**U.S. Department of Transportation**

Office of the Secretary
of Transportation

The Inspector General

Office of Inspector General
Washington, DC 20590

August 5, 2010

The Honorable John L. Mica
Ranking Member
Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

The Honorable Thomas Petri
Ranking Member
Subcommittee on Aviation
Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Dear Ranking Members Mica and Petri:

This letter is in response to your June 10, 2009, roundtable discussion regarding the air traffic control (ATC) system's vulnerability to cyber attack. During the meeting, you requested that my office review the Federal Aviation Administration's (FAA's) progress in implementing the five recommendations from our May 4, 2009, report: *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems.*

In short, FAA has implemented all recommendations except one—deployment of intrusion detection devices to protect ATC system operations. The following table summarizes the status of each recommendation.

| Recommendations | Status |
|---|---|
| 1. Ensure that all Web applications used in the Air Traffic Control (ATC) systems are configured in compliance with Government security standards. | Complete |
| 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. | Complete |
| 3. Take immediate action to correct high-risk vulnerabilities and establish a timetable for remediation of all remaining vulnerabilities identified during this audit. | Complete |
| 4a. Resolve differences with the Cyber Security Management Center (CSMC). | Complete |
| 4b. Establish a timetable for deploying intrusion-detection system (IDS) monitoring devices covering local area networks at all ATC facilities. | Open |
| 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. | Complete |

FAA originally agreed to develop an IDS deployment strategy for all ATC facilities by December 2009 and complete deployment of IDS capabilities at facilities housing the ARTS IIIE[1] by February 2010. Currently, FAA has completed installation at 7 of the 11 ARTS IIIE facilities. FAA has delayed deploying the remaining four ARTS IIIE facilities until January 2011 because critical ARTS IIIE system-wide software upgrades have a priority over IDS installation. FAA has not yet established a timetable for deploying IDS at the remaining ATC facilities. Without IDS capabilities, FAA cannot effectively monitor ATC systems for possible cyber attacks or take action to stop them. We have discussed our concerns with FAA's action plan with the Chief Information Officers for the Department and FAA and have discussed the significant delays in implementing IDS at remaining facilities with Air Traffic Organization (ATO) senior management. ATO management is developing an implementation strategy to address this issue but could not provide a timetable beyond the ARTS IIIE facilities. We will continue to monitor FAA's progress in this area and keep you apprised of any significant changes.

[1] Automated Radar Terminal System IIIE is a sophisticated computer system used by controllers at major U.S. airports to detect, track, and predict aircraft positions.

Thank you for your inquiry and interest. If you have any questions or need further information, please contact me at (202) 366-1959 or Louis King, Acting Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1407.

Sincerely,

Calvin L. Scovel III

Calvin L. Scovel III
Inspector General