



Department of Homeland Security Office of Inspector General

Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure

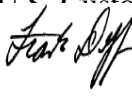




Homeland Security

September 28, 2011

MEMORANDUM FOR: Charles Armstrong
Assistant Commissioner
Office of Information and Technology
U.S. Customs and Border Protection

FROM: 
Assistant Inspector General
Information Technology Audits

SUBJECT: *Final Letter Report: Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure*

Attached for your information is our final letter report, *Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure*. We incorporated the formal comments from U.S. Customs and Border Protection in the report.

The report contains three recommendations aimed at improving U.S. Customs and Border Protection's overall effectiveness in securing its wireless infrastructure. Your office concurred with all of the recommendations. Within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. The report will be posted on our website.

Should you have any questions, please call me, or your staff may contact Richard Saunders, Director, Advanced Technology Division, at (202) 254-5440.

Attachment

Background

Because wireless networks and devices offer connectivity without the physical restrictions associated with wired infrastructures, the use of wireless technology has grown significantly. 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 personnel 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 or rogue deployments of wireless access points.¹

Wireless systems include local area networks, personal area networks, laptop computers, cellular phones, and other devices, such as wireless headphones and other handheld devices. The most common transmission standards used for wireless devices are the Institute of Electrical and Electronics Engineers 802.11 standards and 802.15 Bluetooth[®] technologies.

Owing to the large scale of U.S. Customs and Border Protection's (CBP) responsibilities at airports, seaports, rail inspection areas, and outbound lanes, implementing wireless technologies at these locations would assist the officers, agents, and inspectors in performing their job functions. CBP designed its Enterprise Wireless Infrastructure (EWI) based on 802.11 technologies to accommodate connectivity at CBP sites to promote wireless capabilities or where traditional wired networks may not be feasible. The servers for managing EWI's wireless communications are located at the National Data Center in Springfield, Virginia.

CBP's current wireless infrastructure evolved from the Department of the Treasury's legacy wireless program for the Treasury Enforcement Communications System (TECS). The program was developed to provide personnel with wireless access to TECS at major air, land, and sea ports of entry. In 2003, as technology improved, CBP initiated its EWI program to improve the mobility of its workforce. CBP's Office of Information and Technology had taken steps to deploy a wireless infrastructure at selected locations throughout the continental United States and the Commonwealth of the Northern Mariana Islands. In 2008, CBP tested and deployed EWI as a production system at 51 sites.

Results of Review

CBP has made progress in improving EWI security controls. However, additional steps are needed to further strengthen EWI security. Specifically, CBP needs to (1) remediate its current plans of action and milestones (POA&Ms) in a timely manner, (2) enable and monitor the wireless intrusion detection systems (WIDS) to protect its network, and

¹ A rogue access point is accessible to an organization's employees and outsiders and is not managed as part of the approved network. Most rogue access points are installed by employees and not managed by system administrators.

(3) perform regular vulnerability assessments to identify vulnerabilities and evaluate the effectiveness of existing wireless security controls.

CBP Has Taken Steps To Secure EWI

CBP has taken the following steps to improve its wireless security posture:

- Published a policy and implementation guidance in 2009 to use in developing and implementing its wireless security program.² This policy incorporates guidance from the National Institute of Standards and Technology (NIST), the National Security Agency, and the Department of Defense. In addition, the policy includes a wireless security checklist that provides security requirements for all wireless systems.
- Certified and accredited (C&A) EWI in July 2010, following the process outlined in NIST Special Publication (SP) 800-37.³ The EWI C&A process included all the required C&A documentation, such as a system security plan, risk assessment, system test and evaluation plan, security assessment report, contingency plan, contingency plan test results, and self-assessment.
- Performed an independent security test and evaluation (ST&E) that identified 15 information security program risks, as part of its EWI C&A process. CBP is tracking these information technology (IT) security weaknesses in the Department of Homeland Security (DHS) enterprise management tool.⁴
- Established adequate wireless security configurations to protect its wireless networks and devices against commonly known security vulnerabilities.

For example, CBP (1) uses WPA2 Advanced Encryption Standard between laptops and wireless access points to protect the confidentiality of data; (2) disables the wireless Service Set Identifier (SSID) from being publicly broadcasted to potential attackers;⁵ (3) installs proprietary software on its laptops to connect to the wireless network; and (4) requires personnel to use two-factor

² CBP *Information Systems Security Policies and Procedures Handbook, HB 1400-05D, Attachment Q1*, dated July 27, 2009.

³ Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

⁴ DHS uses an enterprise management tool, Trusted Agent FISMA, to collect and track data related to all POA&Ms, including self-assessments, and C&A data.

⁵ The SSID is a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. From a security point of view, the SSID acts as a simple single shared password between base stations and clients.

authentication to access the wireless network. We verified the effectiveness of these controls through observations or by using the AirMagnet Wi-Fi Analyzer PRO software to conduct testing at selected CBP sites.⁶ Our scans did not identify any high or medium risk vulnerabilities that pose significant threats on authorized CBP wireless networks and devices. Additionally, we did not identify any unauthorized or rogue wireless devices.

- Incorporated wireless security awareness into its annual security awareness and rules of behavior training. In fiscal year 2011, 59,025 of 60,000 (98%) CBP personnel received IT security awareness training. For CBP personnel with significant security responsibilities, 1,223 of 1,231 (99%) have received specialized training as recommended in NIST SP 800-50 and 800-16. The CBP *Information Systems Security Policies and Procedures Handbook, HB 1400-05D, Attachment Q1*, indicates that any appropriate wireless security awareness training should be included in CBP's annual training.

Despite these efforts, CBP faces challenges in fully implementing a secure wireless infrastructure. Specifically, CBP needs to (1) manage and remediate the deficiencies identified in the EWI POA&Ms to ensure that corrective actions are taken; (2) enable wireless intrusion detection functionality to monitor network activity; and (3) perform regular vulnerability assessments to ensure that wireless networks and devices are operating securely.

CBP Needs To Address EWI POA&M Deficiencies

The EWI Information Systems Security Officer (ISSO) is responsible for ensuring the implementation and maintenance of security controls in accordance with DHS policies and the EWI System Security Plan (SSP). In July 2010, as part of EWI's C&A process, the ISSO coordinated with CBP's Security Technology and Policy Branch to perform an independent ST&E. The assessment identified 15 EWI wireless security vulnerabilities and risks that compromise the integrity of the system. The ISSO entered these weaknesses into DHS' enterprise management tool to assess, prioritize, and monitor the progress of corrective actions and remediation efforts.

Although 15 security weaknesses were initially identified, 8 deficiencies were either remediated by the ISSO or granted exceptions by the DHS Chief Information Security Officer (CISO).⁷ CBP requested an exception because it was unable to bring EWI's control weaknesses into compliance with DHS policy. For example, EWI used a Cisco[®]

⁶ The AirMagnet Wi-Fi Analyzer PRO software 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.

⁷ DHS components may request waivers to or exceptions from any portion of *DHS 4300A*, for up to 6 months, any time they are unable to fully comply with policy requirements. Exceptions are generally limited to systems that are unable to comply because of an impact to mission, excessive costs, and commercial-off-the-shelf products that cannot be configured to support control requirements. Requests are made through the component's ISSO for the system to the component's respective CISO, and then to the DHS CISO.

commercial-off-the-shelf product to build its wireless architecture, but this product does not use Secure File Transfer Protocol and Secure Socket Layer Protocol as required by DHS configuration guidelines.⁸ In December 2010, CBP network architects submitted a request to Cisco[®] to explore future code releases to comply with DHS policy; however, these weaknesses have not been addressed.

As of June 2011, CBP had not remediated the seven remaining POA&Ms. For example:

- Wireless activities have not been transitioned from the development team to the DHS Security Operations Center (SOC).⁹
- Field technology officers have not received training on how to handle and respond to EWI system events.
- An EWI alternate site has not been established for backup redundancy.
- Public Key Infrastructure is not being used with EWI because this technology is not available at an organization level.¹⁰

Additionally, the ISSO has not updated the current status of the outstanding seven weaknesses in DHS' enterprise management tool.

According to *DHS 4300A Sensitive Systems Handbook, Attachment H*, a POA&M provides a high-level view of what needs to be done to correct identified weaknesses. POA&M data should be monitored on a continuous basis and updated as events occur. DHS requires that all information in the POA&M be updated at least monthly and be accurate on the first day of each month for Department tracking and reporting purposes.

Without an effective remediation program, identified vulnerabilities may not be resolved in a timely manner, thereby allowing opportunities for unauthorized individuals to exploit these weaknesses and gain access to sensitive information and systems.

CBP Needs To Enable Wireless Intrusion Detection Functionality

CBP has not enabled the WIDS to protect EWI's network from potential malicious activities or threats.¹¹ According to the *CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D, Attachment Q1*, a WIDS should incorporate

⁸ Secure File Transfer and Secure Socket Layer Protocols are used for protecting information during the transmission between a client and the server.

⁹ The DHS SOC coordinates Department-level incident response and reporting, assists DHS' components with incident response, and identifies and resolves computer security irregularities that affect the ability of DHS to conduct its mission. The SOC is responsible for centralized management and oversight of the CBP and the DHS cyber intelligence program, digital media analysis, and penetration testing and vulnerability assessment teams.

¹⁰ Public Key Infrastructure is used as a support service to the Personal Identity Verification system, which provides the cryptographic keys needed to perform digital signature based identity verification, and to protect communications and storage of sensitive verification system data within the identity cards and the verification system.

¹¹ WIDS can inspect the network traffic for policy violations, vulnerability exploitations, anomalous activity, and rogue wireless access points.

remote sensors that monitor the airwaves and report findings to a WIDS management appliance. Further, NIST SP 800-53A recommends that organizations employ automated tools to support real-time analysis of events. These systems scan the airwaves to detect malicious activities such as the installation of unauthorized devices, access point outages, wireless client device hijacking, denial of service attacks, unauthorized ad-hoc or peer-to-peer networks, and other wireless network vulnerabilities.

Without enabling wireless intrusion detection functionality, CBP will not be able to monitor wireless security activity, detect potential attacks, notify the appropriate officials of an incident, and take corrective actions.

CBP Needs To Establish Processes for Performing Regular EWI Vulnerability Assessments

CBP is not performing wireless vulnerability and security scans of EWI to ensure that authorized wireless networks and devices are adequately secured and to detect unauthorized or rogue wireless networks and devices. Scanning tools can identify outdated software, validate compliance with organizational security policy, and generate alerts and reports about identified vulnerabilities. According to the Director of the DHS SOC, CBP does not have the necessary tools or resources to perform on-site wireless security assessments. In addition, according to the CBP Vulnerability Assessment Team liaison, the technical engineers are only capable of scanning wireless access points connected to the wired network.

According to the *DHS 4300A Sensitive Systems Handbook*, CBP is responsible for performing periodic scans to identify vulnerabilities and take corrective actions. Due to the inherent risks of wireless technologies, the *CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D*, requires frequent security testing and evaluation of controls to be conducted for deployed wireless technologies.

Without an established process to perform regular vulnerability assessments, CBP cannot evaluate wireless security risks impacting its operations and timely implement the necessary corrective actions. Without regular vulnerability assessments, inappropriate or malicious activity by an unauthorized or authorized user may not be detected.

Recommendations

We recommend that the CBP Assistant Commissioner, Office of Information and Technology take the following actions to improve EWI's security:

1. Remediate POA&Ms in a timely manner to minimize potential security risks.
2. Enable the WIDS incorporated into EWI's hardware devices to protect its wireless network from potential malicious activities or threats.

3. Establish a process to perform regular vulnerability assessments to evaluate the effectiveness of EWI's wireless security and to detect unauthorized wireless networks and devices.

Management Comments and OIG Analysis

We obtained written comments on a draft report from the CBP Assistant Commissioner, Office of Internal Affairs. We have included a copy of the comments, in its entirety, in appendix B. The CBP Assistant Commissioner concurred with all three recommendations.

Recommendation 1

For recommendation 1, CBP states that it will review and update the POA&Ms in order to update and close those that have been remediated. Those that remain open will reflect what remains to be done in order to minimize their potential security risks.

CBP identified two open POA&Ms to be addressed. The first POA&M is the need to duplicate the data center network infrastructure at the DHS Data Center 1 (Stennis) that supports the EWI. This would facilitate network redundancy in the event of failure of the primary network. The second POA&M provides adequate staff to support the EWI.

A Resource Requirement Request will be submitted as part of the first quarter fiscal year (FY) 2012 submission. Once funding is obtained, CBP will be able to obtain the necessary resources to remediate these open POA&Ms. The completion date for this recommendation is January 1, 2013.

OIG Analysis

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

Recommendation 2

CBP concurs with recommendation 2 based on its understanding that its intent is to fully utilize the WIDS by putting the device on the EWI network and actively monitoring the data captured by the WIDS. CBP has WIDS devices at each of the 51 CBP sites where EWI is deployed and is logging data. However, no one is currently monitoring and reviewing the data for anomalous activity.

CBP has created a Resource Requirement Request to be submitted as part of the first quarter FY 2012 submission to obtain the necessary funding to address the monitoring of the WIDS data. Once funding is obtained, CBP will be able to assign the necessary resources to accomplish that task.

In addition, CBP is presently engaged in transferring ownership of the EWI from the Enterprise Networks and Technology Support Division to the Network Security Office. This process includes documenting the EWI Wireless Control System so that the Network Security Office can properly manage the EWI system in terms of operations and maintenance and generation of audit reports. The proposed completion date for this recommendation is January 1, 2013.

OIG Analysis

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

Recommendation 3

CBP concurs with OIG recommendation 3. CBP has set up vulnerability scans for all EWI Wireless Controllers, and the Wireless Information Systems Security Officer is currently conducting scans. A schedule will be formalized by December 2011 to ensure that the scans are scheduled and conducted on a regular and recurring basis. The proposed completion date for this recommendation is December 31, 2011.

OIG Analysis

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

Appendix A

Purpose, Scope, and Methodology

The objectives of our review were to determine whether CBP has implemented the required wireless security controls on authorized wireless systems and devices and to assess the effectiveness of CBP's ability to detect and prevent unauthorized networks and devices.

We reviewed DHS policies and procedures, as well as prior audit reports. We reviewed CBP wireless topography and design documentation, security authorization packages, and other certification and accreditation deliverables. We interviewed selected personnel, management officials, and subject matter experts that were relevant to this audit. Also, we distributed a questionnaire to the 51 CBP sites that had initially deployed 802.11 wireless technologies to determine where wireless security assessments could be performed and to identify wireless issues or concerns.

In addition to distributing the questionnaire, we conducted fieldwork at CBP headquarters in Washington, DC; National Data Center in Springfield, Virginia; Washington Dulles International Airport in Sterling, Virginia; Dundalk Seaport in Baltimore, Maryland; DHL Facility at the Cincinnati-Northern Kentucky International Airport in Erlanger, Kentucky; CBP Port of Entry in Douglas, Arizona; and the Unisys Government Test Lane Facility in Fredericksburg, Virginia. Fieldwork was performed through conference calls and data calls at the Saipan International Airport and the Rota International Airport in the Commonwealth of the Northern Mariana Islands.

We conducted our review between November 2010 and May 2011. This was a limited scope review; therefore, our work was not performed in accordance with generally accepted government auditing standards. Major OIG contributors to the evaluation are identified in appendix C.

We appreciate the efforts by CBP management and staff to provide the information and access necessary to accomplish this review.

Appendix B Managements Comments to the Draft Letter Report

1300 Pennsylvania Avenue NW
Washington, DC 20229



**U.S. Customs and
Border Protection**

August 31, 2011

MEMORANDUM FOR FRANK DEFFER
ASSISTANT INSPECTOR GENERAL FOR IT AUDITS
DEPARTMENT OF HOMELAND SECURITY

FROM: Assistant Commissioner 
Office of Internal Affairs
U.S. Customs and Border Protection

SUBJECT: Response to the Office of Inspector General's Draft Report
Entitled, "Security Issues with U.S. Customs and Border
Protection's Enterprise Wireless Infrastructure"

Thank you for providing us with a copy of your draft report entitled "Security Issues with U.S. Customs and Border Protection's Enterprise Wireless Infrastructure," and the opportunity to comment on the issues in this report.

The report contains three recommendations directed to U.S. Customs and Border Protection (CBP). A summary of CBP actions and corrective plans to address the recommendations is provided below:

Recommendation #1: Remediate open Plan of Action and Milestones in a timely manner to minimize potential security risks.

CBP Response: Concur. CBP has reviewed and re-baselined the master Plan of Action and Milestones (POAM) list and schedule with the Information System Security Manager (ISSM) in order to remediate what can be closed, and open new POAMs to reflect what still needs to be done in order to minimize potential security risks.

CBP has identified that there are two parts to the risks to be addressed. The first is the duplication of the data center infrastructure supporting the Enterprise Wireless Infrastructure (EWI) within the DHS Data Center 1 (Stennis) facility to support redundancy in the design. The second is providing adequate staff to support the EWI. A Resource Requirement Request (RRR) will be submitted as part of the 1st quarter Fiscal Year 2012 submission. Once funding is obtained, CBP will be able to obtain the necessary resources to remediate the open POAMs.

Completion Date: January 1, 2013

Appendix B Managements Comments to the Draft Letter Report

2

Recommendation #2: Enable the wireless intrusion detection system, which is incorporated into the Enterprise Wireless Infrastructure's hardware devices, to protect its wireless network from potential malicious activities or threats.

CBP Response: Concur. CBP concurs with this recommendation based on the understanding that the intent of the recommendation is to encompass both enabling and monitoring of Wireless Intrusion Detection system (WIDS). CBP has enabled the WIDS but is not currently monitoring the system. CBP has created a Resource Requirements Request (RRR) to be submitted as part of the 1st quarter Fiscal Year 2012 submission to obtain the necessary funding needed to address the monitoring of the WIDS data. Once funding is obtained, CBP will be able to assign the necessary resources to monitor the system.

CBP is presently engaged in transferring ownership of the EWI from Enterprise Networks and Technology Support Division (ENTS) to the Network Security Office (NSO) and Windows Server Farm (WSF). The process entails the documentation of the EWI Wireless Control System (WCS) Windows application information so that the NSO/WSF can properly manage the EWI WCS in terms of monitoring, configuration, administration and generation of audit reports.

Currently, WIDS is functioning at all 51 CBP sites where EWI is deployed and logging is occurring. Attached please find the following documentation demonstrating that WIDS is enabled and logs are being generated:

WIDS Signatures.doc – This document is made up of screen shots from the controller that displays that WIDS is active. Please note that Cisco refers to WIDS under the naming of WPS. Also, WPS/WIDS is enabled as a default configuration and was enabled out of the box upon initial implementation of these devices.

WSMNBG01_configuration.txt – This document is a copy of the configuration showing that WIDS is enabled.

Security Alarm Trending Summary 20110701 103802 374.pdf – This document is from the log files over the past 12 weeks. The system is reporting the necessary data and the logging servers are capturing this data.

Completion Date: January 1, 2013

Appendix B

Managements Comments to the Draft Letter Report

3

Recommendation #3: Establish a process to perform regular vulnerability assessments to evaluate the effectiveness of the Enterprise Wireless Infrastructure's wireless security and to detect unauthorized wireless networks and devices.

CBP Response: Concur. Vulnerability scans have been set up for all EWI Wireless Controllers. Vulnerability Assessment Team (VAT) scans are currently being conducted by the Wireless Information Systems Security Officer (ISSO). A schedule will be formalized by December 2011 to ensure the scans are conducted on a regular and recurring basis.

Completion Date: December 31, 2011

With regard to the sensitivity of the draft report, CBP did not identify any sensitive information that would require a "For Official Use Only" designation or warrant protection under the Freedom of Information Act.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Ashley Boone, CBP Audit Liaison, at (202) 344-2539.

Appendix C
Major Contributors to this Report

Richard Saunders, Director
Steve Matthews, IT Audit Manager
Philip Greene, IT Audit Team Leader
Jamie Horvath, IT Specialist
Patrick Nadon, Report Consultant
Frederick Shappee, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer
Chief Information Security Officer

Customs and Border Protection

CBP Commissioner
CBP Chief Information Officer
CBP Chief Information Security Officer
CBP Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committee, 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.

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; 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.