United States Government Accountability Office

Report to Congressional Requesters

January 2015

INFORMATION SECURITY

FAA Needs to Address Weaknesses in Air Traffic Control Systems

GAO-15-221

GAO Highlights

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

January 2015

INFORMATION SECURITY

FAA Needs to Address Weaknesses in Air Traffic Control Systems

Why GAO Did This Study

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

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

What GAO Recommends

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

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

What GAO Found

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

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

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

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

Contents

Abbreviations

AIT	Office of Information and Technology
ARTCC	Air Route Traffic Control Center
ATC	Air Traffic Control
ATO	Air Traffic Organization
CIO	Chief Information Officer
ERAM	En Route Automation Modernization
FAA	Federal Aviation Administration
FISMA	Federal Information Security Management Act
FTI	FAA Telecommunications Infrastructure
IP	Internet Protocol
ISSO	Information System Security Officer
NAS	National Airspace System
NCO	NAS Cyber Operations
NextGen	Next Generation Air Transportation System
NIST	National Institute of Standards and Technology
POA&M	Plan of Actions and Milestones
SBSS	Surveillance and Broadcast Service System
TFM-I	Traffic Flow Management-Infrastructure

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 29, 2015

Congressional Requesters

The Federal Aviation Administration (FAA) performs critical functions that contribute to ensuring safe, orderly, and efficient air travel in the national airspace system (NAS). Effective air traffic control (ATC) relies on automated systems and networks to provide information to air traffic controllers and aircraft flight crews to work toward ensuring safe and expeditious movement of aircraft. As a piece of critical infrastructure[1] within the nation's transportation sector,[2] the NAS is vitally important in supporting air traffic control operations nationwide, and disruptions could have a significant adverse impact.

Cyber-based threats to federal information systems such as those that FAA relies on for its ATC systems are evolving and growing. These threats can be intentional or unintentional and can come from a variety of sources, including criminals, foreign nations, terrorists, and other adversarial groups. For example, advanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can attack by using multiple means such as cyber, physical, or deception to achieve its objectives[3]—pose increasing risks. Further, the growing interconnectivity among different types of information systems presents increasing opportunities for such attacks. Because of the

[1]The USA PATRIOT Act of 2001 (42 U.S.C. § 5195c(e)) defines critical infrastructure as systems and assets, whether physical or virtual, so vital to our nation that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these.

[2]The transportation systems sector (which includes aviation as a subsector) is 1 of 16 critical infrastructure sectors identified by Presidential Policy Directive 21 (PPD-21). The other sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; and water and wastewater systems

[3]These objectives typically include establishing/extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or establishing the capability to carry out these objectives in the future. An advanced persistent threat (1) pursues its objectives repeatedly over an extended period of time, (2) adapts to defenders' efforts to resist it, and (3) is determined to maintain the level of interaction needed to achieve its objectives.

increasing number of reported information security incidents, coupled with the advancement of security attacks, information and systems at FAA and across the government remain at risk.

Given the critical role the NAS plays in the nation's transportation sector and the growing threats to federal information systems, you asked us to review FAA's information security program. The specific objective of our review was to evaluate the extent to which FAA has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of its existing ATC systems.

This is a public version of a limited distribution report containing sensitive security information that we provided to you. Some of the information in the prior report has been designated as sensitive security information and must be protected from public disclosure. Therefore, this report does not contain detailed descriptions of the control weaknesses and related recommendations identified during our review. Although the information provided in this report is less detailed, it presents the same overall message as the limited distribution report. Also, the overall methodology used for both reports is the same.

To assess FAA's implementation of security controls on its existing ATC systems, we compared FAA's documented policies, procedures, and practices with the relevant information security law and federal guidance, including National Institute of Standards and Technology (NIST) standards and guidelines. We also assessed the implementation of controls over NAS supporting systems and interconnections by examining risk assessment processes, security plans, security control assessments, contingency plans, and remedial action plans. Specifically, we observed controls over the FAA Telecommunications Infrastructure (FTI), Surveillance and Broadcast Service System (SBSS), Traffic Flow Management-Infrastructure (TFM-I); En Route Automation Modernization (ERAM); and En Route Communications Gateway. We performed our work at FAA headquarters in Washington, D.C., and other locations supporting key systems, specifically: the Air Traffic Control Systems Command Center in Warrenton, Virginia; the FAA's William J. Hughes Technical Center in Egg Harbor Township, New Jersey; and at contractor facilities in Herndon, Virginia; Egg Harbor Township, New Jersey; and Melbourne, Florida.

We conducted this performance audit from August 2013 to January 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. A full description of our objective, scope, and methodology can be found in appendix I.

Background

The FAA, an agency of the Department of Transportation, is primarily responsible for the advancement, safety, and regulation of civil aviation, as well as overseeing the development of the air traffic control system. Its stated mission is to provide the safest, most efficient aerospace system in the world. This system, known as the National Airspace System (NAS), includes air traffic control systems, ATC procedures, operational facilities, aircraft, and the people who certify, operate, and maintain them. According to FAA, the system includes more than 19,000 airports, nearly 600 air traffic control facilities, and approximately 65,000 other facilities, including radar, communications nodes, ground-based navigation aids, computer displays, and radios, intended to provide safe and efficient flight services for the public. Over 46,000 FAA personnel and approximately 608,000 pilots operate about 228,000 aircraft within the NAS, including up to 2,850 flights at any given moment. The system operates on a continuous basis, 24 hours a day, every day of the year.

As aircraft move across the NAS, controllers at several types of air traffic control facilities manage their movements during each phase of flight. According to FAA, these facilities include the following:

- More than 500 air traffic control towers supervise flights within about 5 miles from the airport runway. They give pilots taxiing and take off instructions, air traffic clearance, and provide separation between landing and departing aircraft.
- One hundred sixty Terminal Radar Approach Control facilities provide air traffic control services for airspace that is located within approximately 40 miles of an airport and generally up to 10,000 feet above the airport. These facilities handle sequencing and separation of aircraft as they approach major metropolitan areas.
- Twenty-two Air Route Traffic Control Centers (ARTCC) control and monitor airplanes over the continental United States and between airports. Controlling traffic usually at or above 17,000 feet, the typical center has responsibility for more than 100,000 square miles of airspace generally extending over a number of states. Three of the centers also control air traffic over the oceans. Controllers at these

facilities work with pilots to ensure the flight path is smooth and free of other traffic.

- The Air Traffic Control System Command Center manages the flow of air traffic within the United States. This facility regulates air traffic when weather, equipment, runway closures, or other conditions place stress on the national airspace system. In these instances, traffic management specialists at the command center take action to modify traffic demands in order to keep traffic within system capacity.

Figure 1 provides a visual summary of air traffic control across the different phases of flight.

Figure 1: Summary of Air Traffic Control over the United States

Source: GAO based on Federal Aviation Administration information. | GAO-15-221

Many Networked Information Systems Support NAS Operations

The FAA's ability to fulfill its mission depends on the adequacy and reliability of its air traffic control systems, a vast network of computer hardware, software, and communications equipment. The agency relies on more than 100 air traffic control systems to process and track flights around the world. These complex and highly automated systems process a wide range of information, including radar, weather, flight plans, surveillance, navigation/landing guidance, traffic management, air-to-ground communication, voice, network management, and other information—such as airspace restrictions—that is required to support the

agency's mission. In order to successfully carry out air traffic control operations, it is essential that these systems interoperate, functioning both within and across facilities as one integrated system of systems. According to FAA data available at the time of our review, about one-third of air traffic control systems rely on Internet Protocol (IP)-based networking technologies for communication.

FAA's ongoing effort to modernize the ATC system is referred to as the Next Generation Air Transportation System (NextGen). NextGen involves changes to many aspects of air transportation, including the acquisition of new integrated systems (both software and hardware), flight procedures, aircraft performance capabilities, and supporting infrastructure to transform the current air transportation system into one that uses satellite-based surveillance and navigation operations instead of ground-based radar. These changes are intended to increase the efficiency and capacity of the air transportation system while maintaining safety and accommodating anticipated future growth. As demand for the nation's increasingly congested airspace continues to grow, NextGen improvements are intended to enable the FAA to guide and track aircraft more precisely on more direct routes, reduce delays, save fuel, and reduce aircraft exhaust emissions.[4]

The following five key air traffic control systems perform critical air traffic control functions:

- FAA Telecommunications Infrastructure (FTI) forms the basic telecommunications infrastructure for NextGen, replacing the agency's legacy networks to provide consolidated telecom services for the NAS. The FTI is also intended to reduce costs, improve bandwidth, and offer improved information security services, such as encryption, so that an enterprise-wide approach to information security assurance can be achieved.
- Surveillance and Broadcast Service System (SBSS) provides surveillance services to FAA and the aviation community. Most notably, SBSS provides the Automatic Dependent Surveillance-Broadcast service—one of the six NextGen transformational programs—which is FAA's satellite-based successor to radar. This

[4]We currently have a separate review underway examining FAA's integration of information security requirements in its acquisition of NextGen programs. We plan to issue a report on that review later in 2015.

service makes use of Global Positioning System technology to determine and share precise aircraft location information, and streams additional flight information to the cockpits of properly equipped aircraft.

- En Route Automation Modernization (ERAM) replaces the legacy en route Host computer and backup system, developed more than 40 years ago. According to FAA, much of the system has already been deployed. ERAM is designed to be at the heart of NextGen and is key to advancing FAA's transition from a ground-based system of air traffic control to a satellite-based system of air traffic management. As ERAM evolves, it is intended to provide benefits for users and the flying public by increasing air traffic flow and improving automated navigation and conflict detection services, both of which are vital to meeting future demand and preventing gridlock and delays.
- En Route Communications Gateway (ECG) is a communications system that receives data from sources outside the ARTCC, such as flight plan information and weather data, and passes it to other systems, including ERAM.
- Traffic Flow Management-Infrastructure (TFM-I) provides information processing support for FAA traffic management personnel as they coordinate the use of the NAS and respond to conditions of excess demand. TFM-I receives information on planned and active flights, generates forecasts of demand up to several hours ahead, presents this information to Traffic Management Personnel, and provides automation support for traffic management initiatives to resolve or ameliorate congestion.

Each of these systems, in conjunction with many others that make up the NAS computing infrastructure, works to ensure safe flight passageways for aircraft in U.S. airspace from takeoff to landing.

Information Security Is Critical to the Nation's Critical Infrastructures, Including Air Traffic Control Systems

Safeguarding federal computer systems and the systems supporting the nation's critical infrastructures, including the NAS, is essential to protecting national and economic security, and public health and safety. For government organizations information security is also a key element in maintaining the public trust. Inadequately protected systems may be vulnerable to insider threats as well as the risk of intrusion by individuals or groups with malicious intent who could use their illegitimate access to obtain sensitive information, disrupt operations, or launch attacks against other computer systems and networks. Accordingly, since 1997, we have

designated information security as a government-wide high-risk area.[5] In 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure.[6] Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations at risk of disruption, fraud, and inappropriate disclosure.

Recent federal guidance demonstrates that securing critical infrastructures from internal and external threats is a national priority. For example, in February 2013, the President signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," to address concerns about better securing critical infrastructure from cyber threats. This order, among other things, directed executive branch agencies to promote the adoption of cybersecurity practices; increase the volume, timeliness and quality of cyber threat information sharing; incorporate privacy and civil liberties protections into every initiative to secure critical infrastructure; and explore the use of existing regulation to promote cybersecurity. The order also directed the National Institute of Standards and Technology (NIST) to develop a technology-neutral voluntary framework for improving critical infrastructure cybersecurity. The framework, issued in February 2014,[7] is designed to help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources.

Although many legacy air traffic control systems continue to rely on point-to-point communications, NAS systems, including NextGen systems, increasingly use IP technologies to communicate over interconnected computer networks. With the increased use of such technologies, however, comes increased risk: integrating critical infrastructure systems with information technology networks provides significantly less isolation from the outside world than predecessor systems, creating a greater need to secure these systems from remote, external threats.

[5]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997).

[6]See, most recently, GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: Feb. 14, 2013).

[7]NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Gaithersburg, Md.: Feb. 12, 2014).

Several Organizations within FAA Are Responsible for Information Security

The operational arm of the FAA is the Air Traffic Organization (ATO), which is responsible for providing safe and efficient air navigation services to the nation's airspace. ATO is led by a Chief Operating Officer who reports directly to the FAA Administrator. The ATO includes seven service units: Air Traffic, Management, Mission Support, Program Management Organization, Safety and Technical Training, Systems Operations, and Technical Operations.

Several entities within ATO share responsibility for information security-related activities over air traffic control systems. The NAS Security Risk Executive is the individual with overall responsibility for overseeing all information security-related activities across ATO, including the security of air traffic control systems. ATO's Information Security Systems Group, within Technical Operations Services, includes NAS Cyber Operations (NCO), ISS Engineering, and an Authorization Team. Ensuring that each air traffic control system is properly secured and protected is the responsibility of an Information Systems Security Officer (ISSO), and the system owner is responsible for planning, directing, and managing resources for the system, including ensuring that the system meets all security requirements throughout its life cycle. The Security Risk Executive, Authorization Team, NCO, system owners, and ISSOs are jointly responsible for carrying out security program activities for NAS systems, including conducting system risk assessments, documenting system security plans, testing security controls, managing remedial action plans, monitoring and responding to incidents, and planning for contingencies.

The FAA Office of Information and Technology (AIT) is responsible for the security of FAA's non-NAS information systems. The office resides within FAA's Office of Finance and Management and is headed by the Chief Information Officer (CIO), who has overall responsibility to oversee the security of the agency's information and information systems. The FAA Chief Information Security Officer is responsible for developing, documenting, and implementing an agency-wide information security program and for assisting the CIO in ensuring compliance with federal law pertaining to information security and other applicable policies, standards, requirements and guidelines.

Requirements for Ensuring the Security of Federal Information Systems Are Established in Law and Guidance

Federal law and guidance specify requirements for protecting federal information and information systems. The Federal Information Security Management Act of 2002 (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or another organization on behalf of an agency.[8]

FISMA assigns certain responsibilities to NIST, which is tasked with developing, for systems other than national security systems, standards and guidelines that must include, at a minimum, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

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:

- Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*,[9] requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values from among the security categories that the agency identifies for each type of information resident on those information systems.

[8]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As our review was finishing, the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) was enacted. However, the new law, which supersedes FISMA, incorporates the requirements from FISMA that we relied upon in our report. Accordingly, no changes to our findings were necessary.

[9]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

- Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*,[10] specifies minimum security requirements for federal agency information and information systems and a risk-based process for selecting the security controls necessary to satisfy these minimum security requirements.
- NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems*,[11] assists organizations in understanding the purpose, process, and format of information system contingency plan development through practical, real-world guidelines. While the principles establish a baseline to meet most organizational needs, it is recognized that each organization may have additional requirements specific to its own operating environment. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle.
- NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*,[12] explains how to apply a risk management framework to federal information systems, including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
- NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*,[13] provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems. The guidance also provides a

[10]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

[11]NIST, *Contingency Planning Guide for Federal Information Systems*, SP 800-34, Revision 1 (Gaithersburg, Md.: May 2010).

[12]NIST, *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).

[13]NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

structured yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.

- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*,[14] 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.
- NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*,[15] provides guidance for securing industrial control systems, including supervisory control and data acquisition systems, distributed control systems, and other systems performing control functions. The document also provides an overview of industrial control systems and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. Because there are many different types of industrial control systems with varying levels of potential risk and impact, the document provides a list of many different methods and techniques for securing them.
- NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*,[16] informs members of the information security management team (agency heads; CIOs; senior agency information security officers, also commonly referred to as chief information security officers; and security managers) about various aspects of information security that they will be expected to implement and oversee in their respective organizations. In addition, the handbook

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

[15]NIST, *Guide to Industrial Control Systems (ICS) Security*, SP 800-82 (Gaithersburg, Md.: May 2013).

[16]NIST, *Information Security Handbook: A Guide for Managers*, SP 800-100 (Gaithersburg, Md.: October 2006).

provides guidance for facilitating a more consistent approach to information security programs across the federal government.

Security Weaknesses Place Air Traffic Control Systems at Risk

Although FAA has taken steps to safeguard its air traffic control systems, significant security control weaknesses remain in NAS systems and networks, threatening the agency's ability to adequately fulfill its mission. FAA established policies and procedures for controlling access to NAS systems and for configuring its systems securely, and it implemented firewalls and other boundary protection controls to protect the operational NAS environment. However, a significant number of weaknesses remain in the technical controls—including access controls, change controls, and patch management—that protect the confidentiality, integrity, and availability of its air traffic control systems. Additionally, significant interconnectivity exists between non-NAS systems and the NAS operational environment, increasing the risk from these weaknesses. Further, the agency had not yet fully implemented an agency-wide information security program to ensure that controls are appropriately designed and operating effectively. A key reason for both the technical control weaknesses and the security management weaknesses is that FAA had not fully established an integrated, organization-wide approach to managing information security risk that is aligned with its mission. These shortcomings put NAS systems at increased and unnecessary risk of unauthorized access, use, or modification that could disrupt air traffic control operations.

FAA Did Not Consistently Control Access to NAS Systems

A basic management objective for any agency is to protect the resources that support its critical operations and assets from unauthorized access. An agency can accomplish this by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computer resources (e.g., data, programs, equipment, and facilities), thereby protecting them from unauthorized disclosure, modification, and loss. Specific access controls include boundary protection, identification and authentication of users, authorization restrictions, cryptography, and audit and monitoring procedures. Without adequate access controls, unauthorized users, including intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or for personal gain. In addition, authorized users could intentionally or unintentionally modify or delete data or execute changes that are outside of their authority.

Although FAA had issued security policies, it did not consistently protect its network boundary from possible intrusions; identify and authenticate users; authorize access to resources; ensure that sensitive data are encrypted; or audit and monitor actions taken on NAS systems and networks.

Although Control Mechanisms Were Put in Place, FAA Did Not Always Adequately Protect the Boundary of NAS Systems

Boundary protection controls are used to restrict connections into and out of networks and to control connections between network-connected devices. Implementing multiple layers of security to protect an information system's internal and external boundaries can reduce the risk of a successful cyber attack. For example, multiple firewalls can be deployed to prevent both outsiders and insiders from gaining unauthorized access to systems. NIST Special Publication 800-53[17] recommends organizations monitor and control communications both at the external boundary of the system and at key internal boundaries within the system. NIST also recommends information systems connect to external networks or systems only through managed interfaces such as gateways, routers, or firewalls. FAA policy states that connections between NAS systems/networks and any non-NAS network or non-NAS information systems must occur through the NAS Enterprise Security Gateway.

While FAA implemented numerous controls to separate NAS systems from non-NAS systems, it did not always sufficiently protect connections between external partners and NAS operational systems or limit interconnectivity between operational and mission support environments. The excessive interconnectivity between NAS and non-NAS environments increased the risk that FAA's mission-critical air traffic control systems could be compromised.

FAA Did Not Consistently Implement Controls for Identifying and Authenticating Users of NAS Systems

Information systems need to be managed to effectively control user accounts and identify and authenticate users. Users and devices should be appropriately identified and authenticated through the implementation of adequate logical access controls. Users can be authenticated using mechanisms such as a password and user ID combination. NIST SP 800-53 recommends, and FAA policy requires, strong password controls for authentication, such as passwords that are at least eight alphanumeric characters in length, contain at least one upper- and one lower-case

[17]NIST, SP 800-53.

letter, contain numbers and special characters, and expire after a predetermined period of time.[18]

However, FAA did not consistently implement identification and authentication controls in accordance with its security policies and NIST guidance. For example, certain servers and applications supporting NAS systems did not implement sufficiently strong password controls. As a result, FAA is at increased risk that accounts could be compromised and used by unauthorized individuals to access sensitive information or systems.

FAA Did Not Always Ensure Users Were Properly Authorized to Access NAS Systems

Authorization encompasses access privileges granted to a user, program, or process. It is used to allow or prevent actions by that user based on predefined rules. Authorization includes the principles of legitimate use and least privilege.[19] NIST guidance recommends that organizations implement controls to ensure that only authorized users can access the system. This includes, but is not limited to, uniquely identifying all users, periodically reviewing access to the system, disabling accounts that no longer need access to the system, and assigning the lowest level of permission necessary for a task. NIST also recommends that systems and devices be configured so that only the functionality necessary to support organizational operations is enabled in order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized network connectivity.

FAA did not always ensure that users' access to key air traffic control systems was authorized in accordance with FAA policies and NIST guidance. In several cases, FAA and its contractors did not properly document that system users were authorized to access NAS systems. Additionally, FAA did not always ensure that periodic reviews of user access to NAS systems were performed in accordance with FAA policies and NIST guidance. As a result, users of these air traffic control systems may have greater access than they need to fulfill their responsibilities,

[18]FAA policy permits passwords of 13 or more random, non-sequential characters to never expire, and requires them to be changed only in the event they are compromised. The policy states this is permitted based on research suggesting the time required to crack such a password makes such an attack impractical.

[19]Users should have the least amount of privileges (access to services) necessary to perform their duties.

increasing the risk that these systems could be compromised, either inadvertently or deliberately.

Sensitive Data Were Not Always Sufficiently Encrypted

Cryptographic controls can be used to help protect the integrity and confidentiality of data and computer programs by rendering data unintelligible to unauthorized users and/or protecting the integrity of transmitted or stored data. Cryptography involves the use of mathematical functions called algorithms and strings of seemingly random bits called keys to (1) encrypt a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential; (2) provide an electronic signature that can be used to determine if any changes have been made to the related file, thus ensuring the file's integrity; and (3) link a message or document to a specific individual's or group's key, thus ensuring that the "signer" of the file can be identified. NIST guidance states that the use of encryption by organizations can reduce the probability of unauthorized disclosure of information. NIST Special Publication 800-53 recommends that organizations employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission, encrypt passwords while being stored and transmitted, and establish a trusted communications path between users and security functions of information systems. Additionally, when federal agencies employ cryptography, NIST standards require them to use Federal Information Processing Standard (FIPS) 140-2-validated algorithms.

FAA did not always ensure that sensitive data were encrypted when transmitted or stored, as called for by its policies and NIST guidance. For example, certain network devices supporting NAS systems did not always encrypt authentication data when transmitting them across the network, and other systems did not always encrypt stored passwords using sufficiently strong encryption algorithms in compliance with FIPS 140-2. Due to these weaknesses, FAA faces an increased risk that attackers could compromise accounts or intercept, view, and modify transmitted data, thereby threatening the confidentiality, integrity, and availability of the NAS.

FAA Did Not Consistently Implement Sufficient Audit and Monitoring Controls

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation of and response to suspicious activities. Audit and monitoring controls can help security

professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network- and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. Network-based intrusion detection systems capture or "sniff" and analyze network traffic in various parts of a network. FISMA requires that each federal agency implement an information security program that includes procedures for detecting, reporting, and responding to security incidents.

FAA did not consistently implement sufficient audit and monitoring controls. For example, FAA did not always have sufficient capability to monitor network traffic or ensure that NAS systems were sufficiently logging security-relevant events. As a result of these weaknesses, FAA faces an increased risk that it will be unable to detect and respond to unauthorized or malicious activities on its systems.

While Background Investigations Were Conducted in Accordance with Policy, Changes to Network Systems and Software Were Not Always Properly Controlled

In addition to access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an agency's information. These controls include policies, procedures, and techniques for implementing personnel security and securely configuring information systems. While FAA conducted background investigations in accordance with its policy, weaknesses in its configuration management processes increase the risk of unauthorized use, disclosure, modification, or loss of sensitive information and information systems supporting FAA's mission.

FAA Conducted Background Investigations in Accordance with Policy

Policies related to personnel actions, such as hiring, termination, and maintaining employee expertise, are important considerations in securing information systems. If personnel policies are not adequate, an entity runs the risk of (1) hiring unqualified or untrustworthy individuals; (2) providing terminated employees opportunities to sabotage or otherwise impair entity operations or assets; (3) failing to detect continuing unauthorized employee actions; (4) lowering employee morale, which may in turn diminish employee compliance with controls; and (5) allowing staff expertise to decline. Hiring procedures should include contacting references, performing background investigations, and ensuring that periodic reinvestigations are consistent with the sensitivity of the position, in accordance with criteria from the Office of Personnel Management. FAA policy requires positions to be designated by sensitivity and risk level, and describes requirements for conducting background investigations for employees and contractors, including periodic reinvestigations of individuals in positions of higher risk or sensitivity.

FAA ensured that the employees and contractors we sampled on the TFM-I, ERAM, SBSS, and FTI programs had appropriate background investigations. Specifically, all of the employees and contractors we sampled had up-to-date background investigations that were consistent with the risk designation of their positions. As a result, FAA reduced its risk that it has employed or contracted for unqualified or untrustworthy individuals on these programs.

FAA Did Not Always Properly Control Changes to Network Devices or Ensure Key Systems Were Fully Patched

Configuration management is an important control that involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. Configuration management involves, among other things, (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) obtaining reasonable assurance that systems are configured and operating securely and as intended. In addition, establishing controls over the modification of information system components and related documentation helps to prevent unauthorized changes and ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure that all hardware, software, and firmware programs and program modifications have been properly authorized, tested, and approved. Patch management, a component of configuration management, is important for mitigating the risks associated with software vulnerabilities. When a software vulnerability is discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. Without the patch, an attacker can exploit the vulnerability to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other systems. Outdated and unsupported software is more vulnerable to attack and exploitation because vendors may no longer provide updates, including security updates.

According to NIST SP 800-53, configuration management activities should include documenting approved configuration-controlled changes to information systems, retaining and reviewing records of the changes, auditing those records, and coordinating and providing oversight for configuration change control activities through a mechanism such as a

change control board. Additionally, NIST Special Publication 800-128[20] states that patch management procedures should define how the organization's patch management process is integrated into configuration management processes, how patches are prioritized and approved through the configuration change control process, and how patches are tested for their impact on existing secure configurations. FAA policy describes detailed requirements for controlling changes to NAS systems.

FAA did not always ensure that changes to network devices supporting air traffic control systems were managed in accordance with FAA policies for configuration change control. Specifically, significant changes were made to a key network device on one NAS system without following the system's defined change control process, which requires that changes be documented, analyzed for potential security impacts, tested, and approved before being implemented. Without adequately controlling configuration changes to network devices, an increased risk exists that changes could be unnecessary, may not work as intended, or may result in unintentional side effects that could impact mission-critical operations.

Additionally, the agency did not always ensure that security patches were applied in a timely manner to servers and network devices supporting air traffic control systems, or that servers were using software that was up-to-date. For example, certain systems were missing patches dating back more than 3 years. Additionally, certain key servers had reached end-of-life and were no longer supported by the vendor. As a result, FAA is at an increased risk that unpatched vulnerabilities could allow its information and information systems to be compromised.

FAA Did Not Fully Implement Its Information Security Program, Limiting the Effectiveness of Information Security Controls

An entity-wide information security program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. FISMA requires each agency to develop,

[20]NIST, *Guide for Security-Focused Configuration Management of Information Systems,* SP 800-128 (Gaithersburg, Md.: August 2011).

document, and implement an information security program that, among other things, includes

- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, or practices;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

To its credit, FAA has taken steps to implement an information security program and manage information security risks for its air traffic control systems. FAA produced system security plans for the systems we reviewed which specified the systems' operational contexts, relationships with others systems, general security requirements, and security controls. Additionally, FAA policy requires the periodic testing and evaluation of the controls on agency systems, and the agency has a process for planning, implementing, evaluating and documenting remedial actions to address deficiencies in those controls. FAA also documented a risk assessment policy and conducted risk assessments on the major systems we reviewed. However, FAA did not always consistently document incident response policies, ensure that contractors took required training, adequately test security controls, mitigate security weaknesses in a timely manner, ensure that incident response capabilities for NAS systems were adequate, or fully document and test contingency plans for its air traffic control systems.

Policies and Procedures Were Not Always Complete

A key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern the security over an agency's computing environment. Regarding incident response activities, NIST Special Publication 800-53[21] recommends agencies create an incident response policy and procedures to facilitate the implementation of the policy and associated incident response controls.

Although FAA had developed and documented many information security policies and procedures, incident response policies and procedures were not always complete or approved. For example, although the NCO security group operates as the focal point for NAS incident response activities, ATO's incident response policy establishing NCO as the incident response focal point was still in draft at the time of our review.[22] Additionally, although system-level incident response policies had been finalized for four of the NAS systems we reviewed, they did not always specify incident reporting timeframes or the need for all incidents to be reported. Without finalized and harmonized incident response policies, FAA faces an increased risk that incident response authorities and responsibilities will not be clearly understood by all stakeholders, impeding the agency's ability to efficiently and effectively respond to incidents or to do so in a timely manner.

Users with Significant Security Responsibilities Had Not Always Received Required Security Training

According to FISMA, an agency-wide information security program must include security awareness training for agency personnel, contractors, and other users of information systems that support the agency's operations and assets. This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA also includes requirements for training personnel who have significant responsibilities for information security. Additionally, NIST Special Publication 800-53 recommends that agencies provide incident response training to information system users consistent with their assigned roles and responsibilities.

Further, FAA policy states that all agency personnel and contractors must complete the agency's annual security awareness training, and that

[21]NIST, SP 800-53.

[22]FAA officials were unable to tell us when the policy would be finalized.

individuals with significant information system security responsibilities must receive role-based training specific to their responsibilities. For both security awareness and role-based training, FAA policy also states that records must be kept documenting the name and title of the individual receiving training, their security responsibilities, the type of training received, and the training date.

However, FAA did not always ensure that its employees and contractors took required information security training, including specialized security training and system-specific training, in a timely manner. For example:

- FAA contractors supporting certain NAS systems did not take the required security awareness training.
- Additionally, FAA did not provide periodic refresher security training to individuals with significant security responsibilities on two NAS systems. Although FAA stated that the Department of Transportation security awareness training, combined with on-the-job training, was sufficient, the Department of Transportation training does not cover security topics specific to these systems, and FAA did not define required content for on-the-job training or keep training records, as required by FAA policy.
- FAA had also not sufficiently documented that persons with incident response roles and responsibilities for one of the NAS systems we reviewed had taken required training, and did not provide formal incident response training for personnel on another NAS system.

Without adequately ensuring that personnel take required security training, FAA faces an increased risk that employees may not recognize and respond appropriately to potential security threats and vulnerabilities. Further, without sufficiently documenting that incident responders have taken required training, FAA faces an increased risk that employees will not receive training on performing their roles and responsibilities on a regular basis.

Security Controls Were Not Always Tested Sufficiently

FAA policy, in accordance with NIST guidance, states that security control assessments are to determine the extent to which controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements of the system. NIST Special Publication 800-53A[23] notes that while a high-level

[23]NIST, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, SP 800-53A, Revision 1 (Gaithersburg, Md.: June 2010).

examination of a limited body of evidence can support an assessor's determination that a control is implemented and free of obvious errors, determining whether a control is implemented correctly and operating as intended requires an in-depth analysis of a substantial body of relevant evidence.

While FAA prepared assessments of the security controls for the NAS systems we reviewed, its control assessments were not always comprehensive enough to identify weaknesses that we found in user account management, configuration management, and security awareness training controls. For example, FAA concluded that the account review control for one system was implemented based on examining the system security plan and interviewing officials, but the testers did not examine artifacts such as audit reports to determine if reviews were being conducted as described in the security plan. FAA also concluded that configuration change control had been implemented for another system after examining the system security plan and interviewing personnel; however, artifacts such as change tickets and approval documents were not examined to determine if system changes were controlled in accordance with procedures. Further, FAA's test results indicated that the security awareness training common control was defined, but the testers did not examine training records to verify that personnel on the systems that rely on the control were taking the training as required. ATO officials stated that control assessments were often supported by additional documentation not described in the security control assessment reports; however, the agency was unable to provide evidence to corroborate this statement.

By not conducting more comprehensive tests of security controls, FAA has decreased assurance that controls are implemented correctly and operating as intended. Additionally, because security control assessments are used by agencies to evaluate whether contractors are implementing information security controls effectively, FAA had reduced assurance that its contractors were adequately securing and protecting air traffic control systems.

Identified Security Weaknesses Were Not Always Addressed in a Timely Fashion

FISMA requires that agency-wide information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency. Agencies must establish procedures to reasonably ensure that all information security control weaknesses, regardless of how or by whom they are identified, are addressed through the agency's remediation processes. For each

identified control weakness, the agency is required to develop and implement a plan of actions and milestones (POA&M) based on findings from security control assessments, security impact analyses, continuous monitoring of activities, audit reports, and other sources. When considering appropriate corrective actions to be taken, the agency should, to the extent possible, consider the potential agency-wide implications and design appropriate corrective actions to systemically address the deficiency.

While FAA established POA&Ms for addressing identified security control weaknesses, it did not always complete remedial actions in accordance with established deadlines. For example, of the 147 POA&Ms we reviewed on 4 NAS systems, 58 were not completed by their planned completion dates, and the planned completion dates for 50 had been extended from between 8 months to more than 3 years past the dates that they were originally scheduled to be completed. According to ATO officials, one reason that original deadlines are often missed is that the programs lack sufficient resources and funding to address weaknesses by their original due dates. Without resolving identified vulnerabilities in a timely manner, FAA faces an increased risk, as continuing opportunities exist for unauthorized individuals to exploit these weaknesses and gain access to sensitive information and systems.

NAS Incident Detection and Response Activities Were Limited

Comprehensive monitoring and incident response controls are necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. While strong controls may not prevent all incidents, agencies can reduce the risks associated with these events by detecting and promptly responding before significant damage is done. NIST Special Publication 800-53 recommends that agencies test incident response capabilities for effectiveness. NIST guidance also notes that the ability to identify incidents using appropriate audit and monitoring techniques enables an agency to initiate its incident response plan in a timely manner. Further, NIST guidance also recommends that once an incident has been identified, an agency's incident response processes and procedures should provide the capability to correctly log the incident, properly analyze it, and take appropriate action. NIST guidance also recommends that agencies test their information technology plans, including incident response plans, and document the test results in an after action report. FAA's ATO assigned responsibility for incident handling on NAS systems to NCO, although NAS system owners and operators also have a responsibility to coordinate with NCO in responding to incidents affecting their systems.

FAA has notable shortcomings in security monitoring and incident detection over air traffic control systems. For example:

- NCO does not have sufficient access to effectively monitor the NAS operational environment. For example, there was no full network packet capture and anomaly detection capability for network traffic at major network interface points at FAA operational facilities. Additionally, network traffic flow session data was not integrated into the ad-hoc query systems used by the NCO. Further, NCO lacked access to data from sensors on key network gateways, including intrusion detection, network packet capture, and network flow data, and so cannot adequately monitor the gateways for security-relevant events.
- Although NCO has been given responsibility for incident response for the NAS environment, 26 of the 35 IP-connected NAS systems did not provide security event logs to NCO, including 3 of the systems we reviewed, severely limiting the ability of NCO to effectively monitor the NAS environment.
- The NCO database system containing centralized security logs collected from various NAS systems was ineffective due to weaknesses in its searching function. Specifically, the system could not search past any gaps in the log data. To compensate, NCO personnel would manually parse the data from multiple queries together, but there was not sufficient assurance that all data needed for incident investigations had been retrieved.
- NCO did not have a formal process in place to review and document the potential impact to NAS operations from significant incidents identified internally or by FAA's Cyber Security Management Center. Specifically, NCO did not formally assess the potential risks to the NAS for any of the incidents we reviewed.
- Testing of the NAS incident response capability has been limited. Specifically, while one system had conducted and documented tests of its incident response capability, NCO has not developed after-action reports for all phases of its incident response capability tests, and officials with three systems all indicated they do not test their incident response capabilities.

As a result, there is an increased risk that FAA will not be able to adequately detect, contain, eradicate, or recover from incidents affecting air traffic control systems.

Contingency Plans Were Not Always Complete or Adequately Tested

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If contingency planning controls are inadequate,

even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. NIST Special Publication 800-34[24] recommends that contingency plans include procedures for diagnosing and addressing problems, notifying recovery personnel when the plan needs to be activated, and procedures to be followed in the event that specific personnel cannot be contacted. NIST also recommends that contingency plans include procedures for notifying users when a system has been reconstituted and normal operations have resumed. Additionally, NIST Special Publication 800-53 notes that contingency plans should be tested to determine the plan's effectiveness and the organization's readiness to execute the plan.

FAA did not always ensure that contingency plans for air traffic control systems were complete or that tests of the plans were adequate. Although FAA documented contingency plans for three systems, it did not always include important information in these plans. For example, the contingency plans for two systems did not sufficiently document the means by which key personnel were to be contacted in the event of a disaster or define procedures to follow in the event that specific personnel could not be contacted. Although separate notification procedures were developed for one of the systems, they were not included in the contingency plan either explicitly or by reference. Also, although procedures had been established for notifying users when two of the systems had been reconstituted and normal operations had resumed, the contingency plans for those systems did not include or reference the procedures. Further, the contingency plan for another system did not contain the actual assessment and recovery procedures for the system. Also, FAA tested the contingency plans for three NAS systems, but the tests did not always address key elements of the plans, including notification procedures, recovering the system on an alternate platform, and system performance on alternate equipment.

Without including important information in its contingency plans for air traffic control systems or sufficiently testing its contingency plans, FAA is at an increased risk of employees or contractors not following the correct procedures to appropriately recover systems in a timely manner from service disruptions.

[24]NIST, SP 800-34.

Inadequate Agency-Wide Information Security Risk Management Processes Contribute to Weaknesses in Security Controls and Security Management

One important reason for many of the weaknesses in security controls as well as the security program shortcomings identified in our review is that FAA has not yet fully established an integrated, organization-wide approach to managing information security risk. According to NIST, effective risk management requires organizations such as the FAA to operate in highly complex, interconnected environments using state-of-the-art and legacy information systems—systems that organizations depend on to accomplish their missions and to conduct important business-related functions. The complex relationships among missions, mission/business processes, and the information systems supporting those missions and processes require an integrated, organization-wide view for managing risk. Effective management of information security risk is also critical to the success of organizations in achieving their strategic goals and objectives.

FISMA requires the head of each federal agency to ensure that information security management processes are integrated with agency strategic and operational planning processes. NIST SP 800-39 provides agencies with guidance for developing and implementing an integrated, organization-wide program for managing information security risk to agency operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems. It describes an integrated approach for addressing information security risk at the organization level, the mission/business process level, and the information system level. NIST SP 800-39 states that, in managing information security risk at the organizational level, agencies should establish and implement information security governance, a risk executive function, and risk management strategy in order to ensure that risk management decisions are aligned strategically with the agency's missions and business functions consistent with the organizational goals and objectives. The publication also states that an organization's mission/business processes should be designed to manage risk in accordance with the organizational information security risk management strategy.

Further, NIST SP 800-100 notes that agencies should have a strategic plan for information security, which identifies goals and objectives related to the agency's mission, specifies a plan for achieving those goals, and establishes short- and mid-term performance targets and measures that allow the agency to track manage and monitor its progress towards those goals and objectives. Also, in February 2014, NIST established its *Framework for Improving Critical Infrastructure Cybersecurity*, which

presents a set of industry standards and best practices to help organizations manage cybersecurity risks to critical infrastructure systems, and contains a methodology for organizations to evaluate and strengthen information security programs for critical infrastructure.

While it has taken initial steps, the FAA has not yet implemented an effective, organization-wide program for managing information security risk to its mission and operations. Specifically, the FAA Chief Information Security Officer stated that in November 2013, the agency established a risk executive function at the agency level in the form of a Cyber Security Steering Committee. The committee includes representatives from across FAA, including ATO, NextGen, and FAA's office of security. However, FAA has not yet fully established the governance structures and practices necessary for ensuring that its information security risk management decisions are aligned strategically with its mission. Specifically:

FAA has not clearly and consistently established roles and responsibilities for information security for NAS systems. FISMA requires the head of an agency to (1) ensure that senior agency officials provide security for information and information systems that support operations and assets under their control, and (2) delegate to the agency CIO the authority to ensure compliance with FISMA requirements. Further, according to NIST Special Publication 800-39, one of the tasks of the risk executive is to establish risk management roles and responsibilities. However, existing FAA practices, policies, and documentation are inconsistent in establishing responsibility for NAS information security. While FAA's security management program policy states that primary responsibility for NAS information security rests with the CIO, ATO officials stated that primary responsibility for NAS information security lies with ATO rather than the CIO. FAA's portion of the President's Fiscal Year 2014 Budget Submission states only that the CIO is responsible for non-NAS systems. The steering committee has defined updated roles and responsibilities for information security, which state that executive-level responsibility for the organization-wide information security program lies with the CIO. However, these roles and responsibilities have not yet been implemented. Additionally, AIT officials and ATO officials disagreed about whether the roles and responsibilities had been approved.

Better defining roles and responsibilities is important because FAA officials in AIT and ATO expressed diverging opinions about how information security controls should be implemented in the NAS environment. For example, AIT officials stated that ATO and AIT should

collaborate to identify and reduce duplicative incident response activities between NCO and FAA's existing Cyber Security Management Center, but ATO officials stated that the NCO capability should remain separate from the Cyber Security Management Center because of the unique security requirements of the NAS critical infrastructure.

FAA does not have a strategic plan for information security that is up to date and reflects current conditions. FAA's Information Systems Security Program Policy requires a multiyear information security strategic plan to be developed, maintained, and updated annually. Additionally, NIST SP 800-100 states that agencies should revisit the information security strategic plan when a major change in the agency information security environment occurs. However, the FAA information security strategic plan has not been updated since 2010. Significant changes in the NAS environment, such as the increased reliance on IP networks, increased connectivity between systems, the introduction of NextGen systems, and the designation of the NAS as part of the nation's critical infrastructure, have changed the level and nature of the information security risks facing air traffic control systems. The evolution of connectivity for NAS systems substantially increases risks of Internet-based intrusions and disruptions. AIT officials told us that the Cyber Security Steering Committee plans to revise the information security strategic plan during fiscal year 2015.

Because FAA lacks an up-to-date information security strategic plan, the ATO organization does not have a clear set of goals, objectives, and performance measures around which it can organize its information security program. Responsibility for NAS information security in ATO is distributed across different entities and programs, and ATO officials stated that variation in emphasis on security goals and priorities across the organization makes it challenging to manage information security activities in the NAS environment. For example, according to ATO officials, the NAS incident response organization, NCO, has limited capabilities and available staff because it is required to obtain funding from other program units within ATO, which have different priorities. Additionally, ATO officials stated that remedial actions are often delayed because the program units do not hold system owners accountable for addressing information security weaknesses in a timely manner.

In the absence of clearly defined roles and responsibilities or an updated strategic plan, ATO has begun moving forward with strategic planning activities separately from the steering committee's risk management responsibilities. During our review, ATO evaluated its information security

processes and capabilities against the guidance in the *NIST Framework for Improving Critical Infrastructure Cybersecurity*, with plans to use the results of the evaluation to develop an information security strategic plan for ATO. However, other organizations represented on the steering committee are not involved in this process. Although ATO officials told us that they plan to inform the members of the committee about the results of the review, it is not clear whether the committee intends to use the results in its efforts, or whether ATO's planned information security strategic plan will reflect the priorities of FAA as a whole.

Until it fully establishes an integrated, organization-wide approach to managing information security risk and ensures that federal guidance for securing critical infrastructure is incorporated into its risk management processes, FAA is likely to continue to face challenges in ensuring that risk management decisions are aligned strategically with the its mission and effectively implementing information security controls for air traffic control systems. As a result, the weaknesses we identified are likely to persist.

Conclusions

A large, complex, interconnected system like the NAS inherently faces many security risks. Although FAA took many steps to address these risks, weaknesses remain that challenge the FAA in fulfilling its mission of ensuring the safety and efficiency of the nation's airspace operations. Many weaknesses in access controls and configuration management pose risks to the security of the NAS. The effect of these weaknesses is increased by the significant interconnectivity that exists between the FTI NAS operational environment and the FTI mission support network. Additionally, significant shortcomings limit NCO's ability to detect and respond to security incidents across NAS systems. These weak controls are mirrored in weak security management processes, such as incomplete policies and procedures for incident response and insufficient testing of security controls. Additionally, actions to mitigate identified security weaknesses are often delayed—sometimes for years. All of these weaknesses combine to pose increased risks to the confidentiality, integrity, and availability of NAS systems and thus put the safe and uninterrupted operation of the nation's air traffic control system at risk.

A fundamental cause for these various weaknesses is that FAA has not yet implemented an effective program for managing organizational information security risk to its mission. Although FAA established a cyber security steering committee, roles and responsibilities remain unclear, and AIT and ATO officials continue to disagree on who should be

responsible for the security of NAS systems. Likewise, an out-of-date information security strategic plan contributes to the lack of an adequate risk-based structure to guide implementation of security controls. Further, due in part to the lack of an up-to-date strategic plan for the agency, ATO lacks a clear set of goals, objectives, and performance measures around which it can organize its information security program for NAS systems, making it challenging to manage information security activities such as ensuring that controls are effectively implemented and that system owners address identified security weaknesses in a timely manner.

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

Recommendations for Executive Action

To fully implement its information security program and ensure that unnecessary risks to the security of NAS systems are mitigated, we recommend that the Secretary of Transportation direct the Administrator of FAA to implement the following 14 recommendations:

- Finalize the incident response policy for ATO and ensure that NAS system-level incident response policies specify incident reporting timeframes and the need for all incidents to be reported in accordance with FAA guidance.
- Establish a mechanism to ensure that all contractor staff complete annual security awareness training as required by federal law and FAA policy.
- Establish a mechanism to ensure that all staff with significant security responsibilities receive appropriate role-based training.
- Establish a mechanism to ensure that personnel with incident response roles and responsibilities take appropriate training, and that training records are retained.
- Take steps to ensure that testing of security controls is comprehensive enough to determine whether security controls are in place and operating effectively, by, for example, examining artifacts such as audit reports, change tickets, and approval documents.
- Take steps to ensure that identified corrective actions for security weaknesses are implemented within prescribed timeframes.

- Provide NCO with full network packet capture capability for analyzing network traffic and detecting anomalies at major network interface points at FAA operational facilities.
- Integrate network traffic flow data into NCO's ad-hoc query systems.
- Provide NCO with access to network sensors on key network gateways for reviewing intrusion detection, network traffic, and network session data.
- Provide NCO with security event log data for all IP-connected NAS systems.
- Address identified weaknesses in the search function of the NCO database event query system to eliminate the need for manual workarounds and ensure that all data relevant for security investigations can be retrieved.
- Develop a formal process for NCO to assess significant identified incidents for potential impact to NAS operations.
- Ensure that NAS incident response capabilities are adequately tested, and that test results are sufficiently documented.
- Ensure that contingency plans for NAS systems are sufficiently documented, and that tests of contingency plans address key elements of the contingency plans, including notification procedures, recovering the system on an alternate platform, and system performance on alternate equipment.

Further, to establish an integrated organization-wide approach to managing information security risk and to ensure that risk management decisions are aligned strategically with the FAA's mission, we recommend that the Secretary of Transportation direct the Administrator of FAA to take the following three actions:

- Clearly define organizational responsibilities for information security for NAS systems, and ensure that all relevant organizations, including AIT and ATO, are in agreement with them.
- Update the FAA information security strategic plan to reflect current conditions, including the increased reliance on IP networking and the designation of the NAS as one of the nation's critical infrastructures.
- Create an agency-wide commitment to strategic planning for information security by ensuring that planning activities are coordinated with all relevant organizations represented on the Cyber Security Steering Committee.

We are also making 168 recommendations to address 60 findings in a separate report with limited distribution. These recommendations consist of actions to implement and correct specific information security weaknesses related to access controls and configuration management.

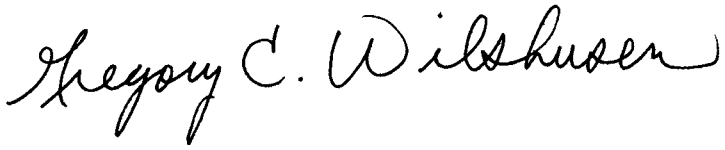
Agency Comments and Our Evaluation

In written comments (reprinted in appendix II) on a draft of this report, the Department of Transportation stated that FAA concurred with our recommendations. The department also stated that FAA recognizes the need to secure the NAS environment as part of the nation's critical infrastructure, and that FAA has taken several steps to improve NAS information security. Additionally, the department stated that FAA recognizes that mission assurance requires the integration of all agency cyber capabilities to support operations and is continuing its efforts to establish an integrated organization-wide approach to managing information security risk. We agree that these actions are important steps for FAA to take, and we also believe that addressing our recommendations will result in valuable improvements in information security over air traffic control systems.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to appropriate congressional committees, the Secretary of Transportation, and other interested parties. In addition, this report will be available at no charge on the GAO website at http://www.gao.gov.

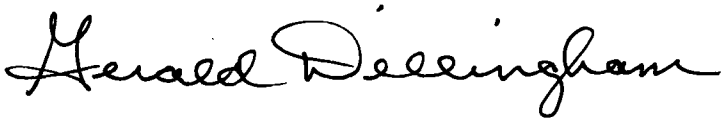
Should you or your staffs have questions on matters discussed in this report, please contact Gregory C. Wilshusen at (202) 512-6244, Dr. Nabajyoti Barkakati, Ph.D., at (202) 512-4499, or Gerald L. Dillingham, Ph.D., at (202) 512-2834. We can also be reached by e-mail at wilshuseng@gao.gov, barkakatin@gao.gov and dillinghamg@gao.gov.

GAO staff who made major contributions to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues

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



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

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 Representatives

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
Chairman
Subcommittee on Transportation Security
Committee on Homeland Security
House of Representatives

Appendix I: Objective, Scope, and Methodology

The objective of our review was to evaluate the extent to which the Federal Aviation Administration (FAA) has effectively implemented appropriate information security controls to protect the confidentiality, integrity, and availability of its existing air traffic control (ATC) systems.

To determine the effectiveness of the FAA's security controls, we gained an understanding of the overall National Airspace System (NAS) control environment and examined controls for the agency's systems and facilities. Specifically, we reviewed controls over the network infrastructure and systems that support the FAA's mission to provide the safest, most efficient aerospace system in the world. We performed our work at FAA headquarters in Washington, D.C. and other locations supporting key systems, specifically: the Air Traffic Control System Command Center in Warrenton, Virginia; the FAA's William J. Hughes Technical Center in Egg Harbor Township, New Jersey; and at contractor facilities in Herndon, Virginia; Egg Harbor Township, New Jersey; and Melbourne, Florida.

To select the information systems for our audit, we evaluated each NAS information system based on several factors, including its relative importance in supporting FAA's mission, expected lifetime, and how widely it is used. Further, we selected only systems that use Internet Protocol (IP)-based communications. Based on this evaluation, we selected a non-generalizable sample of five systems[1] for review: FAA Telecommunications Infrastructure (FTI), Surveillance and Broadcast Service System (SBSS), Traffic Flow Management-Infrastructure (TFM-I), En Route Automation Modernization (ERAM), and En Route Communications Gateway (ECG).

To evaluate FAA's controls over its ATC systems, we used our *Federal Information System Controls Audit Manual*,[2] which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; National Institute of Standards and Technology (NIST) standards and guidelines; FAA policies

[1]Because we examined only 5 of the more than 100 air traffic control systems in the NAS, the results of our review of system-level controls cannot be generalized to the entire NAS environment.

[2]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

and procedures; and standards and guidelines from relevant security and IT security organizations, such as the National Security Agency and the Center for Internet Security.

Specifically, we

- reviewed network access paths to determine if boundaries had been adequately protected;
- reviewed the complexity and expiration of password settings to determine if password management was being enforced;
- analyzed users' access authorizations for four systems to determine whether system access had been approved and properly documented;
- observed configurations for transmitting data across the network to determine whether sensitive data were being encrypted. For the ERAM and ECG systems, we reviewed configuration settings for network devices by reviewing the network device builds that are distributed to Air Route Traffic Control Centers (ARTCC) by the William J. Hughes Technical Center;
- reviewed system security settings to determine if sufficient audit and monitoring controls had been implemented;
- evaluated configuration change control processes for selected systems to determine whether changes were sufficiently documented, tested, and approved in accordance with system procedures; and
- inspected key network devices and servers to determine if critical patches had been installed and/or were up to date.

Additionally, our review of boundary protection controls focused on interconnections between NAS and non-NAS systems.

Using the requirements identified by the Federal Information Security Management Act of 2002, which establishes key elements for an effective agency-wide information security program, and associated NIST guidelines and agency requirements, we evaluated the FAA's information security program by

- analyzing processes and documentation that were part of FAA's information security risk management processes to determine the extent to which the process sufficiently supported the agency's mission and operations;
- examining system security plans to determine whether they described the security controls in place or planned for meeting the security requirements of the system;

- examining security awareness training records to determine whether employees and contractors had received training according to FAA policy and federal guidance;
- analyzing security testing and evaluation results for four systems to determine whether testing of management, operational, and technical controls was sufficient to conclude that controls were in place and operating effectively;
- examining remedial action plans for four systems to determine whether FAA addressed identified vulnerabilities in a timely manner;
- examining contingency plans and contingency test results for selected systems to determine whether those plans were appropriately documented and had been sufficiently tested; and
- reviewing FAA's processes for identifying and responding to information security incidents to determine whether FAA has implemented an effective incident response capability for its air traffic control systems.

As part of our review of the FAA's information security program, we reviewed several sources of computer-generated data. These included FAA's

- inventory of NAS information systems,
- IT security training completion data, and
- employee background investigation data.

To verify the reliability of these data, we examined them for obvious outliers, omissions, errors, and consulted with FAA officials to resolve any identified anomalies. We also interviewed knowledgeable officials regarding controls on the security training and employee background investigation data, including how and by whom it is input and used. We determined that these sources of data were sufficiently reliable for our purposes.

We conducted this performance audit from August 2013 to January 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

JAN 12 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) currently provides the safest, most efficient aerospace system in the world. The Agency is fully cognizant of the vital requirement to secure the National Airspace System (NAS) cyber environment as part of the nation's critical infrastructure. The FAA has achieved major milestones to improve NAS cybersecurity by:

- Creating the NAS Cyber Operations (NCO) to provide monitoring and response capabilities that are fully integrated with NAS operations and supported by other FAA cyber capabilities.
- Implementing a NAS Information Security Continuous Monitoring Plan to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
- Integrating with industry and other government agencies to promote cybersecurity situational awareness and cross-organizational synergy for threat information sharing.
- Publishing and updating critical infrastructure cybersecurity policies that take into account the unique availability requirements of the NAS and ensure compliance with government security mandates.
- Continuing efforts to strengthen boundary protection for critical infrastructure segregation to restrict access to the NAS Domain.
- Creating a Cybersecurity Steering Committee that is responsible for developing an Agency-wide comprehensive cyber risk management strategy and a cybersecurity governance structure that fuses organizational strategic goals and objectives.

The FAA's Air Traffic Organization has leveraged the National Institute of Standards and Technology (NIST) Cybersecurity Framework to identify, prioritize, and track continuous security improvements to meet current and future threats against the FAA's critical infrastructure. The FAA recognizes that mission assurance requires the integration of all Agency cyber capabilities to support operations and is continuing its efforts to establish an integrated organization-wide approach to managing information security risk.

The FAA has reviewed the draft report and offers the following comments:

- The NCO, in coordination with the Federal Telecommunication Infrastructure program, is maturing to provide greater technical capabilities for analyzing network traffic and NAS

system level event information. In support of the defense-in-depth strategy, the NCO provides the NAS cyber common operational picture for the Agency. The NCO is a mission multiplier to the overall Department of Transportation's strategic approach to cyber monitoring, detection, and incident response. The FAA is committed to the continued development of the NCO as a key component of operational resiliency and to the maturing of its capabilities to support a NAS Domain that continues to operate under a range of cyber conditions.

- A cyber workforce development plan is being coordinated to establish baseline technical and management skills and training to support the functional cybersecurity roles and responsibilities delineated in NIST documentation. The Agency is leveraging the Presidential National Initiative for Cybersecurity Education to increase cybersecurity awareness and competence across the Agency and to build an agile, highly-skilled cybersecurity workforce capable of responding to a dynamic and rapidly evolving array of threats.
- Within NIST Special Publication (SP) 800-82 Rev2 (May 2014), *Guide to Industrial Control System (ICS) Security*, the Air Traffic Control System is specifically identified as critical infrastructure that operates in an ICS environment. It further states that, "Although some characteristics are similar, ICS also have characteristics that differ from traditional information processing systems. Some of these characteristics include significant risk to the health and safety of human lives…" And that, "ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems." The FAA is using the defense-in-depth strategies defined in NIST SP 800-82 coupled with guidance contained in NIST SP 800-39, *Managing Information Security Risk*, to establish an integrated, organization-wide approach for managing risk and establishing appropriate governance structures to ensure that security risks and strategic planning are considered within the context of the Agency's mission.

After reviewing the draft report, the FAA concurs with the recommendations and will provide a detailed response to each recommendation after publication of the final report.

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

Keith Washington
Acting Assistant Secretary for Administration

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Nabajyoti Barkakati, Ph.D., (202) 512-4499, barkakatin@gao.gov

Gerald L. Dillingham, Ph.D., (202) 512-2834 or dillinghamg@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Gary Austin, Lon Chin, West Coile, John de Ferrari, Wilfred Holloway, Nick Marinos, and Chris Warweg (assistant directors); Sher'rie Bacon; Chris Businsky; William Cook; Saar Dagani; Jennifer Franks; Lee McCracken; John Ockay; Justin Palk; Krzysztof Pasternak; Monica Perez-Nelson; Eugene Stevens; Michael Stevens; and Adam Vodraska made key contributions to this report.