Audit: Air traffic systems vulnerable to attack

May 6 2009, By LOLITA C. BALDOR , Associated Press Writer

(AP) -- The nation's air traffic control systems are vulnerable to cyber attacks, and support systems have been breached in recent months allowing hackers access to personnel records and network servers, according to a new report.

The audit done by the Department of Transportation's inspector general concluded that although most of the attacks disrupted only support systems, they could spread to the operational systems that control communications, surveillance and flight information used to separate aircraft.

The report noted several recent cyber attacks, including a February incident when hackers gained access to personal information on about 48,000 current and former FAA employees, and an attack in 2008 when hackers took control of some FAA network servers.

Auditors said the Federal Aviation Administration is not able to adequately detect potential cyber security attacks, and it must better secure its systems against hackers and other intruders.

"In our opinion, unless effective action is taken quickly, it is likely to be a matter of when, not if, ATC (air traffic control) systems encounter attacks that do serious harm to ATC operations," the auditors said.

In response to the findings, FAA officials stressed that the support systems and traffic control networks are physically isolated from each

other.

"It's not possible to use the administrative and mission support network to access the air traffic control network," said FAA spokeswoman Laura Brown.

But the FAA agreed that more aggressive action should be taken to secure the networks and fix high-risk vulnerabilities.

According to the report, the FAA received 800 cyber incident alerts during the fiscal year that ended Sept. 30, 2008, and more than 150 were not resolved before the year finished. Fifty of those, the auditors said, had been open for more than three months, "including critical incidents in which hackers may have taken over control" of some computers.

Officials tested Internet-based systems that are used to provide information to the public such as communications frequencies for pilots, as well as internal FAA computer systems. The tests found nearly 4,000 "vulnerabilities," including 763 viewed as "high risk." The vulnerabilities including weak passwords, unprotected file folders, and other software problems.

The weaknesses could allow hackers or internal FAA workers to gain access to air traffic systems, and possibly compromise computers there or infect them with malicious codes or viruses, the audit warned.

Such software gaps, the report said, are "especially worrisome at a time when the nation is facing increased threats from sophisticated nation-state-sponsored cyber attacks."

In its response top the audit, the FAA said corrective actions are already being taken, and that others should be in place in the coming months.

The audit is the latest in a series of reports and warnings about weaknesses in the U.S. government's computer networks, including revelations that spies have hacked into the U.S. electric grid and that a military aircraft program was breached, although classified information was not compromised.

The Obama administration, meanwhile, is wrangling over a recently completed review of the nation's cybersecurity, which is expected to detail how the U.S. should manage and secure its networks.

On the Net:

FAA: http://www.faa.gov/