REVIEW OF WEB APPLICATIONS SECURITY AND INTRUSION DETECTION IN AIR TRAFFIC CONTROL SYSTEMS

Federal Aviation Administration

Report Number: FI-2009-049
Date Issued: May 4, 2009

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Report on Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems
Report Number: FI-2009-049

Date: May 4, 2009

From: Rebecca C. Leng Rebecca Leng
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Acting Federal Aviation Administrator

This report presents the results of our audit of Web applications security and intrusion detection in air traffic control (ATC) systems. This audit was requested by the Ranking Minority members of the House Committee on Transportation and Infrastructure and its Aviation Subcommittee.

Homeland Security Presidential Directive (HSPD)–7 designates air traffic control systems as part of the Nation's critical infrastructure due to the important role commercial aviation plays in fostering and sustaining the national economy and ensuring citizens' safety and mobility. Essentially, HSPD-7 requires the Secretary of Transportation to ensure that the ATC system is protected from both physical and cyber security threats to prevent disruptions in air travel and commerce.

The need to protect ATC systems from cyber attacks requires enhanced attention because the Federal Aviation Administration (FAA) has increasingly turned toward the use of commercial software and Internet Protocol (IP)[1]-based technologies to modernize ATC systems. While use of commercial IP products, such as Web applications,[2] has enabled FAA to efficiently collect and disseminate information to facilitate ATC services, it inevitably poses a higher security risk to ATC systems than when they were developed primarily with proprietary software.

[1] Internet Protocol (IP) is a communications standard describing how data are sent from one computer to another over the Internet.

[2] A Web application is a software program running on a Web server that can be accessed by using a Web browser. A Web server may host multiple Web applications. For purposes of this report, we use "Web application" to refer to either a Web application or a Web server.

Now, attackers can take advantage of software vulnerabilities in commercial IP products to exploit ATC systems, which is especially worrisome at a time when the Nation is facing increased threats from sophisticated nation-state-sponsored cyber attacks.

Accordingly, the objectives of this performance audit were to determine whether (1) Web applications used in supporting ATC operations are properly secured to prevent unauthorized access to ATC systems, and (2) FAA's network intrusion-detection capability is effective in monitoring ATC cyber-security incidents.

KPMG, LLP, of Washington, D.C., under contract to the Office of Inspector General (OIG), completed the audit work for the first objective. This work included vulnerability assessment and penetration testing on selected Web applications used in supporting ATC operations. We performed a quality control review of the audit work carried out by KPMG to ensure that it complied with generally accepted government auditing standards. In our opinion, KPMG's audit work complied with applicable standards. We supplemented KPMG's work by conducting an analysis of significant cyber incidents reported by FAA in recent years. KPMG's report detailing findings of vulnerabilities and penetration results was provided to FAA in November 2008 for corrective action. This report summarizes both KPMG's and our results.

We performed audit work to address the second objective. This work included analysis of FAA's cyber intrusion-detection capability and interviews with key personnel. We conducted our audit in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Details of our scope and methodology are described in Exhibit A.

RESULTS IN BRIEF

Web applications used in supporting ATC systems operations are not properly secured to prevent attacks or unauthorized access. In addition, FAA has not established adequate intrusion-detection capability to monitor and detect potential cyber security incidents at ATC facilities.

Web Applications Security

We tested 70 Web applications, some of which are used to disseminate information to the public over the Internet, such as communications frequencies for pilots and controllers; others are used internally within FAA to support eight ATC systems.[3] Our test identified a total of 763 high-risk, 504 medium-risk, and 2,590 low-risk vulnerabilities,[4] such as weak passwords and unprotected critical file folders.

By exploiting these vulnerabilities, the public could gain unauthorized access to information stored on Web application computers. Further, through these vulnerabilities, internal FAA users (employees, contractors, industry partners, etc.) could gain unauthorized access to ATC systems because the Web applications often act as front-end interfaces (providing front-door access) to ATC systems. In addition, these vulnerabilities could allow attackers to compromise FAA user computers by injecting malicious code onto the computers. During the audit, KPMG and OIG staff gained unauthorized access to information stored on Web application computers and an ATC system, and confirmed system vulnerability to malicious code attacks.

- Unauthorized access was gained to information stored on Web application computers associated with the Traffic Flow Management Infrastructure system, Juneau Aviation Weather System, and the Albuquerque Air Traffic Control Tower;

- Unauthorized access was gained to an ATC system used to monitor critical power supply at six en route centers; and

- Vulnerability found on Web applications associated with the Traffic Flow Management Infrastructure system was confirmed, which could allow attackers to install malicious codes on FAA users' computers.

[3] While Web technologies are used to support many ATC systems, this audit covered only the following eight systems: FAA's Air Route Traffic Control Center Critical Essential Power System Power Monitoring System (APMS), TECHNET, En Route Automation Modernization/En Route Information Display System (ERAM/ERIDS), Computer-Aided Engineering Graphics (CAEG), Automated Inventory Tracking System ver. 2 (AITSv2), Airport Surveillance Radar—Local Area Network (ASRLAN), Juneau Aviation Weather System (JAWS), and Traffic Flow Management Infrastructure (TFM-I).

[4] High-risk vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium-risk and low-risk vulnerabilities may provide an attacker with useful information, such as error messages revealing system configuration, that they can then use to compromise a computer system.

This occurred because (1) Web applications were not adequately configured[5] to prevent unauthorized access and (2) Web application software with known vulnerabilities was not corrected in a timely matter by installing readily available security software patches released to the public by software vendors.

Intrusion-detection Capabilities

To effectively monitor and detect potential cyber-security incidents on a network, intrusion-detection-system (IDS) sensors need to be installed at various critical network points. There, sensors automatically generate security alerts when potential cyber attacks are detected so that further incident response can be made. FAA's intrusion-detection capability is ineffective because of inadequate deployment of IDS sensors at the facility level and a lack of timely remediation of incidents detected. Specifically,

- ATC systems are located at hundreds of operational facilities such as en route centers, terminal radar approach control facilities, and airport control towers. However, IDS sensors have been deployed to only 11 of these ATC facilities. Further, none of the IDS sensors are installed to monitor ATC operational systems at these facilities, such as the IP-based network associated with the Host Computer System. Instead, these sensors provide monitoring coverage only for mission-support systems, such as e-mail systems.

- During Fiscal Year (FY) 2008, more than 800 cyber incident alerts were issued to the Air Traffic Organization (ATO), which is responsible for ATC operations. As of the end of FY 2008, over 150 incidents (17 percent) had not been remediated, including critical incidents in which hackers may have taken over control of ATO computers.

Without fully deploying IDS monitoring capability at ATC facilities and timely remediation against cyber incidents, FAA cannot take effective action to stop or prevent these cyber attacks, thus increasing the risk of further attacks on ATC systems.

In recent years, serious cyber attacks have occurred on FAA networks. For example, in February 2009, hackers compromised an FAA public-facing Web application computer and used it as a conduit to gain unauthorized access to personally identifiable information (PII) on 48,000 current and former FAA employees. In 2008 hackers took control of FAA's critical network servers

[5] Software configuration involves setting up a software system for one's particular uses, such as changing a factory-set default password of "PASSWORD" to one less easily guessed.

(domain controllers) and gained the power to shut down the servers, which could cause serious disruption to FAA's mission-support network. In 2006 a viral attack, widely distributed on the Internet, spread to FAA's ATC systems, forcing FAA to shut down a portion of its ATC systems in Alaska.

In our opinion, unless effective action is taken quickly, it is likely to be a matter of *when,* not *if,* ATC systems encounter attacks that do serious harm to ATC operations. As indicated by the former Director of National Intelligence,

> "Our information infrastructure . . . increasingly is being targeted for exploitation and potentially for disruption or destruction. . . . Terrorist groups . . . have expressed the desire to use cyber means to target the United States. . . . It is no longer sufficient for the U.S. Government to discover cyber intrusions in its networks, clean up the damage, and take legal or political steps to deter further intrusions. We must take proactive measures to detect and prevent intrusions from whatever source, as they happen, and before they can do significant damage."[6]

We made a series of recommendations beginning on page 11 to help enhance security over Web applications used in supporting ATC operations and improve the effectiveness of FAA's cyber-incident-monitoring and -response capabilities. FAA concurred with all of our recommendations, and recognized that constant vigilance and effective action are the keys to addressing cyber security in its ATC systems. The response can be found in its entirety in Appendix A.

FINDINGS

Web Applications Used in Supporting ATC Systems Operations Are Not Properly Secured

Web applications used in supporting ATC systems operations are not properly secured to prevent attacks or unauthorized access. KPMG staff conducted two separate security tests—one originated from the Internet and the other from FAA Headquarters' mission-support network. Due to time and resource constraints, only 70 Web applications were tested. Thirty-five of these Web applications are

[6] *Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence* (J. Michael McConnell, Director of National Intelligence, February 5, 2008).

used by FAA to disseminate information to the public over the Internet, such as communications frequencies for pilots and controllers; others are used internally within FAA to support the eight ATC systems. The tests identified a total of 763 high-risk, 504 medium-risk, and 2,590 low-risk vulnerabilities (see Table 1).

Table 1. Internet-based and Internal Security Testing Results

	Number of Web Applications Tested	Number of Vulnerabilities and Risk Level		
		High	**Medium**	**Low**
Internet-based (Public Use)	35	212	169	1,037
Internal (FAA Use)	35	551	335	1,553
Total	**70**	**763**	**504**	**2,590**

Source: KPMG

High-risk vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium-risk and low-risk vulnerabilities may provide an attacker with useful information, such as error messages revealing system configuration, that they can then use to compromise a computer system. The following are examples of risks to ATC systems as a result of Web application vulnerabilities:

- ***Vulnerabilities allowed unauthorized access to information stored on Web application computers.*** Vulnerabilities found in Web application computers associated with the Traffic Flow Management Infrastructure system, Juneau Aviation Weather System, and the Albuquerque Air Traffic Control Tower allowed KPMG and OIG staff to gain unauthorized access to data stored on these computers, including program source code and sensitive PII.

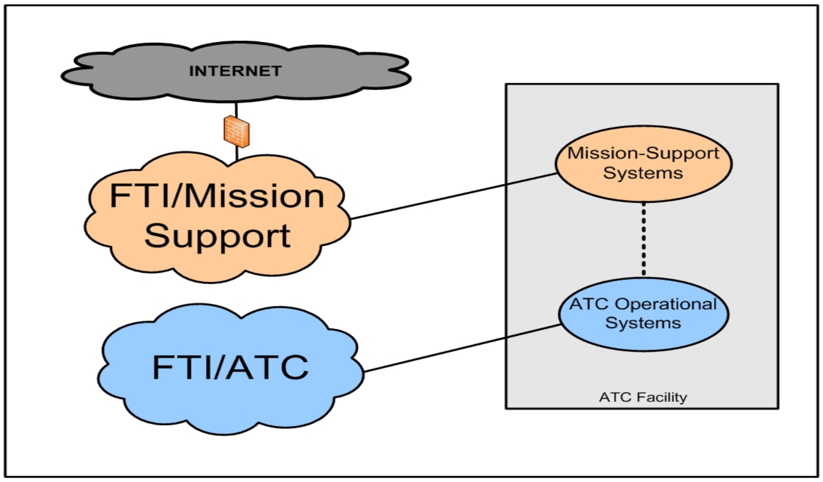
- ***Vulnerable Web applications were used as conduits to gain unauthorized access to and potentially compromise ATC system operations.*** Through vulnerable Web applications, KPMG staff gained unauthorized access to the Power Monitoring System at six en route centers—Anchorage, Boston, Denver, Oakland, Salt Lake City, and Seattle. While this system is not used to separate aircraft, it provides the critical mission-support function of eliminating voltage dropouts and surges caused by sources outside ATC facilities. The unauthorized access enabled KPMG staff to generate power condition reports, which could be used by attackers as intelligence information for planning attacks. A similar incident actually occurred in

February 2009. By using a vulnerable public-facing Web application computer as a conduit, hackers gained unauthorized access to 48,000 PII records stored in an FAA database.

- ***Vulnerable Web applications could allow attackers to execute malicious codes on FAA users' computers.*** This vulnerability was found on Web applications associated with the Traffic Flow Management Infrastructure system. Once infected via these applications, FAA user computers would take orders from hackers to attack other computers or send critical network information to hackers ("exfiltration").[7] A similar incident actually occurred in August 2008. By executing malicious codes, hackers took control of FAA's critical network servers (domain controllers) and gained the power to shut down the servers, which could have caused serious disruption to FAA's mission-support network.

So far most attacks have primarily disrupted FAA's ATC mission-support function. However, it is important to understand that attacks can spread from the mission-support network to the operational network—where real-time surveillance, communications, and flight information is processed to separate aircraft—because of network connections, as shown in Figure 1.

Figure 1. ATC IP-based Network Infrastructure[a]



[a] This infrastructure consists primarily of the backbone FAA Telecommunications Infrastructure (FTI) and several local area networks; FAA relies on this infrastructure to conduct ATC operations. ATC systems are hosted on local area networks at ATC facilities, which have connections to both FTI operational and mission-support networks. (Source: OIG)

[7] In recent years, huge amounts of U.S. Government (including Department of Transportation) and commercial data were "exfiltrated" to foreign domains on the Internet. This has resulted in a sweeping effort to strengthen Government-wide cyber security by the Office of Management and Budget.

Because of network connections—authorized (such as performing system maintenance) and unauthorized (such as inadequate network setup)—between FAA's mission-support and ATC systems, the risk of cyber attacks is magnified. These FAA security-related events of recent years highlight the risk of cyber attacks:

- In FY 2006, we reported that FAA's Remote Maintenance Monitoring System was connected to the less-secure mission-support network, which created security exposure to ATC operations;

- In FY 2006, a viral attack originating from the Internet spread from administrative networks to ATC systems, forcing FAA to shut down a portion of its ATC systems in Alaska;

- In FY 2008, hackers took over FAA computers in Alaska, becoming FAA "insiders." By taking advantage of FAA's interconnected networks, hackers later stole FAA's enterprise administrator's password in Oklahoma, installed malicious codes with the stolen password, and compromised FAA's domain controller in its Western Pacific Region. At that point, hackers had the ability to obtain more than 40,000 FAA user IDs, passwords, and other information used to control a portion of the FAA mission-support network.

- In FY 2009, hackers compromised an FAA public-facing Web application computer on the Internet and used it as a conduit to enter an FAA internal database server. Included in the server was PII on 48,000 current and former FAA employees, including names, dates of birth, Social Security numbers, pay grades/bands, addresses, veterans' preferences, usernames and passwords, and education/medical/health information.

These Web vulnerabilities occurred because (1) Web applications were not adequately configured to prevent unauthorized access and (2) Web application software with known vulnerabilities was not corrected in a timely manner by installing readily available security software patches released to the public by software vendors.

Intrusion-detection Capabilities Are Not Adequate to Protect ATC Systems

As previously shown in Figure 1, the ATC IP-based network infrastructure consists primarily of its backbone FTI wide-area network and numerous local area networks within ATC facilities. While the FTI wide-area network is monitored by an FAA contractor, FAA relies on DOT's Cyber Security Management Center

(CSMC) to monitor cyber incidents at the facility level. Adequate monitoring is critical for ensuring timely detection of network security incidents. However, FAA's intrusion-detection capability is ineffective because of inadequate deployment of IDS sensors and a lack of timely remediation of incidents detected. Specifically,

- ***Cyber incidents were not effectively monitored at ATC facilities.*** To identify potential cyber incidents, FAA needs IDS sensors installed at key locations to collect critical information for security analyses. ATC systems are located at hundreds of operational facilities such as en route centers, terminal radar approach control facilities, airport control towers, and flight service stations. However, IDS sensors have been deployed to only 11 of these ATC facilities—five en route centers, four terminal radar approach control facilities or airport traffic control towers, and the Technical Center in Atlantic City and Mike Monroney Aeronautical Center in Oklahoma City (see Table 2).

Table 2. CSMC IDS Sensor Coverage

		Number of Facilities with IDS Sensors Installed	
Major ATC Facilities	**Total Number of Facilities**	**ATC Network**	**Mission-support Network**
En route centers	21	0	5
Terminal radar approach control facilities	166	0	4
Airport traffic control towers	512		
Flight service stations	33	0	0
FAA Technical Center	1	0	1
Mike Monroney Aeronautical Center	1	0	1
Remote Sites	*	0	0
Total	**734**[#]	**0**	**11**

[*] in the thousands

[#] excluding remote sites

Source: FAA

Further, these IDS sensors provide monitoring coverage only for mission-support systems at these facilities, not for ATC operational systems. As a result, CSMC has little visibility into operations at ATC facilities, and cannot identify potential cyber attacks against ATC operational systems.

According to CSMC and ATO management officials, effective IDS deployment requires close cooperation between CSMC and ATO. However, this cooperation has been lacking. Insufficient understanding of FAA network infrastructure was also a contributing factor, resulting in deployment of IDS sensors on an ad-hoc basis, which made CSMC monitoring of ATC systems less effective. For example, FAA has not fully studied the connectivity of its network infrastructure (network mapping), including the locations of critical network points.

- ***Cyber incidents were not remediated in a timely manner.*** Once a cyber incident is detected, it must be examined and remediated quickly to minimize the security risk to the network. During FY 2008, ATO received 877 cyber-incident alerts from CSMC. As of the end of FY 2008, 151 incidents (17 percent) were still unresolved. Fifty of these had been open for more than 3 months, including critical incidents in which hackers may have taken over control of ATO computers.

  According to both CSMC and ATO officials, the lack of needed information—such as IDS sensor data, critical data being collected on a network device in real-time (logging), and complete IP address information—was a major factor in being unable to pinpoint the actual network location when an incident occurred or the computer affected by the incident. This lack of information has significantly impeded ATO's ability to respond to cyber incidents. For example, in March 2008, ATO officials directed CSMC to close over 60 unresolved cyber incidents identified in FYs 2006 and 2007, stating that they were "nonactionable due to inability to perform further analysis because of time considerations."

The Federal Information Security Management Act of 2002 requires agencies to have procedures for detecting, reporting, and responding to security incidents. Without effectively deploying IDS monitoring capability at ATC facilities, FAA cannot be fully aware of potential cyber attacks on ATC systems. More seriously, the lack of timely remediation against cyber incidents left unsecured FAA computers on its networks. As a result, FAA cannot take effective action to stop or prevent these cyber attacks, which increases the risk of further attacks on ATC systems.

RECOMMENDATIONS

We recommend that the Acting Federal Aviation Administrator direct FAA's Chief Information Officer and ATO's Chief Operating Officer to:

1. Ensure that all Web applications used in ATC systems are configured in compliance with Government security standards;

2. Strengthen the patch management process by (a) identifying Web applications with known vulnerabilities, and (b) promptly installing relevant security patches in a timely manner;

3. Take immediate action to correct high-risk vulnerabilities and establish a timetable for remediation of all remaining vulnerabilities identified during this audit;

4. Resolve differences with CSMC and establish a timetable for deploying IDS monitoring devices covering local area networks at all ATC facilities; and

5. In conjunction with CSMC officials, identify the information needed for remediation and establish procedures to ensure timely remediation of cyber incidents based on incident criticality as assessed by CSMC.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided FAA with our draft report on March 3, 2009, and received its response on April 16, 2009. FAA concurred with all of our recommendations, and said that it recognized that constant vigilance and effective action are the keys to addressing cyber security in its ATC systems. FAA also pointed out that a critical element of its cyber security is the separation of the network infrastructure between the National Airspace System (NAS) for aircraft separation and FAA administrative/ATC mission-support systems. We recognize the separation of FAA's network infrastructure. However, as stated in our report, cyber attacks can spread from the mission-support network to the NAS network because of system interconnections.

FAA further stated that it recognized the importance of dealing with all system vulnerabilities and will treat vulnerabilities in this report with the utmost diligence.

FAA’s response can be found in its entirety in Appendix A. The responses to our recommendations are summarized as follows:

Recommendation 1: Concurred. FAA stated that it is actively analyzing the identified vulnerabilities, and will develop new Plans of Action and Milestones (POA&Ms) based on the analysis. The analysis was scheduled for completion by April 30, 2009. FAA uses the DOT Secure Web Application Standards as the basis for securely configuring Web applications, and will ensure that the Web applications identified in our report are in compliance with these standards. New system POA&M items will be developed by July 31, 2009.

Recommendation 2: Concurred. FAA stated that security patching vulnerabilities identified in our report will be addressed via the ATO Certification and Accreditation Remediation Management process. The ATO audit/compliance team will audit the existence of appropriate security patches. Patch implementation will be performed in accordance with established FAA configuration management processes. These corrective actions will be included in system POA&Ms by July 31, 2009.

Recommendation 3: Concurred. FAA will ensure that the high-rated vulnerabilities correlated to FAA systems are handled with high priority for immediate implementation. Implementation will be tracked via the POA&M process. FAA is now reviewing detailed data from our testing to assess the criticality of the vulnerabilities identified. The review was scheduled for completion by April 30, 2009. Based on the findings, FAA will develop a timetable for remediation by July 31, 2009. However, FAA agreed to take immediate action to fix critical vulnerabilities. In follow-up meetings, FAA committed to sharing its April evaluation results and action plan on fixing critical vulnerabilities with us in May 2009.

Recommendation 4: Concurred. While FAA believes that its relationship with CSMC is essentially sound, within 30 days the FAA CIO—along with the CIO for ATO—will meet with CSMC leadership to discuss strengths and weaknesses of interactions between their organizations and identify any areas in need of improvement.

As an additional level of protection, internal NAS facility IP demarcation points between NAS entities and mission-support entities have been identified by FAA as requiring additional IDS sensors to be installed. FAA plans to implement IDS capability at the facilities housing one of the NAS systems (ARTS IIIE) in

February 2010. A deployment strategy for the remaining automation systems will be developed in December 2009.

Recommendation 5: Concurred. ATO has recently implemented two process improvements: a Reconciliation of Findings process and an Open Incident Handling process, thereby reducing the number of open incidents. In conjunction with CSMC, ATO has taken steps to improve timely response of cyber incidents. Specifically, CSMC and ATO are working together through focused meetings and cyber security-related workshops to refine the process of identifying the criticality of incidents for remediation. A refined process will be developed in August 2009.

ACTIONS REQUIRED

FAA's actions taken and planned are responsive to our recommendations and are considered resolved. These actions are also subject to follow-up provisions in Department of Transportation Order 8000.1C.

We appreciate the courtesies and cooperation of the FAA Office of the Chief Information Officer, ATO, CSMC, OST, and KPMG representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407 or Dr. Ping Z. Sun, Program Director, at (202) 366-1478.

#

cc: Acting Chief Information Officer, DOT
Chief Information Officer, FAA
Chief Operating Officer, ATO
Martin Gertel, M-1
Anthony Williams, ABU-100

EXHIBIT A. SCOPE AND METHODOLOGY

This audit was conducted by KPMG of Washington, D.C., under contract to DOT OIG, and by OIG staff. The audit was conducted at FAA Headquarters, CSMC, selected FAA facilities and at the FTI operational center in Melbourne, Florida.

OIG staff performed an Internet search and reviewed the ATO Risk Assessment Process Site Survey Plan. The search and review generated two lists of Web applications used to support ATC operations. The lists served as a basis for KPMG's conducting the external and internal vulnerability assessment/penetration tests. OIG staff also conducted an analysis of significant cyber incidents identified by FAA.

KPMG's detailed methodology is documented in its report. The following summarizes the contractor's scope and methodology:

- The contractor performed an external vulnerability assessment/penetration test by using open-source (freeware) and commercial scanning software. The test was done through an Internet connection at KPMG Headquarters. Based on OIG input, a total of 35 public-accessible Web application computers were included during the test.

- The contractor performed an internal vulnerability assessment/penetration test by using open-source and commercial scanning software. The test was conducted at FAA Headquarters. Based on OIG input, a total of 35 internal Web application computers were included in the test. To reduce any potential impact on ATC operations, a portion of the test was conducted at night.

OIG staff visited the FTI Security Operations Control Center in Melbourne, Florida, and the DOT CSMC in Leesburg, Virginia. We interviewed Center officials, examined available data pertaining to identified cyber incidents, and reviewed intrusion-detection monitoring policies and procedures.

The audit work was performed between June 2008 and January 2009. We conducted our audit in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Dr. Ping Zhong Sun	Program Director for IT Audit Computer Laboratory
Mitchell Balakit	Contracting Officer's Technical Representative
Vasily Gerasimov	Computer Scientist
Michael P. Fruitman	Writer-Editor

APPENDIX A. MANAGEMENT COMMENTS

Federal Aviation Administration

Memorandum

Date: April 16, 2009

To: Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits

From: Ramesh K. Punwani, Assistant Administrator for Financial Services/CFO

Prepared by: Anthony Williams, x79000

Subject: OIG Draft Report: Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems

The Federal Aviation Administration (FAA) appreciates the Department of Transportation (DOT) Office of the Inspector General (OIG) efforts in the subject draft report that will assist FAA in identifying weaknesses in the FAA web infrastructure that have not previously been detected.

FAA operates with the ongoing knowledge that Cyber security is one of the key components to the safe operation of the National Air Space System (NAS) and Cyber security is a top priority for FAA as identified in the FAA Flight Plan. The Air Traffic Organization (ATO) places the highest priority on pursuing and maintaining a safe and secure Air Traffic Control (ATC) system.

ATO recognizes that constant vigilance and effective and expeditious action are the keys to addressing Cyber security in its ATC systems. It has demonstrated its commitment to ensuring NAS safety and Cyber security through the extensive measures it has taken to reduce the risk of Cyber attack. Some of these steps include: implementing a comprehensive Information System Security (ISS) Program in support of Federal Information Security Management Act (FISMA) requirements; separating NAS operational ATC systems from Mission Support and Administrative systems; identifying and fixing Cyber security weakness in a prioritized process, with expedited processes in place to address critical issues identified as high priority; and modernizing ATO Cyber security through improvements in processes and technology.

One important element of NAS system Cyber security is the separation of infrastructure elements. Specifically, the FAA networking infrastructure is comprised of two major networks that are separated physically and logically:

- The FAA Administrative/ATC Mission Support (Admin/MS) Network: Provides Wide Area Network (WAN) support to FAA services, except ATC operations.
- The National Airspace System (NAS) Network: Provides WAN services that support ATC operations. ATC systems are prohibited by FAA Order 1370.95, Wide Area Network Connectivity Security, from directly connecting to the FAA Admin/MS Network or any other on-NAS network.

The OIG report findings focus entirely on vulnerabilities associated with Admin/MS system assets. The OIG used commercially available scanning tools to assess the security of the Admin/MS elements of the ATO infrastructure and vulnerabilities were identified. FAA recognizes the importance of dealing with all identified system vulnerabilities in a logical and orderly manner, and will treat vulnerabilities identified in the OIG report with the utmost diligence and conduct mitigation to include as many families of vulnerabilities as possible in parallel. Immediate attention will be focused on mitigating high and moderate risk vulnerabilities in FAA public facing websites and FAA websites that provide Mission Support services.

OIG Recommendation 1: Ensure that all Web applications used in ATC systems are configured in compliance with Government security standards.

FAA Response: Concur. The FAA Telecommunications Infrastructure (FTI) NAS IP WAN currently has intrusion-detection-system (IDS) sensors deployed that monitor data flow into and out of 27 ATC NAS operational facilities, which provides coverage for all NAS IP connected facilities. In addition, internal NAS facility IP demarcation points between NAS entities and Mission Support entities have been identified by the FAA as requiring additional IDS sensors to be installed. Vulnerabilities identified in the OIG report will be prioritized based on their level of risk and addressed through the ATO Certification and Accreditation (C&A) Remediation Management process. Web applications are also assessed as part of system C&A Risk Assessments conducted on a 3-year cycle, and will receive continued scrutiny and attention as risks are identified.

FAA is actively analyzing the OIG audit report raw data, which will correlate OIG report findings to FAA systems so that new Plans of Action and Milestones (POAMs) can be developed. The analysis will be complete by April 30, 2009. The FAA uses the DOT Secure Web Application Standards as the basis for securely configuring web applications and will ensure that the web applications identified in the OIG report are in compliance with these standards. New system POAM items will be developed by July 31, 2009; however, FAA will take immediate corrective action on any critical vulnerabilities.

In addition, the ATO ISS Program Compliance/Audit Plan ensures that FAA has a valid NAS ATC operational web application inventory that is configured in accordance with DOT Secure Web Application Standards.

OIG Recommendation 2: Strengthen the patch management process by (a) identifying Web applications with known vulnerabilities, and (b) promptly installing relevant security patches in a timely manner.

FAA Response: Concur. Security patching vulnerabilities identified in the OIG report will be addressed via the ATO C&A Remediation Management process. The vulnerabilities identified by OIG are being assessed, and remediation actions will be prioritized based on the level of risk presented. As part of the ATO ISS Program Compliance/Audit Plan defined in Recommendation 1, the audit/compliance team will be auditing the existence of appropriate security patches. The FAA is analyzing the specific scanning tool report data provided by OIG and is correlating findings to FAA systems for POAM development. Patch implementation will be performed in accordance with established FAA configuration management processes. System POAM items will be developed by July 31, 2009; however, FAA will take immediate corrective action on any critical vulnerabilities.

As part of its standardized process for patch management, ATO Security Certification Teams are responsible for ensuring that patch management procedures are properly developed and implemented. The ATO has developed a Standard Operating Procedure (SOP) template and guidance document for the NIST SP 800-53 System Integrity (SI) control family that defines the patch management procedures to be implemented for each system. The ATO ISS Program conducted a workshop in December 2008 to review the security SOP guidance and ensure that Security Certification Teams and System Owners understand the procedure development requirements. FAA will continue its efforts to ensure that this process results in the timely and effective implementation of system patches.

OIG Recommendation 3: Take immediate action to correct high-risk vulnerabilities and establish a timetable for remediation of all remaining identified during this audit.

FAA Response: Concur. FAA recognizes that the vulnerability scanning tools used to perform the OIG Web Audit did identify some vulnerabilities in the Admin/MS systems. The FAA takes all security vulnerabilities very seriously and will ensure that the high rated vulnerabilities that are correlated to FAA systems as part of the actions defined in the responses to Recommendations 1 and 2 are handled as high priority configuration management changes for immediate implementation. Implementation will be tracked via the POAM process. The FAA is now reviewing the detailed data from the OIG's testing. As part of that review, it is evaluating the extent of which those vulnerabilities identified in the draft report as high risk coincide with FAA's definition of high risk and conform to NIST standards. In addition, vulnerabilities identified by FAA internal scans are also receiving priority attention and will be remediated. Lower priority issues will be addressed as appropriate. The review of vulnerabilities identified by the OIG will be completed April 30, 2009. Based on the findings, the FAA will develop a timetable for remediation by July 31, 2009; however, FAA will take immediate corrective action on any critical vulnerabilities.

OIG Recommendation 4: Resolve differences with Cyber Security Management Center (CSMC) and establish a timetable for deploying IDS monitoring devices covering local area networks at all ATC facilities.

FAA Response: Concur. FAA intends to ensure that it has a smooth and effective working relationship with the CSMC that is conducive to expeditious and effective interactions. While FAA believes that the relationship with CSMC is essentially sound, within 30 days, the FAA

Chief Information Officer (CIO) along with the CIO for ATO will meet with the CSMC leadership to discuss strengths and weaknesses of interactions between their organizations and identify any areas in need of improvement. In addition, the FAA CIO is creating service level agreements with all FAA lines of business.

In regard to IDS monitoring devices, FAA has actions underway to complete its network of IDS monitoring systems and is currently implementing and monitoring boundary and internal network protection measures.

As an added measure of NAS operations network protection, the FAA FTI NAS IP WAN currently has IDS sensors deployed that monitor data flow into and out of 27 ATC NAS operational facilities, which provides coverage for all NAS IP connected facilities. The FTI NAS IP WAN is configured to provide these IDS sensors with visibility into the data traffic traveling into and out of the NAS operational LAN infrastructures as well as all other NAS IP WAN connected facility LANs. This existing configuration allows for reviewing the majority of IP data traffic that is used for NAS ATC operational systems. Additionally, the FTI service has a Security Operations Center that monitors the IDS sensor data and works with appropriate FAA Cyber security organizations, including the CSMC, to resolve security events.

As an additional level of protection, internal NAS facility IP demarcation points between NAS entities and Mission Support entities have been identified by the FAA as requiring additional IDS sensors to be installed. While it would not be appropriate to discuss the specific demarcation points in this memo, FAA would be happy to provide details to the OIG in another forum. However, we note that some of these IDS systems will be fully operational this year, having passed key site testing on March 10, 2009. The current completion date for the implementation of all IDS's at ARTS IIIE facilities is February 2010. A deployment strategy for the remaining automation systems will be developed by December 2009.

OIG Recommendation 5. In conjunction with CSMC officials, identify the information needed for remediation and establish procedures to ensure timely remediation of cyber incidents based on criticality as assessed by CSMC.

FAA Response: Concur. The ATO has recently implemented two process improvements: a Reconciliation of Findings process; and an Open Incident Handling process, thereby reducing the number of open incidents. The improved processes have reduced the amount of time to respond to new CSMC findings, provided more efficient tracking of all open findings, and allowed for more comprehensive documentation and reporting capability.

In conjunction with CSMC, ATO has taken steps to improve timely response of cyber incidents. Specifically, the CSMC and ATO are working together through focused meetings and cyber security related workshops to refine the process of identifying the criticality of information for event remediation. A refined process will be developed by August 2009.

S:\\ABU-100\Share\OIG GAO\08-30 Web Applications Security doc:ARWilliams 4/16/09

The following pages contain textual versions of the tables and figure found in this document. These pages were not in the original document but have been added here to accommodate assistive technology.

Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems.

Section 508 Compliance Presentation.

Table 1. Internet-based and Internal Security Testing Results.

35 Internet-based or public use web applications were tested. On those web based applications 212 high risk, 169 medium risk, and 1,037 low risk vulnerabilities were found.

35 internal or Federal Aviation Administration use web applications were tested. On those web based applications 551 high risk, 335 medium risk, and 1,553 low risk vulnerabilities were found.

The total number of tested web application was 70. A total of 763 high-risk, 504 medium-risk and 2,590 low-risk vulnerabilities were found.

Source: KPMG.

Figure 1. Air Traffic Control Internet Protocol Based Network Infrastructure.

This infrastructure consists primarily of the backbone Federal Aviation Administration Telecommunications Infrastructure and several local area networks; Federal Aviation Administration relies on this infrastructure to conduct Air Traffic Control operations. Air Traffic Control systems are hosted on local area networks at Air Traffic Control facilities, which have connections to both Federal Aviation Administration Telecommunications Infrastructure operational and mission-support networks.

Table 2. Cyber Security Management Center Intrusion Detection Systems Sensor Coverage.

For the en route centers, the total number of facilities was 21, the number of facilities with Intrusion Detection Systems sensors installed on the Air Traffic Control network was 0 and the number of facilities with Intrusion Detection Systems sensors installed on the mission-support network was 5.

For the terminal radar approach control facilities, the total number of facilities was 166. For the airport traffic control towers the number of facilities was 512. For the combined terminal radar approach control facilities and airport traffic control tower facilities the number of facilities with Intrusion Detection Systems sensors installed on the Air Traffic Control network was 0 and the combined number of facilities with Intrusion Detection Systems sensors installed on the mission-support network was 4.

For the flight service stations, the total number of facilities was 33, the number of facilities with Intrusion Detection Systems sensors installed on the Air Traffic Control network was 0 and the number of facilities with Intrusion Detection Systems sensors installed on the mission-support network was 0.

For the Federal Aviation Administration Technical Center, the total number of facilities was 1, the number of facilities with Intrusion Detection Systems sensors installed on the Air Traffic Control network was 0 and the number of facilities with Intrusion Detection Systems sensors installed on the mission-support network was 1.

For the Mike Monroney Aeronautical Center, the total number of facilities was 1, the number of facilities with Intrusion Detection Systems sensors installed on the Air Traffic Control network was 0 and the number of facilities with Intrusion Detection Systems sensors installed on the mission-support network was 1.

For the remote sites, the total number of facilities is in the thousands, the number of facilities with Intrusion Detection Systems sensors installed on the Air Traffic Control network was 0 and the number of facilities with Intrusion Detection Systems sensors installed on the mission-support network was 0.

The total number of major Air Traffic Control facilities was 734, excluding the remote sites. The total number of facilities with Intrusion Detection Systems sensors installed on the Air Traffic Control network was 0 and the total number of facilities with Intrusion Detection Systems sensors installed on the mission-support network was 11.

Source: Federal Aviation Administration.