

A promotional banner for Mother's Day Deals. On the left is the FTD logo featuring a yellow figure holding a bouquet. The text "MOTHER'S DAY DEALS" is in large, bold, black letters. To the right, it says "STARTING AT \$19.99" with the price in a large, bold font. Further right is a yellow button with the text "SHOP NOW" and a right-pointing arrow. The background on the right side of the banner shows a bouquet of purple and white roses.

FTD

MOTHER'S DAY DEALS

STARTING AT
\$19.99

SHOP NOW >

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

[See a sample reprint in PDF format.](#)

[Order a reprint of this article now](#)

THE WALL STREET JOURNAL

WSJ.com

MAY 7, 2009

FAA's Air-Traffic Networks Breached by Hackers

By [SIOBHAN GORMAN](#)

WASHINGTON -- Civilian air-traffic computer networks have been penetrated multiple times in recent years, including an attack that partially shut down air-traffic data systems in Alaska, according to a government report.

The report, which was released by the Transportation Department's inspector general Wednesday, warned that the Federal Aviation Administration's modernization efforts are introducing new vulnerabilities that could increase the risk of cyberattacks on air-traffic control systems. The FAA is slated to spend approximately \$20 billion to upgrade its air-traffic control system over the next 15 years.

The increasing reliance of modernized systems on the Internet "is especially worrisome at a time when the nation is facing increased threats from sophisticated nation-state sponsored cyber attacks," wrote Assistant Inspector General Rebecca Leng.

"We are working on developing security architecture for that whole system," said FAA spokeswoman Laura Brown. "We have identified it as an issue we need to focus some attention on, and we're doing that."

Security tests identified 763 "high risk" vulnerabilities that could allow hackers access to administrative systems, which could then provide a path to more-sensitive operational systems, the report said.

Ms. Brown rejected the report's conclusions that hackers could get into critical air-traffic operational systems through administrative systems.

"It's not possible to use the administrative and mission support network to access the air-traffic control network," she said. "We have specific orders that prohibit them from being directly connected."

The Wall Street Journal reported last month that an Air Force air-traffic control system had been compromised, alarming intelligence officials who feared that such an attack could be used to interfere with air-traffic systems.

Most of the known penetrations of FAA systems involved administrative networks that manage air-traffic flow and electric power, as well as email systems and internal and external Web sites, the report said.

The nature of one 2006 attack is a matter of dispute between the inspector general and the FAA. The report says the attack spread from administration networks to air-traffic control systems, forcing the FAA to shut down a portion of its traffic control systems in Alaska. Ms. Brown said it affected only the local administrative system that provides flight and weather data to pilots, primarily of small aircraft.

Last year, hackers of unspecified origin "took over FAA computers in Alaska" to effectively become agency insiders, and traveled the agency networks to Oklahoma, where they stole the network administrator's password and used it to install malicious codes, the report said. These hackers also gained the ability to obtain 40,000 FAA passwords and other information used to control the administrative network, it said.

In February, another cyber break-in yielded the personal information of 48,000 current and former agency

employees.

"The threat of hackers interfering with our air-traffic control systems is not just theoretical; it has already happened," said Republican Rep. Tom Petri of Wisconsin, one of the lawmakers who requested the report. "We must regard the strengthening of our air-traffic control security as an urgent matter."

Tom Kellermann, a vice president at Core Security Technologies, a cybersecurity company, likened the threats cited by the report to the television show "24" in which terrorists hack into and commandeer the FAA's air-traffic control system to crash planes. "The integrity of the data on which ground control is relying can be manipulated, much as seen in '24,'" he said.

Most critical infrastructure, such as the electric grid, have developed links between administrative and operational control systems that indirectly link the control systems to the public Internet, intelligence officials said.

The report warned that the FAA isn't well equipped to detect intrusions into its computer system, noting that it has detection sensors at only 11 of its 734 facilities across the country. All of those detectors are placed on administration or "mission support" systems, with no detectors on any of its operational systems, giving it little visibility into potential problems with operational networks, the report said.

When intrusions are detected, they aren't addressed quickly enough, the report said. Fifty unresolved incidents had been open for more than three months, it found, "including critical incidents in which hackers may have taken over control" of computers within the FAA's operations wing.

The FAA "is identifying and fixing weaknesses," Ms. Brown said, such as scanning software for potential vulnerabilities.

—Christopher Conkey contributed to this article.

Write to Siobhan Gorman at siobhan.gorman@wsj.com

Printed in The Wall Street Journal, page A6

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com