April 2015

AIR TRAFFIC CONTROL

FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen

GAO Highlights

Highlights of GAO-15-370, a report to congressional requesters

Why GAO Did This Study

FAA is responsible for overseeing the national airspace system, which comprises ATC systems, procedures, facilities, and aircraft, and the people who operate them. FAA is implementing NextGen to move the current radar-based ATC system to one that is based on satellite navigation and automation. It is essential that FAA ensures effective information-security controls are incorporated in the design of NextGen programs to protect them from threats.

GAO was asked to review FAA's cybersecurity efforts. This report (1) identifies the cybersecurity challenges facing FAA as it shifts to the NextGen ATC system and how FAA has begun addressing those challenges, and (2) assesses the extent to which FAA and its contractors, in the acquisition of NextGen programs, have followed federal guidelines for incorporating cybersecurity controls. GAO reviewed FAA cybersecurity policies and procedures and federal guidelines, and interviewed FAA officials, aviation industry stakeholders, and 15 select cybersecurity experts based on their work and recommendations by other experts.

What GAO Recommends

GAO recommends that FAA: 1) assess developing a cybersecurity threat model, 2) include AVS as a full member of the Committee, and 3) develop a plan to implement NIST revisions within OMB's time frames. FAA concurred with recommendations one and three, but believes that AVS is sufficiently involved in cybersecurity. GAO maintains that AVS should be a member of the Committee.

View GAO-15-370. For more information, contact Gerald L. Dillingham, Ph.D. at (202) 512-2834 or dillinghamg@gao.gov, Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Nabajyoti Barkakati, Ph.D. at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

As the agency transitions to the Next Generation Air Transportation System (NextGen), the Federal Aviation Administration (FAA) faces cybersecurity challenges in at least three areas: (1) protecting air-traffic control (ATC) information systems, (2) protecting aircraft avionics used to operate and guide aircraft, and (3) clarifying cybersecurity roles and responsibilities among multiple FAA offices.

- As GAO reported in January 2015, FAA has taken steps to protect its ATC systems from cyber-based threats; however, significant security-control weaknesses remain that threaten the agency's ability to ensure the safe and uninterrupted operation of the national airspace system. FAA has agreed to address these weaknesses. Nevertheless, FAA will continue to be challenged in protecting ATC systems because it has not developed a cybersecurity threat model. NIST guidance, as well as experts GAO consulted, recommend such modeling to identify potential threats to information systems, and as a basis for aligning cybersecurity efforts and limited resources. While FAA has taken some steps toward developing such a model, it has no plans to produce one and has not assessed the funding or time that would be needed to do so. Without such a model, FAA may not be allocating resources properly to guard against the most significant cybersecurity threats.
- Modern aircraft are increasingly connected to the Internet. This interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems. As part of the aircraft certification process, FAA's Office of Safety (AVS) currently certifies new interconnected systems through rules for specific aircraft and has started reviewing rules for certifying the cybersecurity of all new aircraft systems.
- FAA is making strides to address the challenge of clarifying cybersecurity roles and responsibilities among multiple FAA offices, such as creating a Cyber Security Steering Committee (the Committee) to oversee information security. However, AVS is not represented on the Committee but can be included on an ad-hoc advisory basis. Not including AVS as a full member could hinder FAA's efforts to develop a coordinated, holistic, agency-wide approach to cybersecurity.

FAA's acquisition management process generally aligned with federal guidelines for incorporating requirements for cybersecurity controls in its acquisition of NextGen programs. For example, the process included the six major information-technology and risk-management activities as described by NIST. Timely implementation of some of these activities could have been improved based on their importance to NextGen, cost, and deployment status. The Surveillance and Broadcast Services Subsystem (SBSS)—which enables satellite guidance of aircraft and is currently deployed in parts of the nation—has not adopted all of the April 2013 changes to NIST security controls, such as intrusion detection improvements, although the Office of Management and Budget guidance states that deployed systems must adopt changes within one year. Systems with weaknesses that could be exploited by adversaries may be at increased risk if relevant controls are not implemented.