



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.

April 2015

AIR TRAFFIC CONTROL

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

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.

Contents

Letter		1
	Background	4
	FAA's Shift to NextGen Implementation Raises Cybersecurity Challenges That FAA Has Taken Some Steps to Address	11
	Selected Experts Generally Agreed That FAA's Enterprise Approach Is Appropriate, but Noted That Further Actions Could Enhance Cybersecurity	15
	FAA's Acquisition Management Process Reflects Federal Guidance, but Management of Security Controls and Contractor Oversight Could Be Improved	24
	Conclusions	40
	Recommendations	41
	Agency Comments	42
Appendix I	Objectives, Scope, and Methodology	45
Appendix II	Comments from the Department of Transportation	48
Appendix III	GAO Contact and Staff Acknowledgments	51
Table		
	Table 1: Experts Providing Responses to Cybersecurity Challenges Facing FAA	45
Figures		
	Figure 1: National Airspace System's Transition to an IP Network	5
	Figure 2: NextGen Foundational Programs	7
	Figure 3: Legacy NAS ATC Systems Compared to NAS IP Networks	14
	Figure 4: Aircraft Diagram Showing Internet Protocol Connectivity Inside and Outside of Aircraft	19
	Figure 5: Phases of the FAA's Acquisition Life Cycle and National Institute of Standards and Technology's Information-Technology and Risk-Management Activities	26
	Figure 6: Security Activity's Progress for Each of NextGen's Foundational Program	30

Abbreviations

ADS-B	Automatic Dependent Surveillance—Broadcast
AMS	Acquisition Management System
ARAC	Aviation Rulemaking Advisory Committee
ASISP	aircraft system's information security/protection
ATC	air traffic control
ATO	Air Traffic Organization
AVS	Office of Safety
CATM	Collaborative Air Traffic Management
<i>CDM</i>	<i>Continuous Diagnostics and Mitigation</i>
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSC	Cybersecurity Steering Committee
CSMC	Cyber Security Management Center
CSS-Wx	Common Support Services—Weather
Data Comm	Data Communications
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FISMA	Federal Information Security Management Act of 2002
GPS	Global Positioning System
IP	Internet Protocol
ISS	Information Systems Security
IT	information technology
NAS	national airspace system
NCO	NAS Cyber Operations Center
NextGen	Next Generation Air Transportation System
NIST	National Institute of Standards and Technology
NVS	NAS Voice Switch
OMB	Office of Management and Budget
POA&M	plans of action and milestones
RTCA	Radio Technical Commission for Aeronautics
SBSS	Surveillance and Broadcast Services Subsystem
SWIM	System Wide Information Management
US-CERT	United States Computer Emergency Readiness Team
WBS	work breakdown structure

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



April 14, 2015

Congressional Requesters

Cyber-based threats to federal information systems are evolving and growing. These threats can come from many sources, including criminals and other adversarial groups, foreign nations, terrorists, and insiders. Further, the growing interconnectivity among information systems presents increasing opportunities for cyber attacks. Specifically, the number of incidents reported by federal agencies to the United States Computer Emergency Readiness Team¹ (US-CERT) has increased dramatically in recent years from 5,503 incidents reported in fiscal year 2006 to 60,753 incidents in fiscal year 2013. Federal policy identifies 16 infrastructure sectors critical to the nation's security, economy, and public health and safety²—including the nation's air-traffic-control and federal-information technology systems—that rely extensively on computerized information systems and electronic data. Effectively implementing appropriate security over the information systems and data can make these sectors more resilient to attack or unintentional compromise.

For more than 10 years, the Federal Aviation Administration (FAA) has been modernizing the air-traffic control (ATC) system across the national airspace system (NAS). FAA initiated its current modernization efforts in 2004 with the Next Generation Air Transportation System (NextGen), which consists of several programs that provide digital communications between controllers and pilots, as well as between satellite-based surveillance and navigation. NextGen increases reliance on integrated information systems and distribution of information, digital communication methods, and Global Positioning System (GPS) technology that may put the ATC system at greater risk for intentional or unintentional information-

¹US-CERT hosts the Department of Homeland Security's federal information-security incident center. When cybersecurity incidents occur, agencies are to notify the center.

²These 16 critical infrastructure sectors are: financial services; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and wastewater systems. White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21 (Feb. 12, 2013).

system failures and breaches. You asked us to examine these risks. This report identifies the cybersecurity challenges facing FAA as it shifts to the NextGen ATC system and how FAA has begun addressing those challenges. In addition, this report assesses the extent to which FAA and its contractors, in the acquisition of NextGen programs, have followed federal guidelines for incorporating cybersecurity controls.

To ascertain the key challenges FAA faces and how it is addressing them, we reviewed relevant cybersecurity documents from FAA and asked FAA officials to provide us with detailed descriptions of their cybersecurity plans as they relate to the NextGen ATC system. We interviewed FAA officials in the Air Traffic Organization—specifically the Technical Operations Information Security Office, NAS Cyber Operations Center, and the Program Management Office; the Office of NextGen; the Office of Safety; and the Office of Finance and Management—to identify information about the cybersecurity risks and challenges officials have identified, as well as mitigation strategies either in place or planned. We interviewed a diverse but non-generalizable sample of 15 aviation and cybersecurity experts in private industry and academia to obtain their views on FAA’s efforts to address NextGen cybersecurity issues. We selected these experts based on their knowledge of these topics, as demonstrated by their publications, participation as experts in prior relevant GAO work, or recommendation by other experts. We also reviewed studies on NextGen cybersecurity challenges and spoke with a variety of industry stakeholders and academics.

To assess the extent to which FAA and its contractors, in the acquisition of NextGen programs, have followed federal guidelines for incorporating cybersecurity controls, we compared pertinent FAA policies, procedures, and practices with selected federal information-security laws and federal guidance, including standards and guidelines from the National Institute of Standards and Technology (NIST).³ In particular, we compared FAA’s Acquisition Management System (AMS)⁴ against NIST’s risk

³NIST is responsible for developing technical standards for the information-security programs across government.

⁴FAA’s Acquisition Management System (AMS) provides policies and guidance for managing its acquisitions.

management guidelines⁵ and information-technology security guidelines⁶ to determine if it follows these guidelines for the six foundational NextGen programs, Surveillance and Broadcast Services Subsystem (SBSS), Data Communications (Data Comm), NAS Voice Switch, Collaborative Air Traffic Management (CATM), Common Support Service-Weather (CSS-Wx), and System Wide Information Management (SWIM). We analyzed FAA's documentation of key cybersecurity activities for these programs and interviewed program managers to determine if FAA completed the key activities in the process, or has plans to complete activities that were started but not completed. We then chose two key NextGen acquisitions, SBSS and Data Comm. We chose them for a detailed, in-depth review because of their importance to NextGen, their cost, and their deployment status. SBSS has completed key activities in the acquisition cycle. Our reviewing Data Comm, which has not completed the cycle, should allow insight into how the process has changed and what still might be an issue for upcoming programs. For these two programs, we assessed how well FAA and its contractors completed key cybersecurity activities and the extent to which they complied with AMS and NIST guidelines relating to cybersecurity. As part of this effort, we also compared documentation of program activities and plans to these requirements, and interviewed agency officials. We also reviewed pertinent sections of prior GAO reports related to cybersecurity. We performed our work at FAA headquarters in Washington, D.C.; the Air Traffic Control Systems Command Center in Warrenton, Virginia; and an FAA contractor location in Herndon, Virginia. See appendix I for a more detailed description of our scope and methodology.

We conducted this performance audit from September 2013 to March 2015, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁵NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 Revision 1 (Gaithersburg, Md.: February 2010).

⁶NIST, *Security Considerations in the System Development Life Cycle*, SP 800-64 (Gaithersburg, Md.: October 2008).

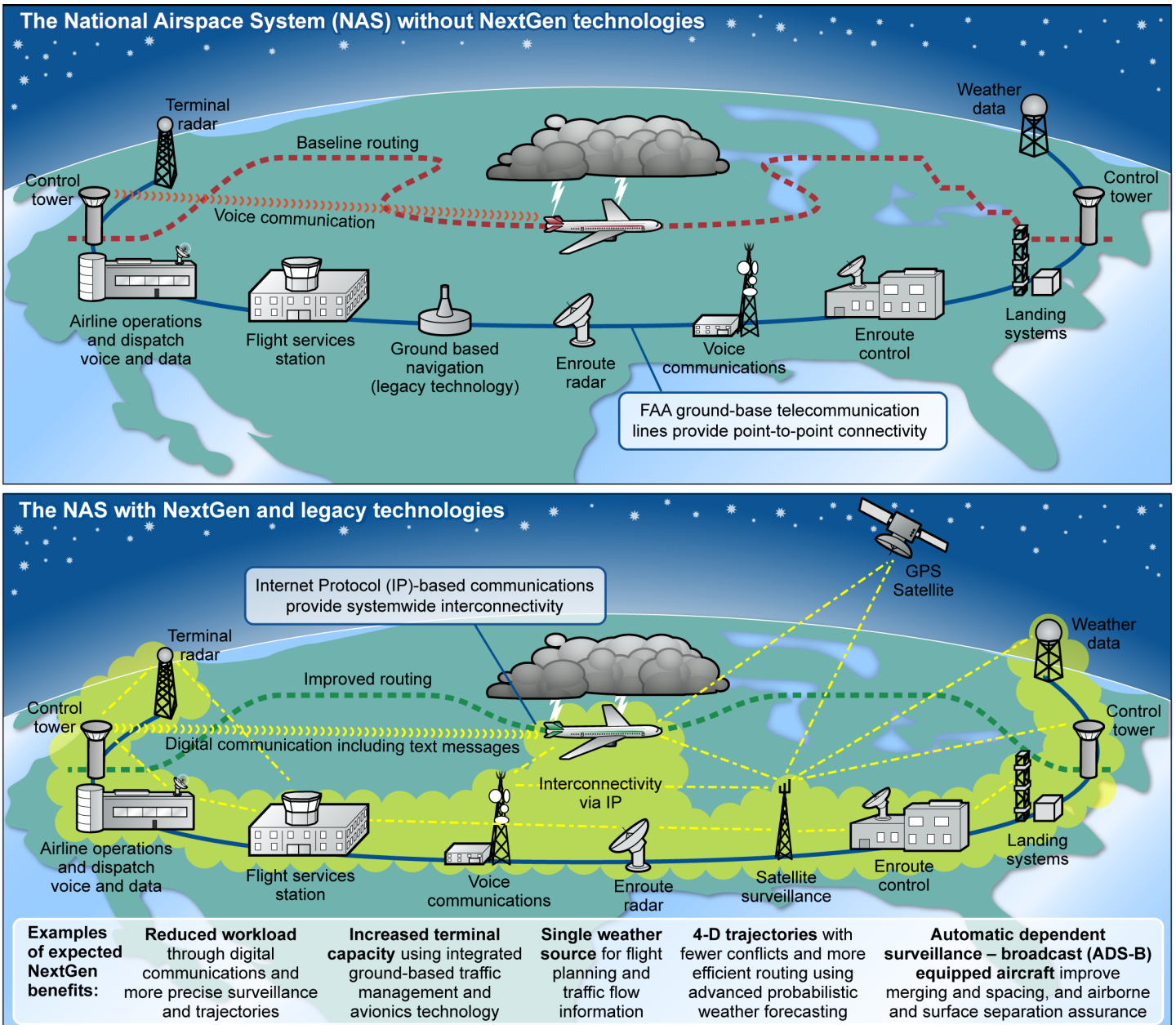
Background

FAA's Transition to NextGen

NextGen is a modernization effort begun in 2004 by FAA to transform the nation's ground-based ATC system into a system that uses satellite-based navigation and other advanced technology. This effort is a multiyear, incremental transformation that will introduce new technologies and leverage existing technologies to affect every part of the NAS. These new technologies will use an Internet Protocol (IP) based network to communicate.⁷ See figure 1 below for a graphic illustration of the different parts of the NAS, the flow of information among them, and their transition to an IP-based network.

⁷Internet Protocol, the principal communications protocol on which the Internet is based, is a networking technology that has been the industry's standard method to network computer systems since the late 1990s.

Figure 1: National Airspace System's Transition to an IP Network

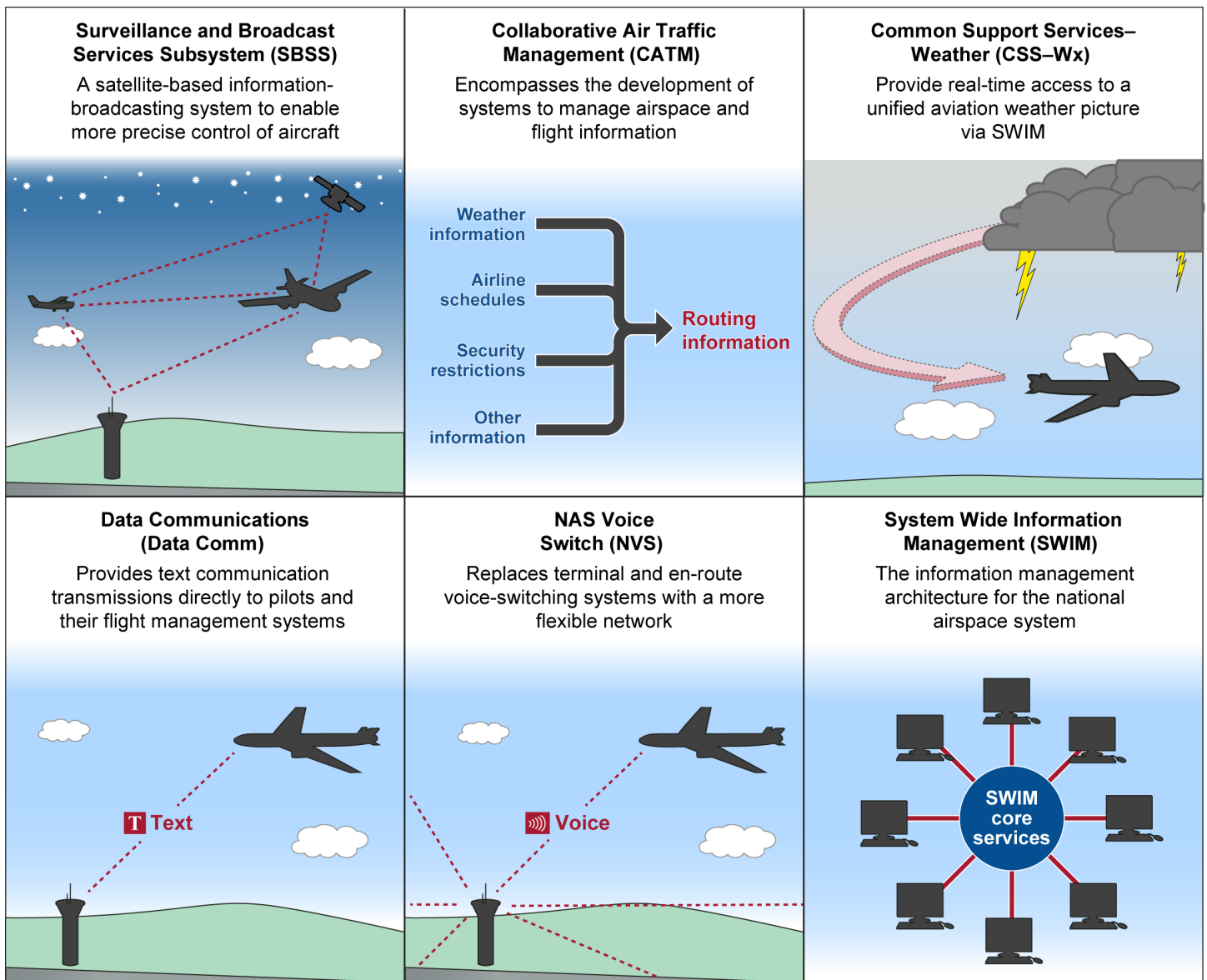


Source: GAO. | GAO-15-370

According to FAA, the shift to NextGen technologies will require FAA to replace its proprietary, relatively isolated ATC computer systems with information systems that interoperate and share data throughout FAA's operations and those of its aviation partners. These combined aviation operations are known as *the enterprise*. These new systems, which will be described in detail later in this report, will use IP-networking technologies to communicate across the enterprise. This transformation involves acquiring, certifying, and operating a vast network of navigation, communications, and surveillance systems, including information systems in the cockpits of thousands of aircraft (avionics); it will also employ digital and Internet-based computer-networking technologies, exposing the air-traffic control (ATC) system to new cybersecurity risks.

NextGen comprises many programs that are in various stages of acquisition and deployment in the NAS. FAA classifies six programs as its foundational NextGen programs: Surveillance and Broadcast Services Subsystem (SBSS), Collaborative Air Traffic Management (CATM), Common Support Services Weather (CSS-Wx), Data Communications (Data Comm), NAS Voice Switch (NVS), and System Wide Information Management (SWIM) (see fig. 2).

Figure 2: NextGen Foundational Programs



Source: GAO. | GAO-15-370

For the six programs we examined, FAA relies on contractors to assist with or complete most of the broad information technology and risk management activities. NIST, OMB, and FISMA state that regardless of whether a security task was performed by a contractor or by a federal

agency, the federal agency is ultimately responsible for ensuring system security. The AMS requires that FAA program officials monitor the contractors' performance in implementing contractual requirements, including those related to security.

Several Offices within FAA Have Cybersecurity Responsibilities

- The Office of the Chief Information Security Officer within the Office of Finance and Management oversees cybersecurity across the three main areas of FAA activity known as *domains* (i.e., NAS ATC operations, Mission Support, and Research and Development [R&D]). This office provides operational security services to the Mission Support and R&D domains through efforts across FAA, as well as the Cyber Security Management Center (CSMC). The CSMC provides system monitoring and vulnerability remediation for FAA's standard information-technology systems that support the agency. Mission-support information systems, such as email, are separate from the NAS and R&D domain systems.⁸
- The Air Traffic Organization (ATO), the operational arm of FAA, implements and oversees cybersecurity measures for ATC information systems through several of its offices.⁹ The ATO's NAS Security Risk Executive (Risk Executive) located in Technical Operations has responsibility for cybersecurity on all NAS ATC systems, including continuous monitoring, threat response coordination, and policy.¹⁰ According to FAA, the Risk Executive works internally with FAA's Security and Hazardous Materials Office and NextGen offices, and externally with Department of Homeland Security (DHS) and airline stakeholders to provide an understanding of FAA's critical mission and how it relates to other critical infrastructures. Another office within ATO, the NAS Cyber Operations unit, is responsible for monitoring some NAS systems, network data

⁸According to FAA Order 1370.82A, the CIO appoints the Chief Information Security Officer—who is responsible for developing, implementing, and funding the agency Information Systems Security program—to provide security for agency information and information systems

⁹The ATO includes seven service units: Air Traffic Services, Management Services, Mission Support Services, Program Management Organization, Safety and Technical Training Services, Systems Operations Services, and Technical Operations Services.

¹⁰FAA created the ATO's NAS Security Risk Executive position in summer 2012, but the position description is still in draft form and is not yet codified in policy.

flows, and cyber events to detect anomalous and unauthorized cyber activities in the NAS domain. ATO's Program Management Office is responsible for developing and fulfilling cybersecurity and all other system requirements for NAS information systems, including NextGen systems, through the acquisitions process.

- The Office of NextGen develops and disseminates cybersecurity policy on NextGen's system engineering and controls, develops the NAS Enterprise Architecture, which is the agency's long-term strategic plan for NextGen that includes, among other things, the information systems security (ISS) plans, and is responsible for the overall implementation of FAA's NextGen initiative.
- The Office of Security and Hazardous Material Safety performs internal forensics investigations on computers that CSMC identifies as involved in activity that may compromise cybersecurity.
- The Office of Safety certifies the safety of all aircraft and aircraft equipment, including the software components for the avionics systems that could affect the safe operation of an aircraft.

Federal Cybersecurity Guidance for Information Systems

The Federal Information Security Management Act of 2002 (FISMA)¹¹ established a comprehensive framework to better ensure the effectiveness of security controls¹² over information resources that support federal operations and assets. FISMA¹³ requires each agency to develop, document, and implement an agency-wide information-security program, using a risk-based approach to determine and address cybersecurity requirements for information system management. Such a program includes planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies. Federal cybersecurity guidelines, such as those published by NIST, strongly encourage agencies to implement information cybersecurity early in the

¹¹Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 as updated, by the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (codified at 44 U.S.C. §§ 3551 – 3558).

¹²Security controls are technical or administrative safeguards or countermeasures to avoid, counteract, or minimize loss or unavailability.

¹³FISMA was superseded by the Federal Information Technology Modernization Act of 2014, but FISMA retains requirements for agencies to implement an agency-wide information security program.

process of developing information systems. In this manner, the cybersecurity requirements can change as needed and be integrated cost-effectively.¹⁴ NIST also provides a process for integrating information-security and risk-management activities into the system development process over the life of the system. Accordingly, NIST has developed a risk management framework of standards and guidelines for agencies to follow in developing information security programs. Relevant publications include the following:

- *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* provides a process that integrates information-security and risk-management activities into the system development's life cycle including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring of an information system.
- *Security and Privacy Controls for Federal Information Systems and Organizations*¹⁵ provides a catalog of security and privacy controls for federal information systems and organizations, and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The guidance includes privacy controls to be used in conjunction with the specified security controls to achieve comprehensive security and privacy protection.
- *Security Considerations in the System Development Life Cycle*¹⁶ presents a framework for incorporating security across the life cycle of a system and describes a minimum set of security steps needed to effectively incorporate security into a system during its development. It is intended to help agencies select and acquire cost-effective security

¹⁴NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

¹⁵NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

¹⁶National Institute of Standards and Technology, *Security Considerations in the System Development Life Cycle*, SP 800-64, Revision 2 (Gaithersburg, Md.: October 2008).

controls by explaining how to include information-system security requirements in the system development's life cycle.

- In addition to these NIST publications, the Office of Management and Budget's (OMB) Security of Federal Automated Information Resources¹⁷ establishes a minimum set of controls to be included in federal automated information-security programs; assigns federal agency responsibilities for the security of automated information; and links the agency's automated information-security programs and the agency's management control systems.

FAA Acquisition Management System

FAA's Acquisition Management System (AMS) provides policies and guidance for managing all of its acquisitions. The AMS serves as the framework for IT project management and risk evaluation to help ensure that systems are developed and maintained on time and within budget, and that they deliver the capabilities necessary to meet user requirements including the development and integration of cybersecurity controls.

FAA's Shift to NextGen Implementation Raises Cybersecurity Challenges That FAA Has Taken Some Steps to Address

FAA faces cybersecurity challenges in at least three areas: (1) protecting its air traffic control (ATC) information systems, (2) securing aircraft avionics used to operate and guide aircraft, and (3) clarifying cybersecurity roles and responsibilities among multiple FAA offices. FAA has taken several steps to address these challenges, but cybersecurity experts suggested additional actions FAA could take to enhance cybersecurity.

¹⁷OMB, *Management of Federal Automated Information Resources, Circular A-130* Revised.

FAA Faces Cybersecurity Challenges to Protect ATC Information Systems, and Most Experts Consulted Indicated That FAA Could Take Additional Steps

New Networking Technologies Expose ATC Systems to New Cybersecurity Risks

New networking technologies connecting FAA's ATC information systems expose these systems to new cybersecurity risks, potentially increasing opportunities for systems to be compromised and damaged. Such damage could stem both from attackers seeking to gain access to and move among information systems, and from trusted users of the systems, such as controllers or pilots, who might inadvertently cause harm. FAA's ATC-related information systems are currently a mixture of old, legacy systems and new, IP-networked systems. FAA's legacy systems consist mainly of decades-old, point-to-point, hardwired information systems, such as controller voice-switching systems, that share information only within their limited, wired configuration. In contrast, FAA plans for NextGen call for the new information systems to be networked together with IP technology into an overarching system of interoperating subsystems.

According to FAA officials and experts we consulted, the ease of access to these different types of systems, and the potential to damage them, varies. The older systems, depicted on the left in figure 3 below, are difficult to access remotely because few of them connect from FAA to external entities such as through the Internet. They also have limited lines of direct connection within FAA. Conversely, the new information systems for NextGen programs are designed to interoperate with other systems and use IP networking to communicate within FAA, as shown on the right in figure 3 below. According to experts, if one system connected to an IP network is compromised, damage can potentially spread to other systems on the network, continually expanding the parts of the system at risk. As shown in the figure, cybersecurity controls, if properly designed and effectively implemented, can make IP-networked systems more resilient against damage while allowing the systems to interoperate. According to

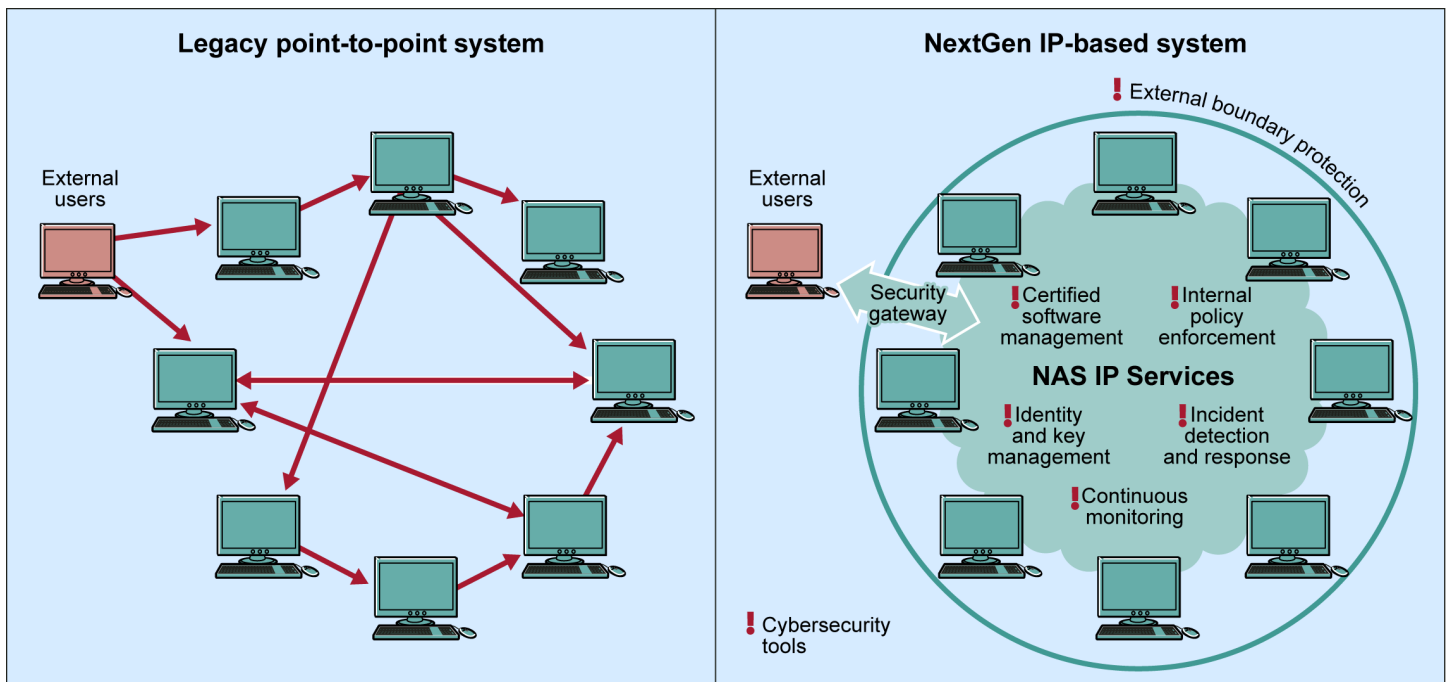
MITRE,¹⁸ because the older systems had limited connectivity, they were generally not protected with cybersecurity controls. Once one of them is breached, it is easy to potentially damage that system, gain access to other systems with which it communicates, and potentially damage those systems as well. According to FAA, so far, approximately 36 percent of the ATC systems in the national airspace system (NAS) are connected using IP, and FAA officials expect the percentage of NAS systems using IP networking to grow to 50 to 60 percent by 2020. According to MITRE and other experts, a hybrid system comprising both IP-connected and point-to-point subsystems increases the potential for the point-to-point systems to be compromised because of the increased connectivity to the system as a whole provided by the IP-connected systems.

We reported in January 2015 that FAA has taken steps to protect its ATC systems from cyber-based threats. However, we stated that significant security-control weaknesses remain that threaten the agency's ability to ensure the safe and uninterrupted operation of the national airspace system. We made numerous recommendations to address these weaknesses, and FAA has concurred with these recommendations.¹⁹

¹⁸MITRE is a not-for-profit organization chartered to work in the public interest. MITRE manages four federally funded research and development centers, including one for FAA. MITRE has its own independent research and development program that explores new technologies and new uses of technologies to solve problems in the near term and in the future. MITRE has done extensive research on cybersecurity issues under contract for FAA.

¹⁹GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*. [GAO-15-221](#). (Washington DC: January 2015).

Figure 3: Legacy NAS ATC Systems Compared to NAS IP Networks



Source: GAO. | GAO-15-370

FAA Is Designing and Deploying an Enterprise Approach Intended to Strengthen the Cybersecurity of Its Information Systems

FAA is developing an approach, called an *enterprise* approach, to connect and protect its information systems enterprise-wide. The enterprise approach views IP-networked systems as subsystems within the larger enterprise-wide system. Under this approach, the subsystems can interoperate while an enterprise-wide set of shared cybersecurity controls,²⁰ called “*common controls*,” and a monitoring program protect and increase the resiliency of the subsystems. According to FAA officials and cybersecurity experts we spoke to, using common controls in an enterprise approach increases the efficiency of cybersecurity efforts. For example, NIST recommends the use of common controls because when new threats to the system are discovered and those threats can be addressed by revisions to common controls, agencies can then

²⁰Cybersecurity controls are safeguards or countermeasures to avoid, counteract, or minimize security risks relating to information systems.

immediately protect all the interoperating subsystems by revising just the common control. For isolated, legacy systems, cybersecurity control revisions have to be developed and implemented uniquely for each individual system. FAA officials said that they apply both common controls and individual system controls, where appropriate, to IP-connected systems interoperating within an enterprise domain, in accordance with NIST guidance and OMB policy.

**Selected Experts
Generally Agreed
That FAA’s Enterprise
Approach Is
Appropriate, but
Noted That Further
Actions Could
Enhance
Cybersecurity**

**A Holistic Threat Model
Could Enhance FAA’s
Cybersecurity Posture**

Twelve of our 15 cybersecurity experts discussed enterprise-level holistic threat modeling, and all 12 agreed that FAA should develop such a model to strengthen cybersecurity agency-wide. NIST and the 12 experts we consulted said that threat modeling, a cybersecurity best practice, enables an organization to identify known threats, including insider threats, across its organization and align its cybersecurity efforts and limited resources accordingly to protect its mission. NIST guidance also states that an integrated, agency-wide view for managing risk can address the complex relationship among missions, the business processes needed to carry out missions, and the information systems supporting those missions and processes. NIST also recommends

organization-wide threat modeling,²¹ assessment, and monitoring because an agency-wide threat model would help to identify all known threats to information systems, allowing an agency to further identify vulnerabilities in those systems.

FAA officials said that FAA has not produced a plan to develop an enterprise-wide threat model but has made some initial steps toward developing such a model. Specifically, FAA officials said that they have examined threats to the future NextGen air-transportation system and are currently working to develop multiple threat models. Such efforts include reviewing the resiliency of the ATC system in conjunction with the Department of Homeland Security (DHS). NIST recommended such a review in its guidelines to promote the protection of critical infrastructure. According to FAA, it also assesses risks associated with individual systems when it acquires them and during system reauthorization. According to FAA, these assessments examine how the system in question interoperates with other systems; however, FAA officials agree that these assessments do not constitute a holistic threat model that might give FAA an agency-wide view of known threats to the entire ATC system. One FAA official said and an aviation advisory group published a report stating that such a threat model would allow FAA to approach cybersecurity in a proactive way, whereas FAA's current activities are reactive. For example, a threat model like that recommended by NIST and our experts could help FAA be more proactive in dealing with the rise of insider threats in federal agencies.²²

FAA officials told us that they have not yet reached a point where they are prepared to pursue a comprehensive enterprise-wide threat model. Some experts told us that developing and maintaining a threat model would be costly and time consuming. FAA officials told us that they have not

²¹NIST recommends developing an organization-wide "risk frame" that establishes the context for risk-based decisions by identifying assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence of cybersecurity incidents, which aligns with the threat modeling discussed by our experts. NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*. SP 800-39 (Gaithersburg, Md.: March 2011).

²²The 2014 malicious insider attack on FAA's Aurora, Illinois, en-route facility, while not facilitated through cyber means, destroyed ATC IP and point-to-point telecommunications lines, preventing ATC electronic communications and the gathering and use of flight data, such as radar data, to track aircraft, resulting in over \$350 million in financial losses to airlines.

determined the funding or time that would be needed to develop such a model or identified the resources needed to implement it. One senior FAA official agreed with the experts' view that an enterprise holistic-wide threat model is expensive and time-consuming to accomplish and maintain; he said that no plan currently exists to produce one for this reason.

While developing a holistic threat model could be costly and time-consuming, in a constrained-resource environment such as FAA's, the information contained in such a model could allow FAA to target resources to parts of the system commensurate with the likelihood of compromise and the danger associated with the potential consequences that might occur. Without a holistic threat model, it is unclear how FAA will be able to develop a more comprehensive picture of threats to its systems, and how they might compromise these systems. Most of our experts said that without this knowledge, FAA might not target its cybersecurity resources and analyses appropriately, leaving some important risks unmitigated while overprotecting against less severe risks.

Continuous-Monitoring Efforts Are Under Way

Ten of the cybersecurity experts we contacted also said that a holistic continuous-monitoring program is necessary for the IP-networked agency-wide approach that FAA is taking to accommodate NextGen programs. Cybersecurity experts and FAA officials told us that a holistic, continuous-monitoring program includes (1) real-time monitoring of the enterprise system's boundaries, (2) detection of would-be attackers probing for vulnerabilities, (3) real-time monitoring and investigation of internal user activity that is outside expectations, and (4) other continuous-monitoring activities such as incident detection, response, and recovery activities and mitigations.

FAA officials said they have implemented some monitoring activities for ATC systems. Although no coordinated policy exists for FAA enterprise-wide continuous monitoring, the Cyber Security Steering Committee has developed a plan that will incorporate DHS's Continuous Diagnostics and Mitigation program²³ in the future. For example, the NAS Cyber Operations (NCO) group, which has responsibility for incident response for NAS ATC systems, daily analyzes ATC's system activity reports, which, among other things, report on cyber attacks. Currently 9 of 39 IP-

²³The Continuous Diagnostics and Mitigation program provides tools and services that enable federal and other government entities to strengthen the security posture of their cyber networks.

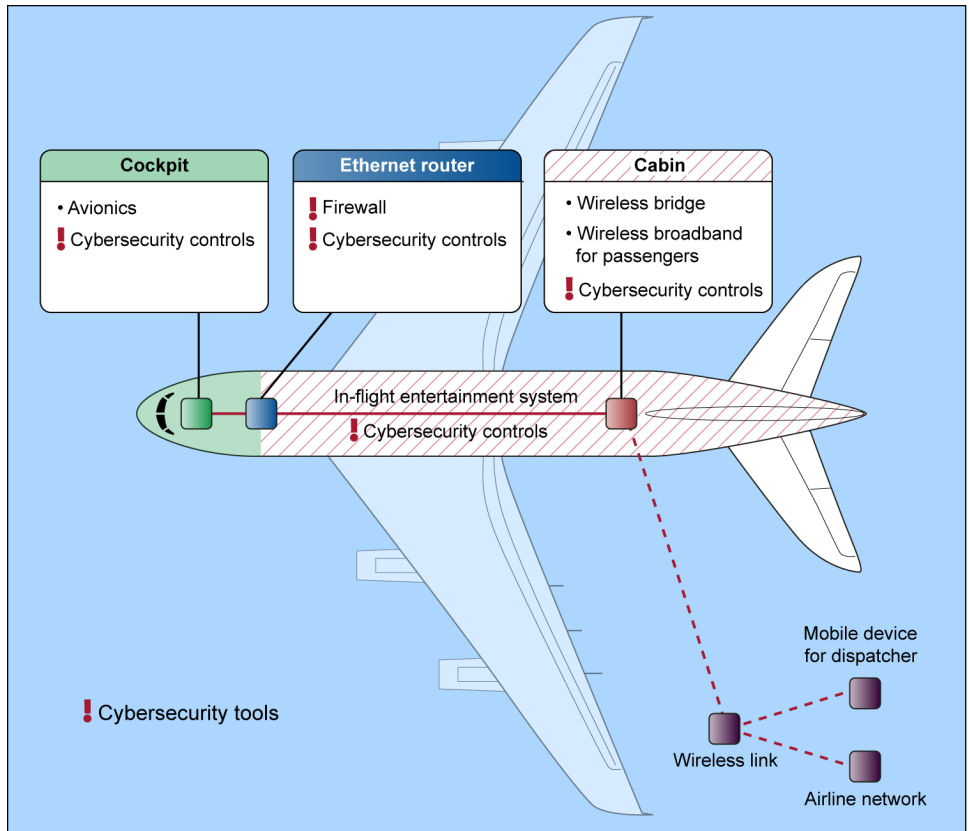
connected ATC systems provide system activity reports for NCO's review. NCO does not currently analyze activity reports for the other 30 systems. We have previously found²⁴ that this limited monitoring ability increased the risk that a cybersecurity event affecting NAS systems could go undetected and recommended that FAA provide the NCO function with sufficient access to provide more comprehensive monitoring. FAA officials said that ATO plans to have all NAS's IP-connected systems reporting daily to NCO within 3 years.

Securing Aircraft Avionics Systems Is an Increasing Challenge as FAA Adapts Its Aircraft Certification Process to Better Focus on Cybersecurity

According to FAA and experts we interviewed, modern communications technologies, including IP connectivity, are increasingly used in aircraft systems, creating the possibility that unauthorized individuals might access and compromise aircraft avionics systems. Aircraft information systems consist of avionics systems used for flight and in-flight entertainment (see fig. 4 below). Historically, aircraft in flight and their avionics systems used for flight guidance and control functioned as isolated and self-contained units, which protected their avionics systems from remote attack. However, according to FAA and experts we spoke to, IP networking may allow an attacker to gain remote access to avionics systems and compromise them—as shown in figure 4 (below). Firewalls protect avionics systems located in the cockpit from intrusion by cabin-system users, such as passengers who use in-flight entertainment services onboard. Four cybersecurity experts with whom we spoke discussed firewall vulnerabilities, and all four said that because firewalls are software components, they could be hacked like any other software and circumvented. The experts said that if the cabin systems connect to the cockpit avionics systems (e.g., share the same physical wiring harness or router) and use the same networking platform, in this case IP, a user could subvert the firewall and access the cockpit avionics system from the cabin. An FAA official said that additional security controls implemented onboard could strengthen the system.

²⁴GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*. [GAO-15-221](#). (Washington DC: January 2015).

Figure 4: Aircraft Diagram Showing Internet Protocol Connectivity Inside and Outside of Aircraft



Source: GAO. | GAO-15-370

FAA officials and experts we interviewed said that modern aircraft are also increasingly connected to the Internet, which also uses IP-networking technology and can potentially provide an attacker with remote access to aircraft information systems. According to cybersecurity experts we interviewed, Internet connectivity in the cabin should be considered a direct link between the aircraft and the outside world, which includes potential malicious actors. FAA officials and cybersecurity and aviation experts we spoke to said that increasingly passengers in the cabin can access the Internet via onboard wireless broadband systems. One cybersecurity expert noted that a virus or malware planted in websites visited by passengers could provide an opportunity for a malicious attacker to access the IP-connected onboard information system through their infected machines. According to five cybersecurity

experts, the threat of malicious activity by trusted insiders also grows with the ease of access to avionics systems afforded by IP connectivity if proper controls, such as *role-based* access,²⁵ are not in place. For example, the presence of personal smart phones and tablets in the cockpit increases the risk of a system's being compromised by trusted insiders, both malicious and non-malicious, if these devices have the capability to transmit information to aircraft avionics systems.

FAA's Office of Safety (AVS) is responsible for certifying the airworthiness of new aircraft and aviation equipment, including software components for avionics systems.²⁶ Although FAA's aircraft-airworthiness certification does not currently include assurance that cybersecurity is addressed,²⁷ FAA currently issues rules with limited scope, called Special Conditions, to aircraft manufacturers when aircraft employ new technologies where IP interconnectivity could present cybersecurity risks. FAA views Special Conditions as an integral part of the certification process, which gives the manufacturer approval to design and manufacture the aircraft, engine, or propeller with additional capabilities not referred to in FAA regulations. For example, FAA issued Special Conditions to address the increased connectivity among aircraft cockpit and cabin systems for the Boeing 787 and Airbus A350 to provide systems cybersecurity and computer network protection from unauthorized external and internal access. FAA officials said that research supporting cybersecurity-related Special Conditions could be aggregated and used to support portions of a new rule, and industry experts we spoke with said they would support the certainty rulemaking would bring.

According to FAA officials and the Radio Technical Commission for Aeronautics (RTCA),²⁸ FAA has not yet developed new regulations to

²⁵*Role-based* security permissions are based on a user's position or function within an organization.

²⁶See GAO, *Aviation Safety: Certification and Approval Processes Are Generally Viewed as Working Well, but Better Evaluative Information Needed to Improve Efficiency*. [GAO-11-14](#) (Washington, D.C.: Oct. 2010).

²⁷"*Airworthy*" means the aircraft conforms to its type design and is in a condition for safe operation.

²⁸Organized in 1935, the RTCA, which includes representatives from industry and FAA, is a private, not-for-profit corporation that develops consensus-based recommendations for communications, navigation, surveillance, and air-traffic management system issues.

certify cybersecurity assurance for avionics systems because historically, aircraft avionics systems were isolated within the aircraft itself and not considered vulnerable to cybersecurity attacks. According to RTCA, FAA's certification process for component airworthiness focuses on design assurance, which evaluates the probability and consequences of component failure. Further, RTCA reports that a focus on cybersecurity assurance would evaluate the likelihood and consequences of cybersecurity failure. The likelihood of an attack takes into account different levels of trustworthiness of entities with access to a component and the relative intention to do harm. However, FAA officials and an aviation expert said that intention has not been considered a factor in avionics component-system failures because other security processes generally prevented untrusted entities from gaining access to avionics components. FAA officials said that the agency recognizes that cybersecurity is an increasingly important issue in the aircraft-operating environment and is shifting the certification focus to address this potential new threat.

FAA's Office of Safety began developing a larger airworthiness rule covering avionics cybersecurity in 2013 but determined more research was necessary before rulemaking could begin and halted the process. In December 2014, FAA tasked its Aviation Rulemaking Advisory Committee (ARAC) with submitting a report within 14 months of the March 2015 kickoff meeting that provides recommendations on rulemaking and policy, and guidance on best practices for information security protection for aircraft, including both certification of avionics software and hardware, and continued airworthiness. FAA states that without updates to regulations, policy, and guidance to address aircraft system information security/protection (ASISP), aircraft vulnerabilities may not be identified and mitigated in a timely manner, thus increasing exposure times to security threats. According to the ARAC task assignment, the report should provide recommendations by early 2016 on whether ASISP-related rulemaking, policy, and/or guidance on leading practices are needed, and the rationale behind such recommendations. If policy or guidance, or both, are needed, among other things, the report should specify which aircraft and airworthiness standards would be affected.

FAA Has Taken Steps to Clarify Cybersecurity Roles and Responsibilities, but Opportunity Exists for Further Action

Cybersecurity roles and responsibilities are spread across FAA among different offices with varying missions and functions related to cybersecurity. FAA is taking steps to align agency cybersecurity orders and policies, as well as IT infrastructure and governance, with the changing needs of the NextGen cyber environment. In November 2013, the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) under the FAA's reorganized IT office began reorganizing and rewriting cybersecurity-related policies and plans agency-wide, and restructuring the agency's IT infrastructure and governance,²⁹ in part to address the shifts in cybersecurity activities and roles due to ATC modernization.³⁰ According to FAA, a working group expects to complete a draft by September 2015 that reflects the restructuring of IT infrastructure. The FAA's CIO is developing an enterprise approach for non-NAS information systems and cybersecurity, and is also leading a cross-agency team in developing the Cyber Security Strategy for 2016–2020. Separately, the ATO is also developing and maintaining an enterprise approach for NAS systems in the ATC domain.³¹

FAA has also taken steps to better coordinate its cybersecurity efforts. FAA runs exercises that simulate cyber attacks and are designed to increase internal collaboration and help clarify roles during such events. Specifically, the NAS Security Risk Executive and other ATO staff

²⁹FAA created the Office of the Deputy Administrator for Information and Technology (AIT) in conjunction with the Office of the CIO. FAA IT Shared Services resides in this office.

³⁰The FAA 2012 Reauthorization required FAA to undertake a thorough review of each program, office, and organization within FAA and to take actions as may be necessary to address the review's findings for, among other things, "reforming and streamlining inefficient processes so that the activities of the Administration are completed in an expedited and efficient manner." Pub. L. No. 112–95, §812, 126 Stat. 11, 124 (2012). One such action FAA has taken is to consolidate cybersecurity responsibility across FAA lines of business.

³¹Historically, before NAS information systems began the transition to IP networking, the Office of the Chief Information Officer, which sits outside of the Air Traffic Organization, had responsibility for NAS information system cybersecurity. Currently, the responsibilities of a security risk executive as described in NIST SP 800-39 are conducted for NAS systems by a position titled the NAS Security Risk Executive. The Cyber Security Steering Committee is in the process of developing policy that would center agency-wide risk executive responsibility in the Committee. Although the NAS Security Risk Executive position has been filled for about 2 years, the position description is still in draft form and the role has not been codified yet. The position does not control its own staff, nor does it receive specific funding.

organized and conducted five of these exercises between 2013 and 2015 involving FAA cybersecurity staff from different FAA offices as well as staff from the departments of Defense and Homeland Security, and MITRE. FAA officials said that these exercises are an integral part of sustaining and improving operational activities and are incorporated into the planning process for all NAS activities. FAA plans to continue conducting one or two per year.

In addition to the ATO's NAS Risk Executive, FAA established the Cybersecurity Steering Committee in November 2013 to better coordinate FAA agency-wide cybersecurity efforts at the executive level and provide an integrated approach to cybersecurity strategy and planning with a mission focus for FAA. The Committee has begun establishing the specific roles and responsibilities required to fulfill its mission. It is chaired by the CISO and includes representatives from ATO, NextGen, and Security and Hazardous Material Safety. These members are tasked with working together to identify, prioritize, strategize, and operationalize cybersecurity requirements, issues, programs, and projects needed to integrate an agency-wide approach to cybersecurity. Given that the Committee is in its early phases of operation, it is too early to tell whether it will be able to provide the cybersecurity visibility and coordination functions as outlined by the committee charter.

While FAA is working to transform the organization of its cybersecurity efforts, the experts we consulted said that it could improve upon those efforts by including all key stakeholders in its agency-wide approach. All 15 of our cybersecurity and aviation experts agreed that organizational clarity regarding roles, responsibilities, and accountability is key to ensuring cybersecurity across the organization. In addition, the five experts who commented on stakeholder inclusion all said that because aircraft avionics systems have the potential to be connected to systems outside the aircraft, aircraft cybersecurity issues should be included in an agency-wide cybersecurity effort. For instance, AVS issues cybersecurity-related rules for aircraft and has begun reviewing rulemaking on cybersecurity, but AVS is not included in developing the agency-wide approach for information systems security and has no representative on the Cybersecurity Steering Committee. FAA states that AVS subject matter experts can be called upon to share information and recommendations but that regulatory aspects associated with cybersecurity for AVS's information systems are addressed by the FAA's CIO and are therefore not under the purview of the FAA Cybersecurity Steering Committee. While AVS has not directly requested to be on this committee, we previously found that it is important to ensure that relevant

FAA's Acquisition Management Process Reflects Federal Guidance, but Management of Security Controls and Contractor Oversight Could Be Improved

participants be included in collaborative efforts.³² This lack of involvement could result in omitting an FAA stakeholder that has an understanding of specific technological changes in aircraft traversing the NAS environment and how these changes might intersect with changing ATC technologies and cybersecurity needs.

According to NIST, one goal of an agency-wide approach to cybersecurity is protecting new information systems from threats by ensuring that when those systems are acquired, they incorporate security controls. To accomplish this goal, FAA's Acquisition Management System (AMS) includes the six major information-technology and security-risk-management activities described in key NIST guidance.³³ While FAA has integrated these six activities into the AMS lifecycle, our analysis of two NextGen foundational programs, SBSS and Data Comm, revealed instances in which some of these activities were not completed properly, or were completed in an untimely manner. In addition, while Data Comm managers have thus far provided oversight of their contractors' security-related acquisition activities, SBSS managers did not possess some of the detailed information that would have enhanced their oversight prior to the system's deployment.

³²See GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*. [GAO-12-1022](#). Washington, D.C.: September 2012). We recommended in 2006 that FAA be more collaborative and include all stakeholders in NextGen efforts as directed by Congress. See GAO, *Next Generation Air Transportation System: Progress and Challenges Associated with the Transformation of the National Airspace System*. [GAO-07-25](#) (Washington, D.C.: November 2006). In response, FAA commented they planned to consider this recommendation.

³³NIST SP800-37, *Guide to Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 and NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, October 2008. The former publication provides guidance for integrating security risk management activities into an organization's life cycle processes. The latter publication provides guidance on how essential information-technology security steps can be integrated into the life cycle. Steps that both publications have in common include system categorization; selecting, implementing and assessing security controls; authorizing the system to operate based on risk; and ongoing monitoring of the security controls. NIST guidance was developed to implement provisions of the Federal Information Security Management Act of 2002 (FISMA).

FAA's Acquisition Management System Incorporates NIST's Information-Security Guidance throughout the Acquisition Life Cycle

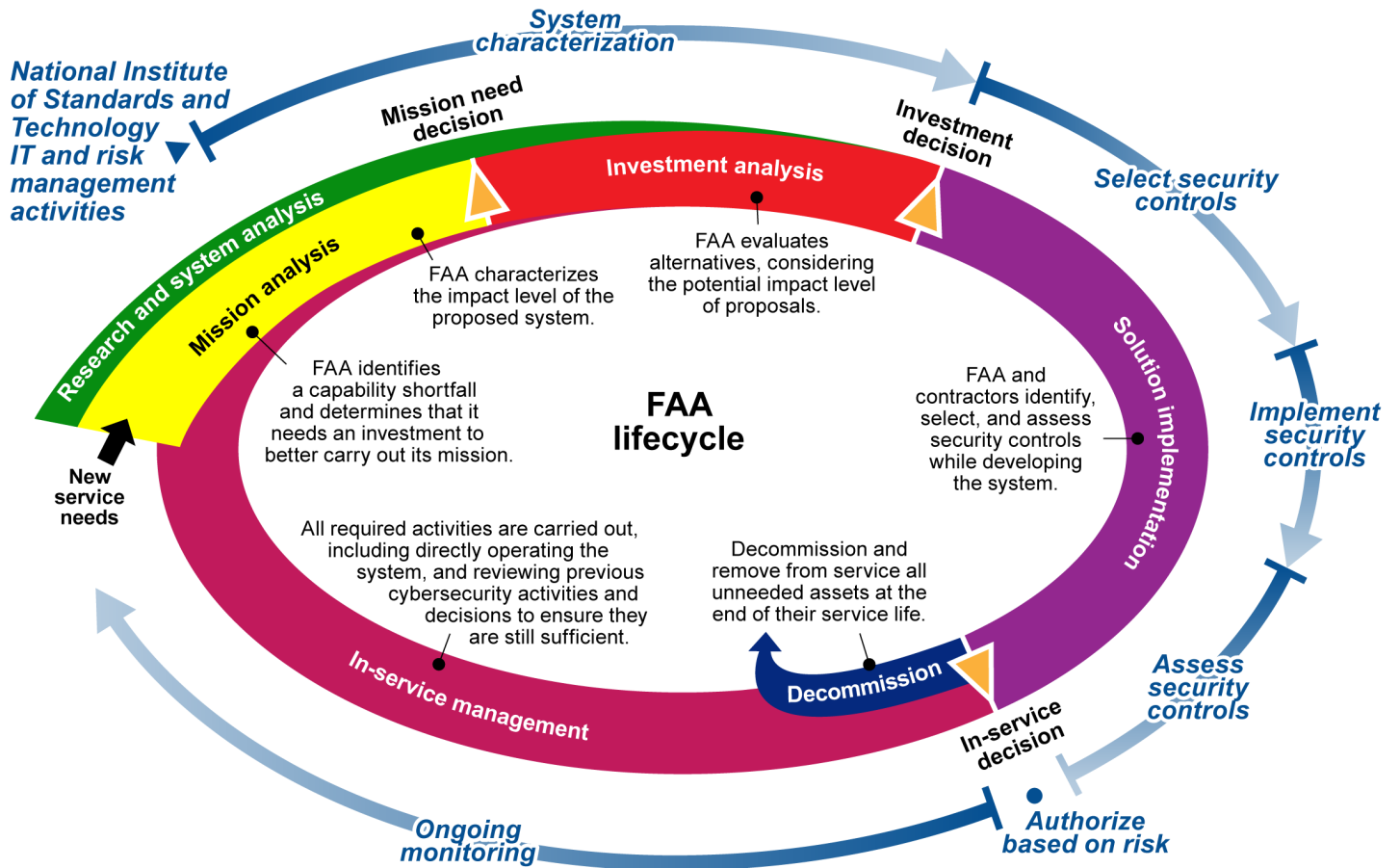
To its credit, FAA has integrated NIST's six broad information-security and risk-management activities into its AMS, which guides the life cycle processes to be followed in developing FAA information systems. These activities include

- categorizing the system's impact level,³⁴
- selecting security controls,
- implementing the security controls,
- assessing the security controls,
- authorizing the system to operate based on the results of security assessments and a determination of risk, and
- monitoring the efficacy of the security controls on an ongoing basis following a system's deployment.

These activities and their relationship to FAA's AMS life cycle are shown in figure 5 below.

³⁴ *Security categorization* determinations consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation (SP 800-37).

Figure 5: Phases of the FAA's Acquisition Life Cycle and National Institute of Standards and Technology's Information-Technology and Risk-Management Activities



Sources: GAO and FAA. | GAO-15-370

System categorization: NIST guidance states that in applying the risk management framework to federal information systems' design and development processes, agencies should first categorize each information system's impact level (i.e., the severity of the consequences

to the agency's mission if a system were compromised).³⁵ In accordance with this guidance and other federal agency requirements, FAA's acquisition process requires that each new system's security impact level be categorized as low, moderate, or high based upon the risks associated with the system and the information it processes, stores, or transmits.³⁶ Of the six foundational NextGen systems we reviewed, all have completed at least an initial categorization process.

Select security controls: NIST guidance states that agencies should next select protective measures, known as security controls, based on the characterization described above.³⁷ According to NIST guidance and federal agency requirements, the impact categorization determines which security control baseline (i.e., starting point for consideration) the system should use, as the low-impact baseline lists fewer controls than the moderate- or high-impact baselines. NIST guidance also states that as part of the selection phase, organizations should tailor the baseline security controls so that they align with the system's specific mission, function, or environment. In some cases, this aligning may include eliminating some inapplicable controls or applying supplemental controls. In accordance with NIST guidance, FAA's acquisition policies require the selection of appropriate security controls that reflect the system's categorization, and allow for appropriate tailoring of security controls. For example, detailed tailoring directions are provided in an FAA handbook that supplements the AMS. In addition, FAA recently drafted guidance to require that programs report, among other things, the cybersecurity decisions and activities conducted in the selection of security controls.

³⁵To determine the impact level of an information system, an agency must first determine the different types of information that the system processes, stores, or transmits. Then, for each information type, the agency categorizes the impact values for three security objectives: confidentiality, integrity, and availability. Last, the agency determines which of the three security objectives has the highest impact value—this "high water mark" measure is the overall information-system security categorization.

³⁶This categorization process is required by Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information Systems*. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, states that agencies should use a minimum baseline of security controls based on the FIPS 199 categorization level. The minimum security baselines for each system categorization are defined in NIST 800-53, *Security and Privacy Controls for Federal Information Systems*.

³⁷Examples of security controls include user identification processes, contingency planning, and the physical security of servers and other hardware.

Implement security controls: NIST guidance also states that once selected, the system must implement controls specified in the security plan. The guidance emphasizes that implementation helps protect systems against possible compromise. When NIST changes its guidance and introduces new security controls, OMB calls for deployed systems to implement the controls within one year of the change, and for systems under development to comply with NIST publications upon their eventual deployment. The handbook that supplements FAA's AMS states that selected and tailored security controls should be implemented; however, according to FAA officials, FAA does not have a policy regarding how quickly to implement new NIST controls, and one official stated that the OMB's direction is "not realistic" given current constraints. The official noted that while the agency recognizes that its implementation cycle for critical cybersecurity controls needs to be more agile and responsive, swift implementation is hampered by federal-funding processes, acquisition requirements, and, as discussed below, the need to extensively test security controls. The official noted that FAA is considering adapting acquisition practices in order to rapidly implement critical controls; however, no definitive plan has been established.

Assess security controls: Additionally, NIST guidance states that assessments are important to ensuring that the security controls are functioning as intended. If a weakness is discovered during the assessment process, agencies are expected to generate a remediation plan to address the identified weakness. OMB directs agencies to develop plans of action and milestones (POA&Ms), which are intended to help agencies act upon assessment findings. Similarly, FAA's acquisition policies state that security controls should be assessed to ensure that they provide the necessary security protection for each acquired system. The FAA handbook that supplements the AMS provides detailed guidance on managing POA&Ms in the event that the assessments discover weaknesses.

Authorize system to operate based on risk: In addition, FAA's AMS states that systems must obtain security authorization approval prior to receiving authorization to operate, which reflects NIST guidance that authorization to deploy a system should only be granted after considering the risks. NIST guidance states the authorizing officials should consider the results of assessments, including POA&Ms, in their decisions. Similarly, the FAA acquisition process requires that the authorizing official receive POA&Ms to assist them in deciding if the system can be deployed. Moreover, the AMS requires that systems be reauthorized at least every 3 years, and the decision regarding whether or not the security risks are acceptable

must be reconsidered at that time. According to both NIST and FAA policy, reauthorization may take place more frequently than every 3 years if significant changes occur to the information system environment.

Monitor security controls on ongoing basis: Last, NIST guidance states that agencies should monitor the security controls on an ongoing basis after deployment, including assessing controls' effectiveness and reporting on the security state of the system. FAA's AMS states that the security controls must be monitored after the system is deployed to ensure that they operate as expected and provide the necessary protection. Examples of FAA's continuous monitoring activities include periodic scans of operational systems, patching vulnerabilities, and updating the system's security plan. FAA's acquisition policies also require that each system assess a subset of its controls every year. Core security controls, which have greater volatility or importance to the organization, are to be assessed every year.³⁸

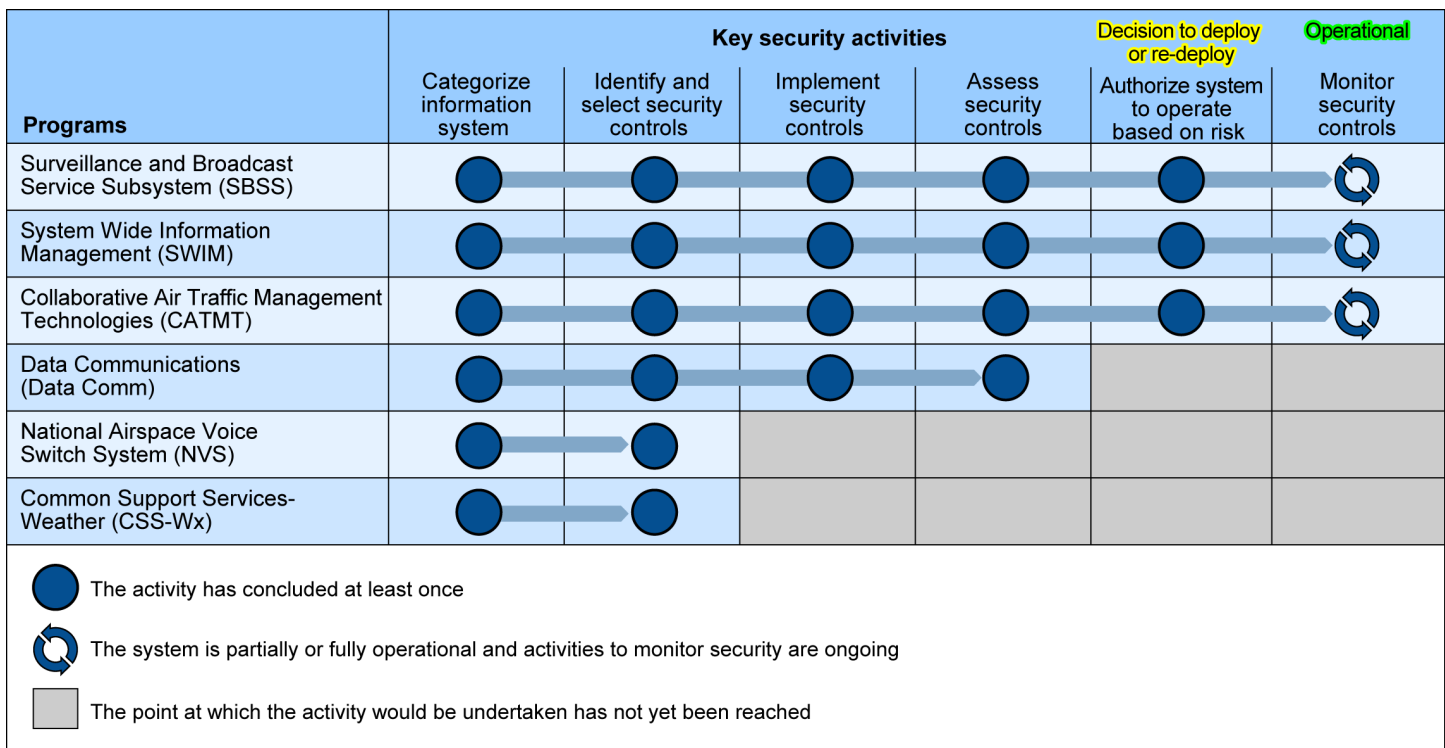
We found that for all six NextGen foundational programs, FAA is addressing the broad security activities described in the AMS and NIST. The six programs are in various stages of the acquisition life cycle, which drives when security design and development activities should be done, as shown in figure 6 (below). For example, Common Support Services-Weather, and NAS Voice Switch are in the early stages of the life cycle, so some security activity milestones have not yet been reached. These two programs have only finished selecting their respective security controls. Other programs, such as SBSS, have performed all of the broad security activities at least once and are now in the post-deployment, ongoing monitoring phase.³⁹ According to FAA policy, during the ongoing monitoring phase, some of the six broad activities will be reviewed or

³⁸The Department of Transportation's Inspector General reported in November 2014 that FAA has not executed all elements of an effective continuous monitoring program. For example, the department has not implemented metrics or monitoring/assessment frequencies. However, the audit confirmed our finding that FAA has a policy for continuous monitoring. Department of Transportation: Office of Inspector General Audit Report FI-2015-009. *FISMA 2014: DOT Has Made Progress But Significant Weaknesses in Its Information Security Remain*. (Washington DC: November 14, 2014.)

³⁹NextGen programs are completed in stages, sometimes referred to as *builds*. As a result, even when one build of a system is operational, the program is not necessarily complete. New features and capabilities can be added to the system over time as future builds move through the acquisition process. Moreover, some steps can be completed more than once. For example, multiple assessments can take place.

repeated to determine whether updates are required. For example, security controls for SBSS have been re-assessed by FAA’s independent risk assessment team, which conducts testing, demonstrations, file reviews, and interviews with relevant personnel before and after a system becomes operational.

Figure 6: Security Activity’s Progress for Each of NextGen’s Foundational Program



Source: GAO analysis based on FAA data. | GAO-15-370

FAA Generally Followed Federal Guidance for Two Selected NextGen Programs, but Opportunities Exist for Improvement

Many of the six broad risk-management activities described in the AMS and NIST guidance involve security controls. These detailed protective measures—which include topics like access control, contingency planning, and physical security measures—are critical to ensuring that systems are sufficiently protected. Among other things, NIST guidance states that agencies should select security controls and assess the efficacy of security controls. In addition, NIST and OMB expect agencies to address weaknesses found during assessments. We analyzed two NextGen programs’ treatment of security controls and remediation

SBSS and Data Comm
Generally Documented
Security Control Selection
Decisions, but Do Not Require
the Most Recent NIST Controls

activities: (1) SBSS, which is operating in some parts of the NAS, including over the Gulf of Mexico, and (2) Data Comm, which has not yet finished the acquisition process but has deployed a test system. We selected these because of their importance to NextGen, cost, and deployment status. Although FAA adhered to aspects of federal guidance on control selection, assessment, and weakness remediation, its implementation of these risk management activities could be or could have been improved.

NIST provides the specific security protections, known as security controls that an organization should consider to help protect an information system.⁴⁰ For a “moderate impact” system, like the majority of the foundational NextGen systems that have completed the categorization process, NIST lists more than 200 such controls as a baseline. However, NIST acknowledges that agencies should tailor security controls so that they are relevant and appropriate for their individual systems. The process of tailoring controls can include electing to rely on common controls rather than selecting a comparable NIST control for implementation,⁴¹ or deciding that controls identified by NIST are not applicable for a particular system. According to NIST guidance, these decisions must be justified and appropriately documented, such as in a system security plan.

When SBSS was developed, FAA and its contractors selected controls from NIST guidance. For example, they selected controls such as an audit record of login attempts and automated mechanisms to alert security personnel to malicious activity. As allowed by the NIST and FAA guidance, SBSS determined that many controls were not applicable or were already covered by existing common controls, such as policies and procedures related to FAA security management activities. SBSS’s initial system-security plan accounted for the majority of moderate baseline controls recommended at the time. However, it did not sufficiently document the implementation details for some controls, including contingency planning and incident response controls. For example, the

⁴⁰NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

⁴¹Common controls are “inheritable,” and are therefore common for all the agency’s systems (e.g., policies and procedures.) According to NIST, typically, these common controls are outside the direct control of the individual systems and programs, and are centrally maintained and managed.

initial system security plan described the existing process that FAA used to detect and respond to incidents affecting NAS systems. However, it did not describe system-level requirements or procedures for incident handling for SBSS. A few of these controls were associated with weaknesses identified during the assessment process, indicating that these controls should have received more consideration during the selection process. Better documentation in the system security plan may have supported such consideration. While FAA's system-security plan template from fiscal year 2009 provided guidance on documenting security controls, the fiscal year 2015 system-security plan template has since been updated based on NIST guidance and provides substantially more detailed instruction than in the past.

In addition, the 2008 SBSS system security plan did not record decisions associated with more than three dozen enhancements that NIST provides to strengthen the controls and that are included in the security baseline. For example, while the system security plan accounted for permitted actions without identification or authentication, it did not document the enhancement that clarified that actions should be permitted to the extent necessary to accomplish mission objectives. This lack of documentation may have been due to limitations in FAA's system security-plan template during that time period. While the template provided instruction that enhancements were to be documented, it did not specifically identify them in the same way that other controls were identified. SBSS continues to update the system security plan and security controls as part of the ongoing monitoring process, and the current system -security plan template covers enhancements.

The Data Comm program is newer than SBSS and is not yet operational, and as such, its initial security control selection is still under way.⁴² As of October 2014, Data Comm had included approximately 60 percent of the more than 250 controls listed in the third version of the NIST 800-53 guidelines, some of which were identified as common controls. As for the slightly more than 100 controls that were identified as out of scope at this time, an FAA official explained that updates will be made as the program

⁴²Data Comm is using a proof-of-concept device to operate a test system at two airports, Memphis and Newark. Although the test system completed certain security processes and received authorization to operate, officials explained that it is not Data Comm; rather, the test system is a tool being used to gather information that will inform the development of Data Comm. The Data Comm system itself is not operational.

matures and that more security controls may be added in the future as deemed necessary. In accordance with NIST guidance, Data Comm has documented its justification for its current selection of NIST controls and its tailoring decisions to date in the system security plan.

However, even though SBSS and Data Comm contractors justify control selection in the programs' respective system-security plans, the contractors are not required to implement the most recent controls unless specifically tasked to do so by FAA. Currently, the SBSS contractor is only obligated to follow the first revision of NIST guidelines from 2006, although NIST has updated the guidelines three times since that time, most recently in 2013. Data Comm's contractor is required to follow the third version of the guidelines, which was published in 2009, and updated in 2010. NIST updates its guidelines to reflect new and emerging threats, and issues new security controls to help agencies better protect their systems. According to NIST, the most recent update was motivated by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the technical competence of the attackers, and the persistence of targeting by attackers). According to FAA, systems can incorporate new controls on an ad-hoc basis or by modifying systems' contracts to reflect updated NIST guidance, and NIST's most recent controls are reflected in FAA's updated templates and guidance.⁴³ However, FAA does not require that contracts be modified within a particular time frame to reflect NIST revisions.

Although the SBSS program asks the contractor to implement more recent NIST controls on an ad-hoc basis, these actions are outside of the contract's requirements and, according to program officials, must be paid for separately. While ad-hoc additions may be sufficient in some cases, SBSS has not yet implemented some of the controls that NIST recommended in its 2010 revision, but plans to address these controls in accordance with NIST's 2013 update as these are part of a large update. SBSS officials explained that they did not previously have funding for an update of such a large scope, but they requested and received funding beginning in fiscal year 2015. According to program officials, these funds will allow them to adopt the missing controls. An FAA official stated that the SBSS program plans to adopt the most recent version of the NIST

⁴³FAA updates its system-security authorization handbook yearly, and the October 2014 update reflects NIST's latest revision to the security controls in 2013.

standards in fiscal year 2016. Given the pace of change in the threat environment, OMB is directing agencies that timely adoption of new NIST guidance, within a year, is critical to enhancing the protection of agencies' information systems. As previously discussed, OMB requires that if NIST updates its security control guidance—which has occurred four times since the guidance was initially developed in 2005—deployed systems must implement all relevant updates within one year.⁴⁴ Systems with weaknesses that could be exploited by these adversaries may be at increased risk if relevant controls in the new NIST guidelines are not implemented.⁴⁵

With regard to Data Comm, an FAA official responsible for the program explained that the program security office had reviewed the changes in the most recent version of the NIST guidelines and that the official did not believe any security control changes that warranted a contract modification.⁴⁶ Rather, the program will identify any security differences between the baseline and the latest NIST 800-53 revision 3 as part of the acquisition process and address them in the resulting POA&Ms, if required. However, the program office did not have an official analysis associated with this decision. NIST guidance recommends that agencies document the assumptions, constraints, and rationale supporting significant risk-management decisions in order to inform future decisions. Without documentation of its analysis, Data Comm's future managers may not be able to react appropriately when the threat landscape

⁴⁴OMB also states that for information systems under development, agencies are expected to be in compliance with the NIST guidance immediately upon deployment of the information system. However, NIST guidance permits agencies to deploy systems even if weaknesses are known, so long as the risks associated with such weaknesses are acceptable to the agency. Agencies create plans of action and milestones (POA&Ms) to help monitor and address weaknesses found prior to deployment.

⁴⁵NIST makes clear in its most recent guidance that its baseline protections should be considered a starting point for information security. Similarly, 8 of the 15 cybersecurity experts we consulted spoke about the protection offered by NIST guidance. All agreed that following NIST guidelines was a necessary basic step, but noted that additional protections will be necessary to provide high-quality cybersecurity protection for NAS systems.

⁴⁶According to NIST, there may be cases when a system's design and existing controls do not warrant a contract modification. For example, if NIST issues an update in response to new threats that do not apply to a particular system, or apply in a very limited manner and are addressed on an ad-hoc basis.

SBSS Did Not Sufficiently Assess Key Controls Prior to Deployment, a Lack Which Contributed to a System Outage

changes to such a degree that a contract modification would be warranted.

FAA did not sufficiently test certain security controls provided by the system's contractor prior to SBSS's deployment. As previously discussed, NIST guidance permits agencies to rely on controls provided by another party, such as a contractor; however, it instructs agencies to ensure that such controls are still sufficient and appropriate. As NIST explains and as GAO has previously found,⁴⁷ the responsibility for mitigating risks arising from the use of contractor-provided systems and security controls lies with the agency. NIST instructs agencies to determine if security controls provided by external parties are sufficient to ensure protection. While NIST guidance provides some latitude in how agencies are to accomplish this task, the guidance makes clear that the steps must be sufficient to ensure the security of the system at hand. However, FAA's pre-deployment testing of SBSS was insufficient. Specifically, according to the SBSS contractor, FAA used a briefing by the contractor to determine that the contractor's processes for managing and controlling changes to SBSS were sufficient. However, the agency did not evaluate the processes to ensure that they were in place and operating effectively until October 2009, nearly a year after the system was initially deployed, when FAA identified significant weaknesses with the SBSS configuration controls⁴⁸ implemented by the contractor.

Shortcomings in these contractor-provided change-management security controls contributed to a significant SBSS system outage. Specifically, in August 2010, an engineer made an error while implementing a system change that caused the network to shut down, which prevented surveillance data transmitted through the hub from reaching FAA control centers. As a result, air traffic controllers could not use SBSS surveillance data to help separate aircraft in the affected locations for nearly 16 hours. A report produced by the SBSS contractor after the outage identified that the outage had occurred because of shortcomings in the processes and controls for managing and controlling changes to the system, and

⁴⁷GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, [GAO-14-612](#). (Washington DC: August 2014).

⁴⁸Configuration management involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle.

recommended steps to ensure that such a disruption would not occur again, including strengthening these controls.⁴⁹ Although FAA's testing had discovered weaknesses in a few of the controls less than a year before the outage, more robust testing of the controls prior to deployment may have indentified these issues earlier—possibly allowing for any identified to be corrected in time to potentially prevent or reduce the impact of the outage. However, these weaknesses had not yet been remedied when the outage occurred.⁵⁰ FAA officials stated the outage has been thoroughly investigated to ensure that the SBSS program and the contractor learned from the experience, and that remedial actions were taken to strengthen the controls. Furthermore, a representative from the SBSS contractor noted that NextGen programs share information on an ad hoc basis to allow other systems to benefit from their experiences.

Although Data Comm has not finished selecting its security controls, an FAA official who manages the program reported that the contractor is testing controls that have been selected thus far.⁵¹ In addition, Data Comm had identified more than 70 controls as of October 2014 that it classified as common controls. As previously discussed, common controls are managed by the agency, and accepting these controls is permitted by NIST guidance. According to FAA, Data Comm and other NextGen systems rely on the integrity of common controls so that they do not have to duplicate effort and spend funds needlessly. However, we recently reported that FAA did not test how some common controls protected the security of systems being added to the ATC environment.⁵² For example, FAA defined the security awareness training common control, but the testers did not examine training records to verify that personnel on the systems that rely on the control were taking the training.

⁴⁹FAA also produced a report in September 2010, which found that monitoring of the ground stations, communication between facilities, and training related to outage response could be improved. The Department of Transportation Inspector General reported in 2011 that FAA was taking action to improve these issues. Department of Transportation Office of Inspector General. AV-2011-149. *FAA Oversight Is Key for Contractor-Owned Air Traffic Control Systems That Are Not Certified* (Washington DC: Aug. 4, 2011).

⁵⁰Untimely resolution of security weaknesses will be discussed in the next section of this report.

⁵¹Due to the iterative process of control selection and testing, we did not determine what percentage of controls had been tested.

⁵²GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*. [GAO-15-221](#). (Washington DC: January 2015).

SBSS Did Not Consistently
and in a Timely Manner
Address System Weaknesses
Discovered during
Assessments

We recommended that FAA ensure that testing of security controls, including common controls, is comprehensive enough to determine whether these controls are operating effectively, and FAA concurred.

According to NIST guidance and the AMS, agencies are expected to create plans of action and milestones (POA&M) when security weaknesses are detected during the testing of an information system. According to NIST and OMB, POA&Ms are a remediation plan with milestone dates for corrective actions that are needed to mitigate the identified weakness.⁵³ In order for a POA&M to be closed, risk must be at an acceptable level. For example, the program might implement additional security controls, or further examination may show that the weakness is an acceptable risk or not actually applicable to the system. However, SBSS has not always remediated weaknesses identified in POA&Ms, which exposes the system to risk. According to FAA, SBSS was deployed in 2008 with weaknesses in the program's intrusion detection system, a shortcoming that was still unresolved as of early 2015. An FAA official explained that remedial actions had not been implemented previously due to a lack of funding, but would be applied as part of an estimated \$42 million update in fiscal year 2015.

In addition, we recently reported⁵⁴ that current POA&Ms for four FAA programs, including SBSS, were not always addressed in a timely fashion. Of 26 SBSS POA&Ms that were completed during 2014, 25 were at least 6 months late, and 12 of these were more than 1 year late. For example, testing showed that certificates for many secure sockets layers, which facilitate secure connections between a server and a browser, had expired. Several FAA officials told us that timely resolution of POA&Ms had been an issue in previous years as well. According to ATO officials, one reason that original deadlines are often missed is that programs lack sufficient resources and funding to address weaknesses by their original due dates. In addition, prior to October 2013, programs used a POA&M-tracking system that one official described as "rudimentary." According to officials, the system only produced updates once a month, which was too

⁵³POA&Ms can be generated at multiple points in the acquisition lifecycle. For example, they can be created during the system development and implementation phase; shortly before systems are presented for authorization to operate; or during ongoing monitoring and review.

⁵⁴GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*. [GAO-15-221](#). (Washington DC: January 2015).

infrequent to facilitate timely oversight and resolution of POA&Ms. In October 2013, FAA implemented a new POA&M database, known as the SMART Tool, that FAA officials say is intended to improve oversight, and could reduce delays in addressing POA&Ms.⁵⁵ Although FAA policy does not identify a maximum amount of time that a POA&M can remain unresolved, delays in addressing security weaknesses extend the amount of time that systems are vulnerable to exploitation. FAA officials agreed that systems are more secure when POA&Ms are resolved in a timely fashion.

In addition, until September 2014, Data Comm had not finished formally documenting the rationale as to why it did not plan to mitigate some of the weaknesses of a test system associated with the program. These weaknesses had been discovered in fiscal year 2013. Specifically, the Data Comm program is using a test system at two locations to obtain feedback from controllers, pilots, and other users. The test system generated 30 POA&Ms in fiscal year 2013, and FAA has since resolved them. However, FAA officials reported that they do not intend to address all of the POA&Ms because they will replace the test system in 2016 with new technology that reflects user feedback. All of the POA&Ms are categorized as “low risk,” and FAA officials explained that their analysis of the costs, risks, and benefits indicates that these POA&Ms are not worth addressing given the replacement schedule; however, this analysis was not initially noted in the POA&M records. As noted previously, NIST guidance states that documenting significant risk management decisions is imperative in order for officials to have the necessary information to make credible, risk-based decisions. We asked Data Comm officials about this concern in September 2014, and were told that Data Comm had taken action to remedy the situation during the course of our audit. Specifically, the POA&M records were updated to reflect the program’s decision process.

⁵⁵According to FAA officials, information on open POA&Ms was completely migrated to the SMART Tool as of December 2013. Given the timing of our review, it was not possible to determine if the SMART Tool improved timeliness.

Oversight of the SBSS Contractors' Security Requirement Development and Security Control Implementation Was Lacking in Some Instances

According to FAA's AMS, procurement should be an integrated part of the acquisition life-cycle management process, and contract administration should include monitoring contract deliverables. We found that FAA and the SBSS contractor communicated about key milestones during the acquisition process, and such communication contributes to the broad goal of contract monitoring. For example, the contractor performed the design-phase risk assessment (which detailed the methodology for control selection), presented that assessment to FAA, and received comments from FAA on the control selection process. However, FAA's ability to monitor SBSS's contract deliverables was reduced by limitations in the system's work breakdown structure (WBS).⁵⁶

A WBS deconstructs the program's end product into successive levels with smaller elements until the work has been subdivided into a level suitable for management control. The lowest, most detailed level of the WBS is defined as the work package level. There were more than 50 work packages for SBSS, but our analysis found that the work packages for SBSS primarily covered management issues for certification and accreditation versus detailed security issues. Consequently, most of the work packages did not address design and development activities for specific, complex, technical-security requirement areas. Moreover, many of the work packages' project implementation activities were not formally tracked or monitored. As a result of these issues, FAA could not effectively monitor the contractor's cost, schedule, and technical problems associated with specific security requirements. The lack of specificity and oversight unnecessarily increased the risk that weaknesses could occur.

SBSS's contractors are also responsible for implementing security controls to address weaknesses, but we found that in at least one case, FAA did not exercise its oversight responsibility to provide the contractor with sufficiently timely feedback on the plans of action (i.e., POA&Ms) that detail which security controls should be adopted. Specifically, in 2013, the contractor provided FAA with cost and schedule assessments associated with 48 POA&Ms. However, despite attempts to solicit feedback, FAA did not provide the contractor with timely feedback on this proposal for 5

⁵⁶A *work breakdown structure* is the cornerstone of every program because it defines the work to be performed and provides the means for measuring the deliverable's status. It provides a framework for estimating costs, developing schedules, identifying resources, and determining where risks may occur. Without a work breakdown structure, it would be much more difficult to analyze the root cause of cost, schedule, and technical problems.

months, when FAA declined the proposal. Instead, FAA determined it would issue a new request for proposals based on more recent NIST guidance (rev. 4) to address these controls.

As Data Comm is still under development, its security requirements and selected controls continue to evolve. Officials stated that they work closely with the contractor to ensure delivery against technical cost and schedule requirements. For the security controls selected thus far, FAA is able to trace the control to the associated security requirement, an ability that indicates that FAA is exercising oversight in this area. We also found that the Data Comm program also monitors system development and security through a variety of meetings, such as monthly Program Management reviews, quarterly Executive Committee meetings, bi-weekly Program Management Working Groups, and weekly Contracts meetings. While the AMS does not delineate specific meeting frequency or agenda requirements, the regularity and content from Data Comm's meetings aligns with the AMS guidance to monitor the contract deliverables.

Conclusions

Through its NextGen initiative, FAA is shifting the ATC system from a point-to-point communications system to an Internet-technology-based, interconnected system, a process of changeover that increases cybersecurity risks. FAA is making strides to address these risks, including implementing an enterprise approach for protecting its systems from cyber attack by both internal and external threats in accordance with NIST and other cybersecurity leading practices; however, FAA has not developed a holistic threat model that would describe the landscape of security risks to FAA's information systems. Such a model would inform the ongoing implementation of FAA's cybersecurity efforts to protect the National Airspace System. Development of a threat model could require significant resources and time, however, and FAA would first need to assess the costs and time frames involved in such an effort. FAA has also recognized that extensive changes to its information-security procedures and some realignment of information security functions within its organization are required to implement a secure, interconnected IP-based ATC system, and has taken a number of steps in this direction. However, the experts we consulted were concerned that FAA's plans for organizational realignment have not adequately considered the role of the Office of Safety, which is responsible for certifying the avionics systems aboard aircraft, including cybersecurity of those systems that enable communication with air traffic control and that guide aircraft.

FAA's acquisition management system is evolving to stay up-to-date on federal cybersecurity guidance as FAA designs and develops NextGen systems; and FAA has made significant strides in incorporating requirements for security controls recommended by NIST guidelines into its acquisition of these systems. While FAA generally followed many of the NIST guidelines for establishing security controls in the two key NextGen acquisitions we examined, we found instances where FAA lacked assurance that security weaknesses were properly addressed. For SBSS, FAA did not ensure that weaknesses identified during security reviews were adequately tracked and in some cases were not resolved on a timely basis. As a result, FAA lacked assurance that weaknesses that could compromise system security were addressed, exposing systems to potential compromise. FAA has taken steps to ensure future incidents do not occur, such as creating a more robust remediation system for tracking weaknesses. Also, for both systems, FAA has not yet adopted, as directed by OMB, the latest security controls recommended by NIST guidelines, which reflect updates to deal with the evolving cybersecurity threat to information. Although FAA anticipates that SBSS will adopt these controls in fiscal year 2016, the program has yet to provide the funding to the contractor to implement the controls. Delays in adopting the latest standards extend the amount of time that system security requirements may not adequately mitigate system exposure to the newest threats.

Recommendations

To better ensure that cybersecurity threats to NextGen systems are addressed, the Secretary of Transportation should instruct the FAA Administrator to take the following three actions.

- As a first step to developing an agency-wide threat model, assess the potential cost and timetable for developing such a threat model and the resources required to maintain it.
- Incorporate the Office of Safety into FAA's agency-wide approach by including it on the Cybersecurity Steering Committee.
- Given the challenges FAA faces in meeting OMB's guidance to implement the latest security controls in NIST's revised guidelines within one year of issuance, develop a plan to fund and implement the NIST revisions within OMB's time frames.

Agency Comments and Our Evaluation

We provided a draft of this report to the Department of Transportation for review and comment. The Department provided written comments, which are reprinted in appendix II. The Department concurred with two of our three recommendations. Specifically, FAA concurred with the recommendation that it assess the potential cost and timetable for developing an agency-wide threat model, and the recommendation that it develop a plan to fund and implement NIST revisions within OMB timeframes.

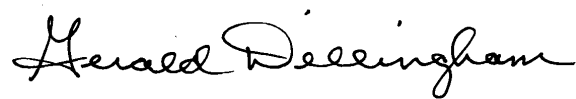
With regard to the recommendation to incorporate the Office of Safety into FAA's agency-wide approach by including it as a member on the Cybersecurity Steering Committee, the Department believes that FAA has already complied with the intent of the recommendation. According to the Department, FAA has transferred cybersecurity personnel from the Office of Safety to the Office of the Chief Information Officer, which manages cybersecurity for all aviation safety information systems. The Department also stated that FAA's Chief Information Office works closely with the Office of Safety on certification standards for non-FAA information systems operating within the National Airspace System. We agree that these actions will help in the execution and coordination of cybersecurity activities involving the Office of Safety. However, we maintain that in addition to these actions, the Office of Safety should be a member of the Cybersecurity Steering Committee, which, as the department notes in its letter, was established to lead FAA's efforts to develop a comprehensive cyber-risk management strategy, and to identify and correct both existing and evolving vulnerabilities in all Internet protocol-based systems. Because aircraft aviation systems are becoming increasingly connected to systems outside the aircraft, the Office of Safety, which is responsible for certifying aircraft systems, should be involved in agency-wide cybersecurity efforts, including cybersecurity planning and vulnerability identification, since such efforts may be crucial in conducting its certification activities. As we state in the report, not including the Office of Safety as a full member of the Committee could hinder FAA's efforts to develop a coordinated, holistic, agency-wide approach to cybersecurity. This lack of involvement could result in omitting an FAA stakeholder that has an understanding of specific technological changes in aircraft traversing the NAS environment and how these changes might intersect with changing ATC technologies and cybersecurity needs.

In its comments the Department stated that FAA is committed to strengthening its capabilities to defend against new and evolving cybersecurity threats. According to the Department, FAA is initiating a comprehensive program to improve the cybersecurity defenses of the

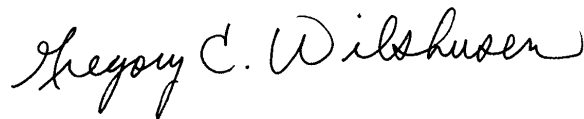
NAS infrastructure, as well as other mission critical systems. The Department's letter lists a number of actions FAA has taken to improve cybersecurity, many of which are described in this report. We applaud FAA's commitment to strengthening cybersecurity in the NAS, and agree that the actions it has taken are important steps for FAA to take. We also believe that addressing our recommendations will result in valuable improvements to the information security of the NAS.

We are sending copies of this report to the Department of Transportation and the appropriate congressional committees. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff members have any questions about this report, please contact me on (202) 512-2834 or at dillinghamg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.



Gerald L. Dillingham, Ph.D.
Director, Physical Infrastructure Issues



Gregory C. Wilshusen
Director, Information Security Issues



Nabajyoti Barkakati Ph.D.
Director, Center for Technology and Engineering

List of Congressional Requesters

The Honorable John Thune
Chairman
The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Bill Shuster
Chairman
The Honorable Peter DeFazio
Ranking Member
Committee on Transportation and Infrastructure
House of Representative

The Honorable Frank A. LoBiondo
Chairman
The Honorable Rick Larsen
Ranking Member
Subcommittee on Aviation
Committee on Transportation and Infrastructure
House of Representatives

The Honorable John Katko
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to (1) identify the key challenges facing FAA as it shifts to the NextGen ATC system and how FAA is addressing those challenges and (2) assess the extent FAA and its contractors followed federal guidelines for incorporating cybersecurity requirements in its acquisition of NextGen programs.

To ascertain challenges FAA faces with NextGen and how FAA has begun addressing these challenges, we obtained relevant security documents from FAA and detailed descriptions of FAA’s cybersecurity efforts from officials. We also selected a non-generalizable sample of 15 cybersecurity and aviation experts with varied experience—some of whom have knowledge of FAA’s internal cybersecurity activities, policies, and personnel. We then analyzed the information about FAA’s cybersecurity efforts, synthesized it, and produced a document that we provided to the experts for their review. FAA concurred that the document was accurate. We then interviewed the experts, collecting information on the cybersecurity challenges they think FAA faces and will face in the NextGen transition. Interviewees also commented, to the extent they were able, on the extent to which FAA’s cybersecurity activities and plans address the identified challenges. We analyzed and synthesized these responses, reporting on the numbers of experts who discussed particular topics as well as the numbers of experts who agreed or disagreed on particular messages. The experts from whom we obtained responses are listed in table 1.

Table 1: Experts Providing Responses to Cybersecurity Challenges Facing FAA

Expert	Organization	Title and position
John Knight, Ph.D.	University of Virginia	Professor, computer science
Steve Bellovin, Ph.D.	Columbia University	Professor, computer science
Rear Adm. Elizabeth Hight	Hewlett-Packard Company	Vice President, Cyber Security Solutions Group, U.S. Public Sector
Ed Skoudis	SANS Institute	Instructor/penetration tester
Phil Venables	Goldman Sachs	Chief Security Risk Officer
Dennis Sawyer	MITRE	Director, Aviation Systems Engineering and Center for Advanced Aviation Systems Development
Christopher Hegarty, Ph.D.	MITRE	Chief Scientist, Center for Advanced Aviation Systems Development
Barbara Endicott-Popovsky, Ph.D.	University of Washington	Director, Center for Information Assurance and Cybersecurity
David Shaw	Global Business Analysis	Founder, Chief Executive Officer
R. John Hansman, Ph.D.	MIT	Professor, Aeronautics and Astronautics and Engineering Systems

Appendix I: Objectives, Scope, and Methodology

Expert	Organization	Title and position
John Campbell	Iridium Communications	Chairman, Government Advisory Board
Richard Heinrich	Rockwell Collins	Director, Commercial Systems Strategy Development
Greg Rice	Rockwell Collins	Principal Cyber Security Engineer
Jeff Snyder	Raytheon	Vice President, Cyber Programs
Ronda Henning, Ph.D.	Harris Corporation	Senior Scientist for Security and Privacy

Source: GAO. | GAO-15-370

Separately, we also obtained the views of several aviation industry officials, including officials from the Airlines for America, Airports Council International—North America, Air Line Pilots Association, General Aviation Manufacturers Association, Garmin, MITRE Corporation,¹ National Air Traffic Controller Association, and the Boeing Corporation. We also reviewed relevant reports issued by GAO, the Inspector General of the Department of Transportation, and the National Academies.

To assess the extent to which FAA and its contractors, in the acquisition of NextGen programs, have followed federal guidelines for incorporating cybersecurity controls, we compared pertinent FAA policies, procedures, and practices with selected federal information security laws and federal guidance, including standards and guidelines from the National Institute of Standards and Technology (NIST). In particular, we compared FAA’s Acquisition Management System (AMS) against NIST’s risk management guidelines and information technology-security guidelines (800-37) and security considerations in software development life cycle (800-64) to determine if FAA’s acquisition policy follows federal cybersecurity guidelines for the six foundational NextGen programs: Surveillance and Broadcast Services (SBSS); Collaborative Air Traffic Management (CATM); Data Communications (Data Comm); NAS Voice Switch (NVS); Common Support Service-Weather (CSS-Wx); and System Wide Information Management (SWIM). The NextGen Foundational Programs consist of different segments, also called builds; parts; and subsystems. Some security activities take place at the program level, while others apply to specific components of the program. We analyzed FAA’s program documentation of key cybersecurity activities as described by

¹MITRE is a not-for-profit organization chartered to work in the public interest. MITRE manages four federally funded research and development centers, including one for FAA. MITRE has its own independent research and development program that explores new technologies and new uses of technologies to solve problems in the near term and in the future.

NIST and interviewed system managers to determine if FAA completed the activities or has plans to complete the activities that were started but not fully completed.

In addition, we chose two key NextGen acquisitions, SBSS and Data Comm, for an in-depth review because of their importance to NextGen, cost, and deployment status. SBSS has completed the acquisition cycle, while Data Comm will allow for insight into how the process has changed and what still might be an issue for upcoming programs. We assessed if FAA had established and implemented a disciplined life-cycle management approach integrated with information security by comparing FAA's policies for system life-cycle management and cybersecurity to NIST guidance on security risk management system acquisition. We also compared documentation of project activities and plans to these requirements, and interviewed officials about FAA's policies and FAA's information security practices. We assessed how well FAA and contractors completed key cybersecurity activities and the extent to which they complied with AMS and NIST requirements relating to cybersecurity. We also compared documentation of project activities and plans to these requirements, and interviewed agency officials about FAA's policies and information security practices. We also reviewed pertinent sections of prior GAO reports related to cybersecurity. We performed our work at FAA headquarters in Washington, D.C.; the Air Traffic Control Systems Command Center in Warrenton, Virginia; and at an FAA contractor location in Herndon, Virginia.

We determined that information provided by the federal and nonfederal entities, such as the type of information contained within FAA's security assessments and Plans of Action and Milestones, was sufficiently reliable for the purposes of our review. To arrive at this assessment, we corroborated the information by comparing the plans with statements from relevant agency officials.

We conducted this performance audit from September 2013 through March 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Department of Transportation



U.S. Department
of Transportation
Office of the Secretary
of Transportation

Assistant Secretary
for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

MAR 31 2015

Gerald L. Dillingham
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

The Federal Aviation Administration (FAA) recognizes that cyber-based threats to federal information systems are becoming a more significant risk and are rapidly evolving and increasingly difficult to detect and defend against. We take this risk very seriously. We know that the Agency must be vigilant against the disruption of critical operations and infrastructure systems as more new internet-connected technologies are introduced into the National Airspace System (NAS). Accordingly, the FAA is committed to strengthening our capabilities to defend against new and evolving threats with a high degree of urgency. The Agency is already in the midst of an expedited transition to a more comprehensive and proactive approach to cyber-threat protection, detection, and rapid response.

It is also important to note that the FAA had already initiated a comprehensive program to improve the cybersecurity defenses of the NAS infrastructure, as well as other FAA mission-critical systems. We are significantly increasing our collaboration and coordination with cyber intelligence and security organizations across the federal government and in the private sector.

Recognizing the need to ensure an Agency-wide view and oversight of cyber-risk, the FAA established an Executive Cybersecurity Steering Committee (CSC) in November 2013, which reports to the Deputy Administrator. The CSC is leading the development of a comprehensive cyber-risk management strategy and governance structure. CSC priorities include the identification and correction of both existing and evolving vulnerabilities on all internet protocol-based systems and the establishment of an Agency-wide threat model for fiscal year 2016.

In moving toward the full implementation of enhanced cybersecurity defenses, the Agency has:

- Published an updated Security Authorization Handbook and supporting templates to incorporate National Institute of Standards and Technology (NIST) requirements for information security and facilitate the implementation of the Risk Management Framework.
- Issued FAA's Policy Statement AIR-21.16-02, Establishment of Special Conditions for Cyber Security, which provides guidance to the Aircraft Certification Offices regarding the application of special conditions to address cyber security vulnerabilities in aircraft certification programs.

- Released Information Security Guidance for System Acquisitions document to support the identification and implementation of requirements for cybersecurity controls in the acquisition process.

The FAA established a Cyber Test Facility at the William J. Hughes Technical Center to enable thorough testing of cybersecurity capabilities to fully understand the impact, if any, before introducing them into our operational systems.

FAA cybersecurity initiatives for fiscal year 2015 include:

- Engaging the Department of Homeland Security (DHS) in their efforts to provide federal agencies with Continuous Diagnostics and Mitigation (CDM) capabilities in support of a Continuous Monitoring strategy for NAS and NextGen. In the near future, the FAA will utilize the DHS acquisition vehicle and associated funding to obtain tools and services to better secure FAA infrastructures and enable early visualization and identification of evolving risks before attacks materialize. This will also enable the FAA to make more informed decisions, prioritize risks, and direct resources to the areas of highest risk. DHS is scheduled to award this contract on April 1, 2015.
- Revising FAA Information System Security (ISS) policies to clarify ISS organizational roles and responsibilities in accordance with NIST guidance. Specifically, complete and submit a draft update to FAA Order for Information Security Policy in coordination with applicable FAA Lines of Businesses and Staff Offices by September 30, 2015.
- Developing an update to the “FAA Cybersecurity Strategy (2016-2020)” by September 30, 2015. This effort will provide a mission-focused strategy to guide the Agency’s efforts. In accordance with NIST guidance, the Non-NAS and NAS Enterprise Architectures are developing tools for the documentation of security architectures and enterprise security requirements. Both the strategic plan and the security architecture will address the current security conditions and the evolution of future NextGen capabilities and will be fully compliant with the requirements of the recent cybersecurity Presidential Orders and Directives.
- Updating the FAA’s Cyber Incident Process to align with the revised US CERT reporting process that will be in effect October 1, 2015. As part of that update, threat intelligence analysis from iSight (DHS sponsored), Intel and Law Enforcement communities will be fused with mission risk priorities for each domain.

The FAA concurs with recommendations 1 and 3 and will implement the appropriate corrective actions by January 30, 2016. The Agency believes it has complied with the intent of recommendation 2. The creation of FAA’s new IT Shared Services organization in October 2013 included the transfer of cybersecurity personnel from the Office of Safety (AVS) to the

**Appendix II: Comments from the Department
of Transportation**

3

Office of the Chief Information Officer (AIT). The cybersecurity of all AVS information systems is now managed by AIT and subject to CSC purview. For external (non-FAA) information systems operating within the NAS, the Chief Information Office works closely with AVS on certification standards to include cybersecurity assurance for aircraft avionics and other information systems.

We appreciate this opportunity to offer additional perspective on the GAO draft report. Please contact Patrick D. Nemons, Deputy Director of Audit Relations, at (202) 366-4986 with any questions or if the GAO would like to obtain additional details about these comments.



Keith Washington
Acting Assistant Secretary for Administration

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Gerald L. Dillingham, Ph.D., (202) 512-2834, or dillinghamg@gao.gov
Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov
Nabajyoti Barkakati, Ph.D., (202) 512-4499, barkakatin@gao.gov

Staff Acknowledgments

In addition to the individual named above, Ed Laughlin, Assistant Director; Gary Austin, Assistant Director; Nick Marinos, Assistant Director; Jake Campbell; Bill Cook; Colin Fallon; Elke Kolodinski; Nick Nadarski; Josh Ormond; Krzysztof Pasternak; and Alison Snyder made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

