# Memorandum

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

Subject: ACTION: Quality Control Review on the
Vulnerability Assessment of FAA's Operational Air
Traffic Control System
Report Number QC-2011-047

Date: April 15, 2011

From: Louis C. King
Acting Assistant Inspector General for Financial
and Information Technology Audits

Reply to
Attn. of: JA-20

To: Federal Aviation Administrator

This report summarizes the results of our information technology vulnerability assessment of the Federal Aviation Administration's (FAA's) operational Air Traffic Control (ATC) systems. This audit was requested by the now-Chairmen of the House Transportation and Infrastructure Committee and the Subcommittee on Aviation.

FAA has 21 Air Route Traffic Control Centers (ARTCC) geographically dispersed across the United States. These Centers are the major communication hubs for flight plan routing and the systems that provide radar and communication services to aircraft operating above 18,000 feet. ATC systems communicate with one another via the same technology used for Internet communication. Although not all ATC systems can be accessed from the Internet, FAA has designed some support systems residing within its Mission Support/Administrative System Network (MSSN) with accessibility through the Internet.

This audit assessed ATC systems and networks located at two FAA facilities within the continental United States. Clifton Gunderson LLP of Calverton, Maryland, completed the audit under contract to the Office of Inspector General (OIG). Clifton Gunderson's audit approach included developing and executing steps within OIG-approved Rules of Engagement (ROE). ROE establish guidelines that determine how selected security tests are conducted. OIG staff performed a quality control review of Clifton Gunderson's audit work to ensure that it complied with generally accepted government auditing standards. Our review disclosed no instances in which Clifton Gunderson did not comply in all material respects with applicable auditing standards. A detailed report was provided to FAA but will not be released to the public due to the sensitivity of the information it contains.

The objective of this audit was to determine whether operational ATC systems can be accessed by unauthorized users from inside ATC facilities through FAA's MSSN. Clifton Gunderson concluded that they were unable to gain access to FAA's operational ATC systems. However, they identified the following weaknesses at the ARTCCs: 1) information disclosure vulnerability; 2) inadequate system patch levels and unsupported operating systems; 3) improper network configurations; and 4) communication system vulnerabilities.

## 1. Information Disclosure Vulnerability

Clifton Gunderson identified an information disclosure vulnerability during testing at one ARTCC that allowed them to view, without using a password, hundreds of pages of sensitive technical information describing network configuration, gateways and other devices. This sensitive information may provide a rogue employee or contractor sufficient understanding to identify and exploit weaknesses in the ATC security structure.

## 2. Patch Management Vulnerabilities on FAA's MSSN

Clifton Gunderson's review of MSSN revealed several critical and high risk Common Vulnerabilities and Exposures (CVE)[1] related to missing or outdated system patches or the running of operating systems no longer supported by their vendors. System patch levels and operating systems that are not kept current not only may result in system unavailability, but may also create a risk of exploitation of security holes for access to ATC systems and data. Any of these systems could be compromised, and allow the attacker to use the system to hide his or her identity in order to launch more attacks.

[1] The Mitre Corporation maintains a database of Common Vulnerabilities and Exposures (CVE) and shares it with the world-wide information technology user community at http:cve.mitre.org/about/faqs.html.

### 3. System Configuration Vulnerabilities on FAA's MSSN

Clifton Gunderson's review of MSSN also revealed several critical and high risk CVEs related to improper system configurations. An attacker could leverage these vulnerabilities to gain total control of the systems. Furthermore, the systems could be used to compromise other systems that depend on the same network management and configuration services.

### 4. Communication System Weaknesses

Clifton Gunderson's review identified a communication system at one location that does not require complex passwords and is no longer supported by the vendor. This lack of sufficiently complex passwords could lead to an unauthorized manipulation of the communication system, a total system shutdown, or falsification and impersonation of facility communications.

Clifton Gunderson's recommendations to correct these and other control deficiencies appear in this report's Exhibit A.

## ACTIONS REQUIRED

Clifton Gunderson provided FAA a draft of the report on February 26, 2011, and received FAA's written comments on April 12, 2011. FAA concurred with all audit findings and recommendations, and has agreed to develop plans to implement corrective actions to remediate all weaknesses. We request that FAA give us a written response that includes specific action taken or planned for each recommendation and target dates for completion.

In accordance with DOT Order 8000.1C, the corrective actions taken in response to Clifton Gunderson's recommendations are subject to follow-up.

We appreciate the courtesies and cooperation of Department of Transportation's representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-4350, or Nathan Custer, Program Director, at (202) 366-5540.

Attachments

#

cc: Chief Information Officer, DOT
Chief Operating Officer, ATO
Assistant Administrator for Information Services/CIO, FAA
Martin Gertel, M-1
Anthony Williams, AAE-001

## EXHIBIT A. RECOMMENDATIONS OF CLIFTON GUNDERSON, LLP, INDEPENDENT AUDITOR

Clifton Gunderson LLP made the following recommendations during its Vulnerability Assessment of FAA's Operational Air Traffic Control System. OIG agrees that FAA management should implement these recommendations in order to enhance FAA's ATC controls.

### Information disclosure vulnerability

1. Restrict access to this site by requiring users to enter ID's and passwords, after demonstrating a valid business need or justification to access this data.

2. Review the value of the information available on the site which should be otherwise protected from dissemination.

3. Review and monitor individual accesses to this information to ensure documents accessible are appropriate based on the level of the user's need to know.

4. Monitor (for reasonableness) any distribution or download of any document which provides information otherwise protected from dissemination.

### Patch management vulnerabilities on the FAA MSSN

5. Apply software patch releases on a timely basis to protect against known vulnerabilities.

6. Ensure the system's Authorizing Official (AO) is promptly informed and a risk acceptance is received for any Critical or High vulnerabilities that are not promptly addressed. If the risk acceptance lapses, or the situation changes, the AO should renew the acceptance of the risk to ensure he/she is kept aware of the unmitigated vulnerabilities present on the system.

7. Upgrade system software and supporting applications to a vendor acceptable supported version.

**System configuration vulnerabilities on MSSN**

8. We recommend FAA management disable unneeded network services where it is determined they are unnecessary or do not serve a valid business purpose.

**Communications system weaknesses**

9. Upgrade the communications operating system to a supported version.
10. Require passwords meet complexity requirements in accordance with DOT/FAA policies.