August 2005

INFORMATION SECURITY

Progress Made, but Federal Aviation Administration Needs to Improve Controls over Air Traffic Control Systems

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-05-712, a report to congressional requesters

Why GAO Did This Study

The Federal Aviation Administration (FAA) performs critical functions that contribute to ensuring safe, orderly, and efficient air travel in the national airspace system. To that end, it operates and relies extensively on an array of interconnected automated information systems and networks that comprise the nation's air traffic control systems. These systems provide information to air traffic controllers and aircraft flight crews to help ensure the safe and expeditious movement of aircraft. Interruptions of service by these systems could have a significant adverse impact on air traffic nationwide.

Effective information security controls are essential for ensuring that the nation's air traffic control systems are adequately protected from inadvertent or deliberate misuse, disruption, or destruction. Accordingly, GAO was asked to evaluate the extent to which FAA has implemented information security controls for these systems.

What GAO Recommends

GAO is recommending several actions intended to improve FAA's information security program. In providing oral comments on a draft of this report, FAA's Chief Information Officer agreed to consider GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-712.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

FAA has made progress in implementing information security for its air traffic control information systems; however, GAO identified significant security weaknesses that threaten the integrity, confidentiality, and availability of FAA's systems—including weaknesses in controls that are designed to prevent, limit, and detect access to these systems. The agency has not adequately managed its networks, software updates, user accounts and passwords, and user privileges, nor has it consistently logged security-relevant events. Other information security controls—including physical security, background investigations, segregation of duties, and system changes—also exhibited weaknesses, increasing the risk that unauthorized users could breach FAA's air traffic control systems, potentially disrupting aviation operations. While acknowledging these weaknesses, agency officials stated that the possibilities for unauthorized access were limited, given that the systems are in part custom built and that they run on older equipment that employs special-purpose operating systems, proprietary communication interfaces, and custom-built software. Nevertheless, the proprietary features of these systems cannot fully protect them from attacks by disgruntled current or former employees who are familiar with these features, nor will they keep out more sophisticated hackers.

A key reason for the information security weaknesses that GAO identified in FAA's air traffic control systems is that the agency had not yet fully implemented its information security program to help ensure that effective controls were established and maintained. Although the agency has initiatives under way to improve its information security, further efforts are needed. Weaknesses that need to be addressed include outdated security plans, inadequate security awareness training, inadequate system testing and evaluation programs, limited security incident-detection capabilities, and shortcomings in providing service continuity for disruptions in operations. Until FAA has resolved these issues, the information security weaknesses that GAO has identified will likely persist.

Air Traffic Control System Command Center

Source: FAA.