked. As part of the Managed Services Transition, the new service provider has assessed the current Enterprise Patch Management System (Altiris) and has found several areas for

---

improvement. Improvement in these areas will strengthen the TSA Patch Management Program. Another area that TSA has identified as in need of improvement is image version control. TSA has an effort underway that will result in TSA having a single end user image. Having a single image will greatly reduce the complexity of running an effective Patch Management Program.

#### OIG Analysis

We agree with the actions being taken to satisfy the intent of this recommendation. This recommendation will remain open until TSA provides documentation to support that the planned corrective actions are completed.

TSA concurred with recommendation 2. According to management, the appropriate patches have been applied, which has closed these potential vulnerabilities on the TSA FAMS [REDACTED]. Correspondence containing proof of the installed patches was provided to the OIG on March 29, 2011. TSA requests that this recommendation be closed.

#### OIG Analysis

FAMS personnel provided us with documentation showing that the patching issues we identified had been addressed. The documentation provided satisfies the intent of this recommendation. We consider this recommendation resolved and closed.

### **DHS' Baseline Configuration Controls Have Not Been Fully Implemented on All Wireless Devices and Supporting Infrastructure Systems**

Although TSA, including FAMS, has implemented a number of configuration controls on its supporting wireless infrastructure and devices, we identified instances of noncompliance with DHS requirements. The improper configuration of system security settings within a network can compromise wireless security and leave TSA's

---

sensitive data at risk. To evaluate compliance with DHS' baseline configuration settings, we interviewed system administrators and assessed supporting system documentation provided against criteria checklists that are based on the department's guidance.

DHS requires, per the Federal Information Security Management Act of 2002, that components implement baseline security settings on their operating systems and appliances. For example, DHS has provided detailed guidance for IT enterprise elements such as Microsoft Windows XP, Windows SQL Server 2005, Windows Server 2003 and 2008, and Windows Active Directory structure. Guides are also published for network appliances, such as Cisco routers and switches. The guides are distributed to provide DHS systems administrators with a clear, concise set of procedures that will ensure a minimum baseline of security when installing or configuring an existing system. The guides also provide system administrators with the information necessary to modify the settings and to comply with DHS policy and architecture requirements.

### **TSA Headquarters Configuration Control Issues**

We manually assessed the configuration settings applied to standard user Windows XP laptop computers at TSA headquarters. Configuration settings of laptops are enforced by Group Policy Objects that are pushed by TSA's Domain Controllers. We also reviewed the BES server, the back-end supporting SQL server, Cisco wireless control system, and a router for compliance with applicable DHS baseline configuration guidelines.

We identified one noncompliance issue with DHS' Secure Baseline Configuration Guide for Windows XP systems on TSA's laptop computers. [REDACTED]

[REDACTED]

[REDACTED]

---

[REDACTED].

We also reviewed the configuration settings of the security controls established on the wireless control system, which is a multifunctional wireless management utility that manages all wireless LAN controllers and wireless access points. Specific noncompliance issues related to local audit logging functions, a weak authentication protocol, and terminal services. Furthermore, we reviewed the security controls for one of TSA's routers and identified noncompliance issues regarding the disabling of unused router interfaces and a disallowed service.

**FAMS Configuration Control Issues**

We conducted manual reviews at FAMS facilities to assess the configuration settings implemented on the [REDACTED]. We identified [REDACTED] instances of noncompliance, [REDACTED]. [REDACTED]. [REDACTED]. [REDACTED]. [REDACTED]. [REDACTED].

The improper configuration of system security settings on TSA's and FAMS' wireless network infrastructure and devices can allow an unauthorized individual the opportunity to take advantage of system weaknesses and gain access to sensitive data. This issue can affect the confidentiality, availability, and integrity of TSA's and FAMS' information.

---

## Recommendations

We recommend that the TSA Chief Information Officer:

**Recommendation #3:** Implement corrective measures to address instances of noncompliance with DHS' security policy on TSA wireless systems and devices.

**Recommendation #4:** Implement corrective measures to address instances of noncompliance with DHS' security policy on FAMS' wireless device support infrastructure.

## Management Comments and OIG Analysis

TSA concurred with recommendation 3. According to management, this recommendation is for the [REDACTED] [REDACTED] discovered during the audit. DHS policy requires [REDACTED] [REDACTED]. [REDACTED] [REDACTED]. [REDACTED] [REDACTED]. [REDACTED] [REDACTED]. [REDACTED] [REDACTED]. [REDACTED] [REDACTED]. [REDACTED] [REDACTED]. [REDACTED] [REDACTED].

TSA mitigates the risk of [REDACTED] associated with this finding by the use of file encryption. TSA deploys Credant Mobile Guardian as part of the base image to provide file-based encryption to all machines that are deployed within the TSA environment. By encrypting the files on the drive, [REDACTED], TSA mitigates any risk that could be caused by not adhering to the DHS policy.

### OIG Analysis

We agree that the action being taken satisfies the intent of this recommendation. This recommendation will remain open until



---

TSA provides documentation to support that the planned corrective action is completed.

TSA concurred with recommendation 4. FAMS does not have a wireless system within its IT environment but instead uses the wireless capabilities of various service providers. The FAMS mobile devices traverse these wireless networks in a secure manner using encryption and other protection measures. The OIG did not identify any findings related to the mobile devices; however, there were findings related to the back-end infrastructure that supports the mobile devices.

Actions related to the OIG's findings fall into two general areas, as detailed below:

- A) Concur and corrected: FAMS corrected the potentially vulnerable service file setting and the use of the Dynamic Host Configuration Protocol server service on the perimeter router. Proof was provided to the OIG as part of the TSA technical comments response.
  
- B) Concur and exception to be requested: The following configurations are needed for the proper functioning of the IT infrastructure, and exceptions to policy will be submitted for each: [REDACTED]  
[REDACTED]  
[REDACTED].

TSA will submit the needed exception requests for the three items.

OIG Analysis

We agree that the actions being taken satisfy the intent of this recommendation. Although the documentation FAMS personnel provided shows that configuration setting issues we identified have been addressed, this recommendation will remain open until FAMS provides documentation to support that the other planned corrective actions are completed.

## Appendix A

### Purpose, Scope, and Methodology

---

The objective of our audit was to determine whether TSA has implemented effective controls to ensure that sensitive information processed by its wireless networks and devices is protected from potential exploits. Specifically, we determined whether TSA has (1) implemented adequate policies and procedures to mitigate the inherent risks associated with the use of wireless networks and devices, (2) implemented an effective process to properly account for its wireless networks and devices, (3) employed adequate physical security controls over its wireless networks, (4) implemented effective system security controls and properly configured its wireless networks and devices, (5) employed active monitoring of its wireless networks and devices to enforce wireless security policy, and (6) certified and accredited its wireless networks in accordance with applicable DHS and Federal Information Security Management Act requirements.

Our audit focused on the requirements and recommendations outlined in the following documents:

- DHS' *Sensitive System Policy Handbook 4300A*, including Attachment Q1: *Sensitive Wireless Systems*
- NIST SP 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-48 – Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-94 – Guide to Intrusion Detection and Prevention Systems
- NIST SP 800-120 – Recommendation for Extensible Authentication Protocol (EAP) Methods Used in Wireless Network Access Authentication
- NIST SP 800-121 – Guide to Bluetooth
- DHS' Cisco Device (Router/Switch) Configuration Guidance
- DHS' Windows Server 2003 Configuration Guidance

## Appendix A

### Purpose, Scope, and Methodology

---

- DHS' Windows XP Secure Baseline Configuration Guide
- DHS' SQL Server Secure Baseline Configuration Guide
- TSA-specific guidance, including the TSA Management Directive 1400.3 – Information Technology Security, TSA Information Technology Security Handbook, and Office of Information Technology's technical standards
- Federal Information Security Management Act of 2002

We interviewed selected personnel and management officials at TSA headquarters and airport facilities. Specifically, we interviewed the Dulles Federal Security Director; Las Vegas Acting Deputy Federal Security Director; TSA's Deputy Division Chief, Office of Security; Chief, Property Management Policy; information system security officers; and an IT and property management specialist. For FAMS, we interviewed the FAMS Deputy Assistant Director; Branch Chief, FAMS Headquarters Security; Chief, IT Security; Las Vegas Assistant Special Agent in Charge; Property Management Branch Manager; and several other staff members, including system administrators and IT specialists.

We also reviewed and evaluated TSA's security policies, standard operating procedures, training data, security authorization packages, and other appropriate documentation. We performed physical security assessments at selected TSA and FAMS facilities. In addition, we used Tenable Nessus scanning software to identify vulnerabilities on wireless components. We also used wireless scanning tools such as AirMagnet Wi-Fi Analyzer Pro, Black Box Wi-Net Detector, and ViStumbler to identify signal leakage, rogue wireless access points, and unauthorized wireless devices. Furthermore, we performed manual reviews to ensure that TSA's wireless devices (i.e., laptops) are properly configured in accordance with applicable guidance. We initially included the detection and identification of Bluetooth personal area network connections at TSA headquarters and FAMS in the audit plan. However, due to technical difficulties experienced early in audit fieldwork, Bluetooth testing was removed from the scope of the audit.

## **Appendix A**

### **Purpose, Scope, and Methodology**

---

Fieldwork was performed at TSA and FAMS headquarters in Virginia; TSA's inventory warehouse in Virginia; Dulles International Airport in Chantilly, Virginia; McCarran International Airport in Las Vegas, Nevada; TSA's Freedom Center in Ashburn, Virginia; and several other FAMS facilities in Ashburn, Virginia; Las Vegas, Nevada; Egg Harbor, New Jersey; and Philadelphia, Pennsylvania.

We conducted this performance audit between November 2010 and April 2011 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major OIG contributors to the audit are identified in Appendix E.

The principal OIG point of contact for the audit is Frank Deffer, Assistant Inspector General, IT Audits, at (202) 254-4100.

**Appendix B**  
**Management Comments to the Draft Report**

---



U.S. Department of Homeland Security  
601 South 12th Street  
Arlington, VA 20598

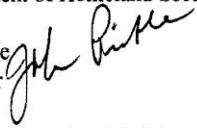


**Transportation  
Security  
Administration**

**JUN 28 2011**

INFORMATION

MEMORANDUM FOR: Charles Edwards  
Acting Inspector General  
U.S. Department of Homeland Security


FROM: John S. Pistole   
Administrator

SUBJECT: Transportation Security Administration's (TSA) Response to  
Department of Homeland Security (DHS) Office of Inspector  
General's OIG Draft Report Titled *Improvements in Patch and  
Configuration Management Controls Can Better Protect TSA's  
Wireless Network and Devices*, OIG Project No. 11-005-ITA-TSA,  
May 2011

Purpose

This memorandum constitutes the formal response by TSA to the draft report from the DHS Office of Inspector General (OIG) titled *Improvements in Patch and Configuration Management Controls Can Better Protect TSA's Wireless Network and Devices*, May 2011. TSA recognizes the importance of effective controls to protect sensitive information processed through wireless networks and devices, and we appreciate the opportunity to review and provide comments to OIG's draft report.

Background

On November 3, 2010, DHS/OIG commenced an audit of the TSA wireless security. The objective of that audit was to determine whether TSA implemented effective controls to protect sensitive information from potential exploits as processed by wireless networks and devices. The audit included wireless network components and mobile devices at TSA Headquarters, TSA laptops, , as well as several field office facilities and devices used by the Federal Air Marshal Service (FAMS).



**Improvements in Patch and Configuration Management Controls Can Better Protect  
TSA's Wireless Network and Devices**

## Appendix B Management Comments to the Draft Report

---

[REDACTED]

2

### Discussion

As noted in the draft report, OIG determined that TSA has implemented effective physical and logical security controls to protect its wireless network and devices. OIG did not detect the presence of any rogue or unauthorized wireless networks or devices attributed to TSA or FAMS. Although signal leakage from TSA's wireless network was identified, OIG determined that this was not a security risk due to the implemented mitigating controls. Results from the audit confirmed that TSA's implementations of its wireless network and mobile devices were largely problem free.

TSA appreciates OIG's recognition that "TSA has implemented policies, processes, and mitigating physical and system controls to protect its [wireless local area network], supporting infrastructure, and devices from potential exploits," and OIG's further acknowledgement that "FAMS has actively worked to secure its infrastructure from the risks associated with the wireless and Bluetooth devices." The OIG audit team did identify high-risk vulnerabilities involving patch and configuration controls on two of the four systems tested. The OIG recommends, and TSA concurs, that improvements are needed to further enhance the security of wireless components and the back-end infrastructure, and to fully comply with the Department's information security policies. All of the identified findings have been addressed or corrected. The OIG's efforts are appreciated and have resulted in the increased protection of wireless infrastructure against potential risks, threats, and exploits for both TSA and FAMS.

**Recommendation #1: Revise the patch management process to ensure that security patches are deployed timely to mitigate the vulnerabilities identified and better secure headquarters wireless systems.**

**TSA Concurs:** Immediately prior to the OIG Audit, TSA had just completed a major transition of its Managed Services contract. As part of this transition, the environments used to test the software changes on TSA systems were unavailable and a backlog of software changes, including patches, resulted. The TSA Testing Environment is now available for end user assets (desktops) and will soon be available for enterprise level devices (servers). The backlog of patches on end user assets is being actively worked. As part of the Managed Services Transition, the new service provider has assessed the current Enterprise Patch Management System (Altiris) and has found several areas for improvement. Improvement in these areas will strengthen the TSA Patch Management Program. Another area that TSA has identified as in need of improvement is image version control. TSA has an effort underway that will result in TSA having a single end user image. Having a single image will greatly reduce the complexity of running an effective Patch Management Program.

**Recommendation #2: Revise the patch management process to ensure that security patches are deployed timely to mitigate the vulnerabilities identified and better secure the FAMS**

[REDACTED]

---

[REDACTED]

Improvements in Patch and Configuration Management Controls Can Better Protect  
TSA's Wireless Network and Devices

## Appendix B Management Comments to the Draft Report

---

[REDACTED]

3

**TSA Concur:** The appropriate patches have been applied, which has closed these potential vulnerabilities on the TSA FAMS [REDACTED]. Correspondence containing proof of the installed patches was provided to the OIG on March 29, 2011. TSA requests that this recommendation be closed.

**Recommendation #3: Implement corrective measures to address instances of noncompliance with DHS' security policy on TSA wireless systems and devices.**

**TSA Concur:** This recommendation is for the [REDACTED] discovered during the audit. DHS policy requires c [REDACTED]

TSA mitigates the risk of [REDACTED] associated with this finding by the use of file encryption. TSA deploys Credant Mobile Guardian as part of the base image to provide file based encryption to all machines that are deployed within the TSA environment. By encrypting the files on the drive, [REDACTED], TSA mitigates any risk that could be caused by not adhering to the DHS policy.

**Recommendation #4: Implement corrective measures to address instances of noncompliance with DHS' security policy on FAMS wireless systems and devices.**

**TSA Concur:** FAMS does not have a wireless system within its information technology (IT) environment but instead uses the wireless capabilities of various service providers. The FAMS mobile devices traverse these wireless networks in a secure manner using encryption and other protection measures. OIG did not identify any findings related to the mobile devices; however, there were findings related to the back-end infrastructure that supports the mobile devices. Actions related to OIG's findings fall into two general areas as detailed below:

- A) Concur and corrected: FAMS corrected the potentially vulnerable service file setting and the use of the Dynamic Host Control Protocol server service on the perimeter router. Proof was provided to the OIG as part of the TSA technical comments response.
- B) Concur and exception to be requested: The following configurations are needed for the proper functioning of the IT infrastructure and exceptions to policy will be submitted for each: [REDACTED]

TSA will submit the needed exception requests for the three items.

[REDACTED]

**Appendix C**  
**Examples of TSA Headquarters High-Risk Vulnerabilities**

[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]		■	[Redacted]
[Redacted]		■	[Redacted]
[Redacted]		■	[Redacted]
[Redacted]		■	[Redacted]
[Redacted]		■	[Redacted]
[Redacted]		■	[Redacted]
[Redacted]	■		[Redacted]
[Redacted]		■	[Redacted]
[Redacted]		■	[Redacted]



**Appendix D**  
**Examples of FAMS High-Risk Vulnerabilities**

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]		■	[REDACTED]
[REDACTED]		■	[REDACTED]
[REDACTED]		■	[REDACTED]
[REDACTED]		■	[REDACTED]
[REDACTED]		■	[REDACTED]
[REDACTED]		■	[REDACTED]
[REDACTED]		■	[REDACTED]

**Appendix E**  
**Major Contributors to this Report**

---

**Information Security Audit Division**

Chiu-Tong Tsang, Director  
Barbara Bartuska, IT Audit Manager  
Mike Horton, IT Officer  
Aaron Zappone, Team Lead  
Thomas Rohrback, IT Specialist  
Michael Kim, IT Auditor  
Amanda Strickler, IT Specialist  
David Bunning, IT Specialist  
Anna Hamlin, Referencer

**Appendix F**  
**Report Distribution**

---

**Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretariat  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
Administrator, TSA  
Chief Information Officer, DHS  
Chief Information Security Officer, DHS  
Chief Information Officer, TSA  
Chief Information Security Officer, TSA  
Director, Compliance and Oversight Program, DHS  
Deputy Director, Compliance and Oversight Program, DHS  
Chief, IT Security, FAMS  
Director, GAO/OIG Liaison Office  
Chief Information Security Officer Audit Liaison, DHS  
TSA Audit Liaison  
FAMS Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees, as appropriate



#### ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at [www.dhs.gov/oig](http://www.dhs.gov/oig).

#### OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov); or
- Write to us at:  
DHS Office of Inspector General/MAIL STOP 2600,  
Attention: Office of Investigations - Hotline,  
245 Murray Drive, SW, Building 410,  
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.