GAO Highlights

Highlights of GAO-15-221, a report to congressional requesters

January 2015

INFORMATION SECURITY

FAA Needs to Address Weaknesses in Air Traffic Control Systems

Why GAO Did This Study

In support of its mission, FAA relies on the NAS—one of the nation's critical infrastructures—which is comprised of air traffic control systems, procedures, facilities, aircraft, and people who operate and maintain them. Given the critical role of the NAS and the increasing connectivity of FAA's systems, it is essential that the agency implement effective information security controls to protect its air traffic control systems from internal and external threats.

GAO was asked to review FAA's information security program. Specifically, the objective of this review was to evaluate the extent to which FAA had effectively implemented information security controls to protect its air traffic control systems. To do this, GAO reviewed FAA policies, procedures, and practices and compared them to the relevant federal law and guidance; assessed the implementation of security controls over FAA systems; and interviewed officials. This is a public version of a report containing sensitive security information. Information deemed sensitive has been redacted.

What GAO Recommends

GAO is making 17 recommendations to FAA to fully implement its information security program and establish an integrated approach to managing information security risk. In a separate report with limited distribution, GAO is recommending that FAA take 168 specific actions to address weaknesses in security controls. In commenting on a draft of this report, FAA concurred with GAO's recommendations.

View GAO-15-221. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Nabajyoti Barkakati, Ph.D. at (202) 512-4499 or barkakatin@gao.gov, or Gerald L. Dillingham, Ph.D. at (202) 512-2834 or dillinghamg@gao.gov.

What GAO Found

While the Federal Aviation Administration (FAA) has taken steps to protect its air traffic control systems from cyber-based and other threats, significant security control weaknesses remain, threatening the agency's ability to ensure the safe and uninterrupted operation of the national airspace system (NAS). These include weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on FAA's systems. Additionally, shortcomings in boundary protection controls between less-secure systems and the operational NAS environment increase the risk from these weaknesses.

FAA also did not fully implement its agency-wide information security program. As required by the Federal Information Security Management Act of 2002, federal agencies should implement a security program that provides a framework for implementing controls at the agency. However, FAA's implementation of its security program was incomplete. For example, it did not always sufficiently test security controls to determine that they were operating as intended; resolve identified security weaknesses in a timely fashion; or complete or adequately test plans for restoring system operations in the event of a disruption or disaster. Additionally, the group responsible for incident detection and response for NAS systems did not have sufficient access to security logs or network sensors on the operational network, limiting FAA's ability to detect and respond to security incidents affecting its mission-critical systems.

The weaknesses in FAA's security controls and implementation of its security program existed, in part, because FAA had not fully established an integrated, organization-wide approach to managing information security risk that is aligned with its mission. National Institute of Standards and Technology guidance calls for agencies to establish and implement a security governance structure, an executive-level risk management function, and a risk management strategy in order to manage risk to their systems and information. FAA has established a Cyber Security Steering Committee to provide an agency-wide risk management function. However, it has not fully established the governance structure and practices to ensure that its information security decisions are aligned with its mission. For example, it has not (1) clearly established roles and responsibilities for information security for the NAS or (2) updated its information security strategic plan to reflect significant changes in the NAS environment, such as increased reliance on computer networks.

Until FAA effectively implements security controls, establishes stronger agency-wide information security risk management processes, fully implements its NAS information security program, and ensures that remedial actions are addressed in a timely manner, the weaknesses GAO identified are likely to continue, placing the safe and uninterrupted operation of the nation's air traffic control system at increased and unnecessary risk.