

August 2005

INFORMATION SECURITY

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



G A O

Accountability * Integrity * Reliability

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of [GAO-05-712](#), a report to congressional requesters

Why GAO Did This Study

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

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

What GAO Recommends

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

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

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

INFORMATION SECURITY

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

What GAO Found

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

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

Air Traffic Control System Command Center



Source: FAA.

Contents

Letter

Results in Brief	1
Background	3
Objective, Scope, and Methodology	9
Although Progress Has Been Made, Air Traffic Control Systems Remain Vulnerable	10
Conclusions	28
Recommendations for Executive Action	29
Agency Comments and Our Evaluation	30

Appendix

Appendix I: GAO Contact and Staff Acknowledgments	33
--	-----------

Figures

Figure 1: Thousands of Aircraft Operating in the National Airspace System	3
Figure 2: Air Traffic Control Tower	4
Figure 3: Air Traffic Control System Command Center	5
Figure 4: Summary of Air Traffic Control over the United States and Oceans	6
Figure 5: Percentage of Staffed Facilities That Have Been Accredited	16

Abbreviations

CIO	Chief Information Officer
DOT	Department of Transportation
FAA	Federal Aviation Administration
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management

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



United States Government Accountability Office
Washington, D.C. 20548

August 26, 2005

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

The Honorable Adam H. Putnam
House of Representatives

The Federal Aviation Administration (FAA) performs critical functions that contribute to ensuring safe, orderly, and efficient air travel in the national airspace system. It 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. Interruptions in FAA's ability to fulfill its missions could have a significant adverse impact on air traffic nationwide.

At your request, we evaluated the extent to which FAA has implemented information security controls for its air traffic control systems. Effective information security controls are essential for ensuring that information technology resources are adequately protected from inadvertent or deliberate misuse, fraudulent use, or destruction.

This report summarizes the results of our review of information security controls in the agency's air traffic control systems. We are also issuing a separate report for limited distribution that contains sensitive security information. It describes in more detail the information security weaknesses that we identified and our specific recommendations for correcting them.

Our review was performed from March 2004 through June 2005 in accordance with generally accepted government auditing standards.

Results in Brief

FAA has made progress in implementing information security for its air traffic control systems by establishing an agencywide information security program and addressing many of its previously identified security weaknesses; however, it still has significant weaknesses that threaten the integrity, confidentiality, and availability of its systems—including weaknesses in controls that are designed to prevent, limit, and detect access to those systems. For example, for the systems we reviewed, the

agency was not adequately managing its networks, system patches, user accounts and passwords, or user privileges, and it was not always logging and auditing security-relevant events. In addition, FAA faces risks to its air traffic control systems due to weaknesses in physical security, background investigations, segregation of duties, and application change controls. As a result, it is at increased risk of unauthorized system access, possibly disrupting aviation operations. While acknowledging these weaknesses, agency officials stated that because portions of their systems are custom built and use older equipment with special-purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited. Nevertheless, the proprietary features of these systems do not protect them from attack by disgruntled current or former employees, who understand these features, or from more sophisticated hackers.

A key reason for the information security weaknesses that we identified in FAA's air traffic control systems was that the agency had not yet fully implemented an information security program to ensure that effective controls were established and maintained. FAA has various initiatives under way to improve information security; however, key elements of a security program have not yet been fully implemented. For example, some of the agency's security plans were outdated; security awareness training requirements were not being fully met; system testing and evaluation programs were inadequate; security incident detection capabilities were limited; and shortcomings existed in providing service continuity for disruptions in operations. In response to weaknesses that we had identified, FAA officials told us they recognized that more work was needed to continue to improve their information security program and that they had already corrected many of their electronic access control weaknesses.

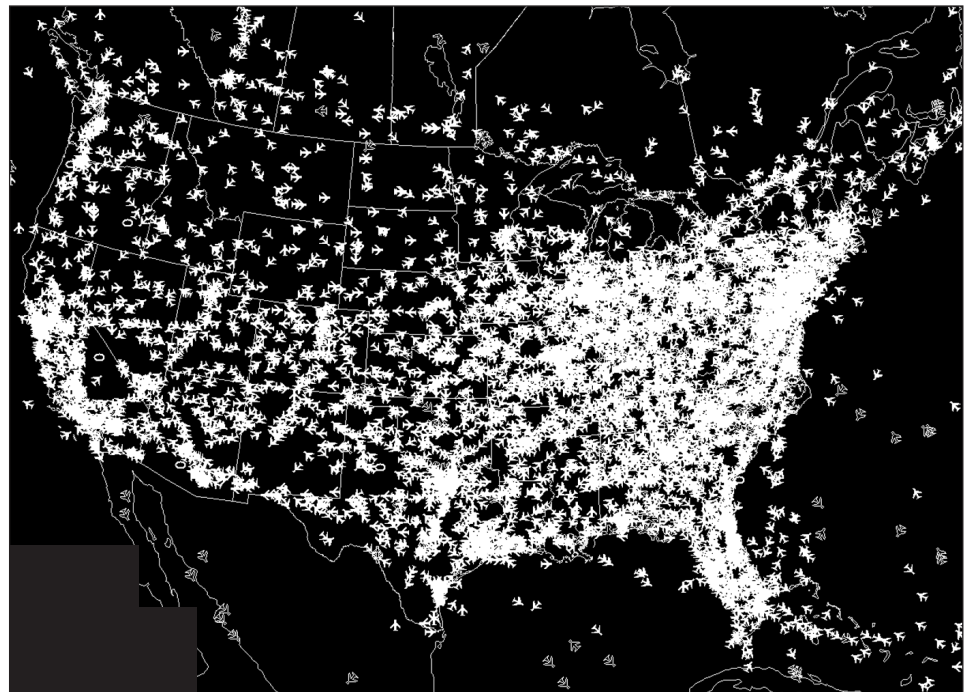
We are making recommendations to the Secretary of Transportation to direct the FAA administrator to fully implement an information security program. In a separate report, with limited distribution because it contains sensitive security information, we are making recommendations to correct the specific weaknesses we identified during our review.

In providing oral comments on a draft of this report, the FAA's Chief Information Officer (CIO) agreed to consider our recommendations and provided other specific comments, which we have incorporated, as appropriate, in the report.

Background

FAA is an agency of the Department of Transportation (DOT); one of its central missions is to ensure safe, orderly, and efficient air travel in the national airspace system. FAA's quarterly administrator's fact book for March 2005 reports that, in 2004, air traffic in the national airspace system exceeded 46 million flights and 647 million people. According to the agency's 2004 annual performance report for its air traffic organization, *Year One—Taking Flight*, at any one time as many as 7,000 aircraft—both civilian and military—could be aloft over the United States (see fig. 1). More than 36,000 employees support the operations that help move aircraft through the national airspace system.

Figure 1: Thousands of Aircraft Operating in the National Airspace System



Source: FAA.

The agency'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. These systems reside at, or are associated with, several types of facilities: air traffic control towers, Terminal Radar Approach Control facilities, Air Route Traffic

Control Centers (or en route centers), and the Air Traffic Control System Command Center. According to FAA,

- Four hundred eighty-eight air traffic control towers (see fig. 2) manage and control the airspace within about 5 miles of an airport. They control departures and landings as well as ground operations on airport taxiways and runways.

Figure 2: Air Traffic Control Tower



Source: FAA.

- One hundred seventy 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, where en route centers' control begins. Terminal controllers establish and maintain the sequence and separation of aircraft.
- Twenty-one en route centers control planes over the United States—in transit and during approaches to some airports. Each center handles a different region of airspace. En route centers operate the computer suite that processes radar surveillance and flight planning data, reformats it for presentation purposes, and sends it to display equipment that is used

by controllers to track aircraft. The centers control the switching of voice communications between aircraft and the center as well as between the center and other air traffic control facilities. Two en route centers also control air traffic over the oceans.

- The Air Traffic Control System Command Center (see fig. 3) 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.

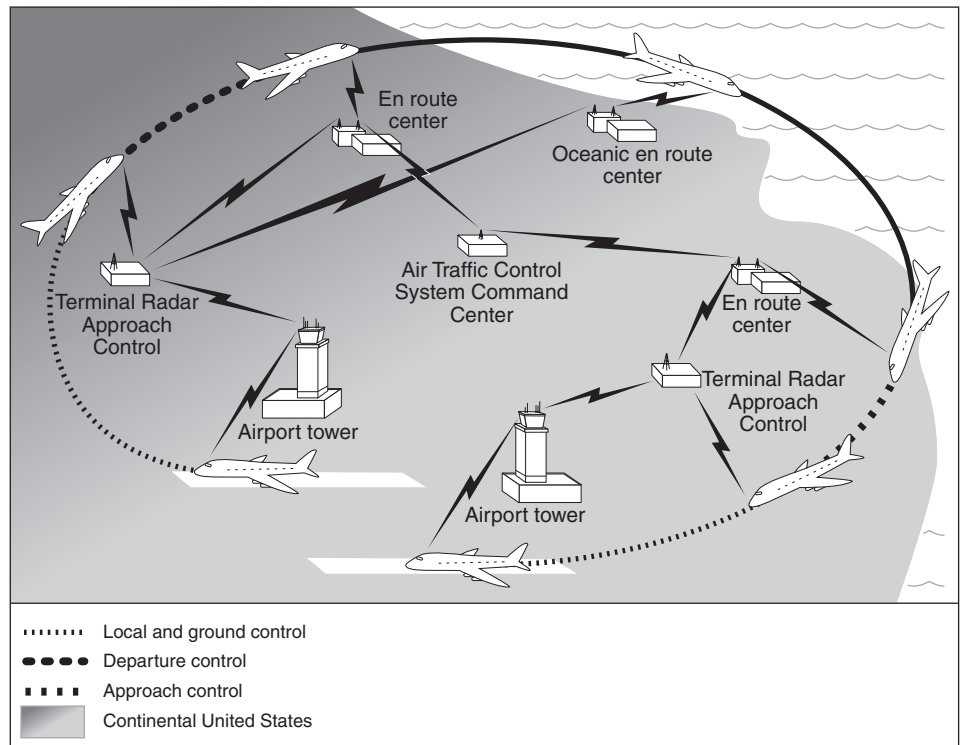
Figure 3: Air Traffic Control System Command Center



Source: FAA.

As aircraft move across the national airspace system, controllers manage their movements during each phase of flight. See figure 4 for a visual summary of air traffic control over the United States and its oceans.

Figure 4: Summary of Air Traffic Control over the United States and Oceans



Source: GAO.

The air traffic control systems are very complex and highly automated. These 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.

To support its operational management functions, the agency relies on several interconnected systems to process and track flights around the world. In order to successfully carry out air traffic control operations, it is essential that FAA’s systems interoperate, functioning both within and across facilities as one integrated system of systems. Each type of facility that we described in the previous section consists of numerous interrelated systems. For example, each of the en route centers, according to FAA officials, relies on 16 systems to perform mission-critical information processing and display, navigation, surveillance, communications, and

weather functions. In addition, systems from different facilities interact with each other so that together they can successfully execute the entire air traffic control process. For example, systems integrate data on aircraft position from surveillance radars with data on flight destination from flight planning data systems, for use on controllers' displays.

As FAA modernizes its air traffic control systems, information security will become even more critical. The agency's modernization efforts are designed to enhance the safety, capacity, and efficiency of the national airspace system through the acquisition of a vast network of radar, navigation, communications, and information processing systems.¹ Newer systems use digital computer networking and telecommunications technologies that can create new vulnerabilities and expose them to risks that must be assessed and mitigated to ensure adequate protection. New vulnerabilities may also result from FAA's increasing reliance on commercially available hardware and software and from growing interconnectivity among computer and communication systems. Increasing interconnection increases the extent to which systems become vulnerable to intruders, who may severely disrupt operations or manipulate sensitive information.

The administrator has designated the CIO as the focal point for information system security within the agency. The CIO is responsible for overseeing the development of the information security program, including oversight of information security policies, architectures, concepts of operation, procedures, processes, standards, training, and plans. This responsibility is delegated to the Office of Information Systems Security, whose mission is to protect the agency's infrastructure through leadership in innovative information assurance initiatives. In addition, the agency has established Information System Security Manager positions, with more detailed information security responsibilities, within FAA's various lines of business, such as the air traffic organization.

¹We have issued numerous reports and testimonies on FAA's modernization efforts. See, for example, GAO, *Federal Aviation Administration: Stronger Architecture Program Needed to Guide Systems Modernization Efforts*, [GAO-05-266](#) (Washington, D.C.: Apr. 29, 2005) and GAO, *Air Traffic Control: FAA's Modernization Efforts—Past, Present, and Future*, [GAO-04-227T](#) (Washington, D.C.: Oct. 30, 2003). Since 1995, we have designated the modernization program as high risk because of the program's size, importance, and complexity and because of the cost and numerous problems it has encountered in systems acquisition.

We have previously reported information security weaknesses at FAA.² For instance, in December 2000, we reported that the agency had physical security vulnerabilities, ineffective operational systems security, inadequate service continuity efforts, an ineffective intrusion detection capability, and ineffective personnel security. We also noted that the agency had not yet implemented its information security program.

Information system controls are an important consideration for any organization that depends on computerized systems and networks to carry out its mission or business. These controls should provide adequate protections against outside as well as inside threats. It is especially important for government organizations, such as FAA, where maintaining the public trust is essential. Inadequately protected systems are at 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.

Since 1997, we have designated information security as a governmentwide high-risk area.³ 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. Congress and the executive branch have taken actions to address the risks associated with persistent information security weaknesses. In December 2002, Congress enacted the Federal Information Security Management Act (FISMA),⁴ which is intended to strengthen the information security of federal systems. In addition, the administration has taken important steps to improve information security, such as integrating it into the President's Management Agenda Scorecard. Moreover, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued security guidance to federal agencies.

²For example, see GAO, *FAA Computer Security: Recommendations to Address Continuing Weaknesses*, [GAO-01-171](#) (Washington, D.C.: Dec. 6, 2000); GAO, *FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses*, [GAO/AIMD-00-252](#) (Washington, D.C.: Aug. 16, 2000); and GAO, *Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety*, [GAO/AIMD-98-155](#) (Washington, D.C.: May 18, 1998).

³GAO, *High Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005).

⁴Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002, P.L. 107-347 (Dec. 17, 2002).

Objective, Scope, and Methodology

The objective of our review was to determine the extent to which FAA had implemented information security for its air traffic control systems. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*,⁵ which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data; (2) previous reports from DOT's Office of Inspector General (OIG); and (3) FISMA, which sets key elements that are required for an effective information security program.

Specifically, we evaluated information system controls that are intended to

- protect resources, data, and software from unauthorized access;
- prevent the introduction of unauthorized changes to application and system software;
- provide segregation of duties in the areas of application programming, system programming, computer operations, information security, and quality assurance;
- ensure recovery of computer processing operations in case of disaster or other unexpected interruption; and
- ensure an adequate information security program.

To evaluate these controls, we identified and reviewed pertinent DOT and FAA security policies and procedures. In addition, to determine whether information system general controls were in place, adequately designed, and operating effectively, we conducted vulnerability testing and assessments of systems from within the agency's network. We also held discussions with agency staff to gain an understanding of FAA's processes and controls. In addition, in order to take advantage of their prior work in this area, we held discussions with OIG staff and reviewed recent information security reports pertaining to air traffic control systems. Because the OIG had recently reviewed the system used by controllers to ensure the safe separation of aircraft, we did not include that system in our review.

⁵GAO, *Federal Information System Controls Audit Manual, Volume I—Financial Statements Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

We performed our review at FAA headquarters and tested operational and management controls⁶ at three other sites. At two additional sites, we tested these controls and, in addition, tested technical controls for three critical air traffic control systems. The limited distribution report contains further details on the scope of our review. This review was performed from March 2004 through June 2005 in accordance with generally accepted government auditing standards.

Although Progress Has Been Made, Air Traffic Control Systems Remain Vulnerable

Although FAA has made progress in implementing information security for its air traffic control systems by establishing an agencywide information security program and addressing many of its previously identified security weaknesses, significant control weaknesses threaten the integrity, confidentiality, and availability of those systems and information. In the systems we reviewed, we identified 36 weaknesses in electronic access controls and in other areas such as physical security, background investigations, segregation of duties, and application change controls. A key reason for these weaknesses is that the agency has not yet fully implemented an information security program. As a result, FAA's air traffic control systems remain vulnerable to unauthorized access, use, modification, and destruction that could disrupt aviation operations.

Electronic Access Controls Were Inadequate

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing electronic controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information. Electronic access controls include those related to network management, patch management, user accounts and passwords, user rights and file permissions, and audit and monitoring of security-relevant events. Inadequate electronic access controls diminish the reliability of computerized information, and they increase the risk of unauthorized

⁶Operational controls focus on controls that are executed by people (as opposed to systems). Management controls address security techniques and concerns that are normally addressed by organization's information security program management, such as management of risk within the organization. Technical controls focus on the security controls that information systems execute; these controls require significant operational considerations and should be consistent with management of security within the organization.

disclosure, modification, and destruction of sensitive information and of disruption of service.

Network Management

Networks are collections of interconnected computer systems and devices that allow individuals to share resources such as computer programs and information. Because sensitive programs and information are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests, deny unauthorized requests, and limit the services that are available on the network. Devices used to secure networks include (1) firewalls that prevent unauthorized access to the network, (2) routers that filter and forward data along the network, (3) switches that forward information among segments of a network, and (4) servers that host applications and data. Network services consist of protocols for transmitting data between network devices. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as denial-of-service attacks.⁷ Because networks often include both external and internal access points for electronic information assets, failure to secure these assets increases the risk of unauthorized modification of sensitive information and systems, or disruption of service.

For the systems we reviewed, FAA did not consistently configure network services and devices securely to prevent unauthorized access to and ensure the integrity of computer systems operating on its networks. We identified weaknesses in the way the agency restricted network access, developed application software, segregated its network, protected information flow, and stored the certificates⁸ that are used for authentication. For example:

- Access for system administration was not always adequately restricted, and unnecessary services were available on several network systems.
- Application software exhibited several weaknesses that could lead to unauthorized access or to service disruptions.

⁷A denial-of-service attack is an attack on a network that sends a flood of useless traffic that prevents legitimate use of the network.

⁸A certificate is a data record that is used for authenticating network entities such as a server or a client.

-
- Although FAA implemented controls to segregate network traffic, weaknesses in the application and infrastructure systems could allow an external attacker to circumvent network controls in order to gain unauthorized access to the internal network.
 - FAA did not encrypt certain information traversing its internal network. Instead, it used clear text protocols that made the network susceptible to eavesdropping.
 - FAA did not comply with federal standards for protected handling of certificates and keys.⁹ Because certificates are a primary tool for controlling access to applications, this improper storage puts major applications at risk of intrusion.

Patch Management

Patch management is a critical process that can help to alleviate many of the challenges of securing computing systems.¹⁰ As vulnerabilities in a system are discovered, attackers may attempt to exploit them, possibly causing significant damage. Malicious acts can range from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; destroy systems; disrupt operations; or launch attacks against other organizations' systems. After a vulnerability is validated, the software vendor develops and tests a patch or workaround. Incident response groups and software vendors issue information updates on the vulnerability and the availability of patches. FAA's patch management policy assigns organizational responsibilities for the patch management process—including the application of countermeasures to mitigate system vulnerability—and requires that patches be kept up to date or that officials otherwise accept the risk.

For the systems we reviewed, FAA did not consistently install patches in a timely manner. For example, patches that had been issued in 2002 had not been applied to certain servers that we reviewed. On another system, the operating system software, from 1991, was outdated and unpatched, although several vulnerabilities had been identified in the meantime. The agency did not believe that the system was vulnerable to unauthorized

⁹Cryptography relies on two basic components: an algorithm and a key. The algorithm is the mathematical function used to encrypt or decrypt, and the key is the parameter used in the transformation. A private key is uniquely associated with an entity.

¹⁰For example, see GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, [GAO-04-706](#) (Washington, D.C.: June 2, 2004).

access or that it was at low risk of exposure to these vulnerabilities. Because FAA had not yet installed the latest patches at the time of our review, firewalls, Web servers, and servers used for other purposes were vulnerable to denial-of-service attacks and to external attackers' taking remote control of them.

User Accounts and Passwords

A computer system must be able to identify and differentiate among users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system distinguishes one user from another—a process called identification. The system must also establish the validity of a user's claimed identity through some means of authentication, such as a password, that is known only to its owner. The combination of identification and authentication—such as user account/password combinations—provides the basis for establishing individual accountability and for controlling access to the system. Accordingly, agencies (1) establish password parameters, such as number of characters, type of characters, and the frequency with which users should change their passwords, in order to strengthen the effectiveness of passwords for authenticating the identity of users; (2) require encryption for passwords to prevent their disclosure to unauthorized individuals; and (3) implement procedures to control the use of user accounts. FAA policy identifies and prescribes minimum requirements for creating and managing passwords, including how complex the password must be and how to protect it. DOT policy also addresses the necessity to assign only one user to a given ID and password.

FAA did not adequately control user accounts and passwords to ensure that only authorized individuals were granted access to its systems. Because the agency did not always comply with complexity requirements, passwords on numerous accounts may be easy for an attacker to guess. Additionally, one of the databases we reviewed did not require strong passwords. We also identified database passwords that were not adequately protected because they were (1) readable by all system users on two Web servers, (2) in clear text format on multiple shared server directories, and (3) written into application program code. Such weaknesses increase the risk that passwords may be disclosed to unauthorized users and used to gain access to the system. Further, administrators and/or users shared user IDs and passwords on various devices, including servers, routers, and switches, thereby diminishing the effectiveness of the control for attributing system activity to individuals. As a result, FAA may not be able to hold users individually accountable for system activity.

User Rights and File Permissions

The concept of “least privilege” is a basic underlying principle for securing computer systems and data. It means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users’ access to only those programs and files that they need to do their work, organizations establish access rights and permissions. “User rights” are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that are associated with a particular file or directory and regulate which users can access them and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. DOT and FAA policies require that access privileges be granted to users at the minimum level required to perform their job-related duties.

FAA permitted excessive access to air traffic control systems, granting rights and permissions that allowed more access than users needed to perform their jobs. For example, FAA had granted users of a database system the access rights to create or change sensitive system files—even though they did not have a legitimate business need for this access. Further, the permissions for sensitive system files also inappropriately allowed all users to read, update, or execute them.

Audit and Monitoring of Security-Relevant Events

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail that they can use to determine the source of a transaction or attempted transaction and to monitor users’ activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events. DOT policy requires that audit logging be enabled on systems so that these events can be monitored.

For the systems we reviewed, FAA did not consistently audit and monitor security-relevant system activity on its servers. For example, on key devices that we reviewed, logging either was disabled or configured to overwrite, or it did not collect information on important security-relevant events such as failed login attempts. As a result, if a system was modified or

disrupted, the agency's capability to trace or recreate events would be diminished.

In response to weaknesses that we identified in electronic access controls, FAA officials told us that they had already corrected many of the weaknesses. Agency officials also pointed out that because major portions of air traffic control systems consist of custom-built, older equipment with special-purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited and therefore mitigate the risks. However, as we noted in our 1998 report¹¹ on FAA information security, one cannot conclude that old or obscure systems are secure simply because their configurations may not be commonly understood by external hackers. In addition, the systems' proprietary features do not provide protection from attack by disgruntled current and former employees who understand them, or from more sophisticated hackers. The weaknesses that we identified could allow unauthorized access to certain systems.

Other Information System Controls Were Not Sufficient

In addition to electronic access controls, other important controls should be in place to ensure the security and reliability of an organization's data. These controls include policies, procedures, and control techniques to physically secure computer resources, conduct suitable background investigations, provide appropriate segregation of duties, and prevent unauthorized changes to application software. However, weaknesses existed in each of these areas. These weaknesses increase the risk of unauthorized access to and modification of FAA's information systems and of disruption of service.

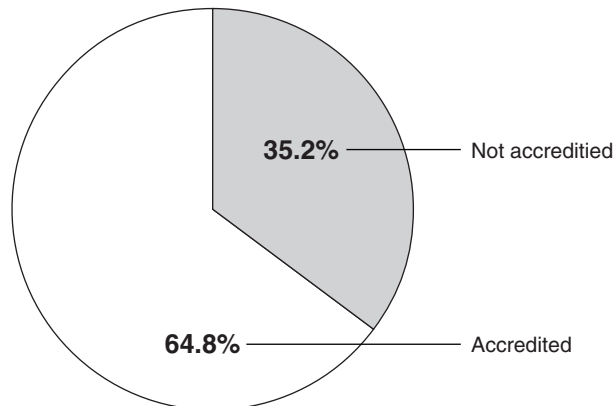
Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. At FAA, physical access control measures (such as guards, badges, and locks—used alone or in combination) are vital to protecting the agency's sensitive computing resources from both external and internal threats.

¹¹GAO/AIMD-98-155.

FAA has implemented a facility security management program that requires all staffed facilities to undergo a physical security review. These physical security reviews are part of an overall facility accreditation program, which requires facilities to meet all required security measures in order to become accredited. Since our December 2000 report, FAA has made progress with this program and has accredited about 430 additional facilities for a total of 64.8 percent of its staffed facilities (see fig. 5).

Figure 5: Percentage of Staffed Facilities That Have Been Accredited



Source: FAA.

Although FAA had taken some actions to strengthen its physical security environment, certain weaknesses reduced its effectiveness in protecting and controlling physical access to sensitive areas such as server rooms. Facility reviews are supposed to determine the overall risk level at the facility, examine the facility's security procedures, and discover local threats and vulnerabilities. However, in 2004, DOT's OIG reported that these physical security reviews generally focused more on the facility's perimeter than on vulnerabilities within the facility. We also identified weaknesses in FAA's physical security controls. Specific examples are listed below:

- FAA did not consistently ensure that access to sensitive computing resources had been granted to only those who needed it to perform their jobs.

-
- At the time of our review, FAA did not have a policy in place requiring that (1) physical access logs be reviewed for suspicious activity or (2) access privileges be reviewed to ensure that employees and contractors who had been granted access to sensitive areas still needed it. As a result, none of the sites we visited could ensure that employees and contractors who were accessing sensitive areas had a legitimate need for access.
 - Sensitive computing resources and critical operations areas were not always secured.
 - FAA did not properly control the badging systems used for granting physical access to facilities. The required information security access controls regarding password protection were inconsistently implemented, and division of roles and responsibilities was not enforced in the automated system.
 - The entrances to facilities were not always adequately protected. Visitor screening procedures were inconsistently implemented, and available tools were not being used properly or to their fullest capability.

These weaknesses in physical security increase the risk that unauthorized individuals could gain access to sensitive computing resources and data and could inadvertently or deliberately misuse or destroy them.

Background Investigations

According to OMB Circular A-130,¹² it has long been recognized that the greatest harm to computing resources has been done by authorized individuals engaged in improper activities—whether intentionally or accidentally. Personnel controls (such as screening individuals in positions of trust) supplement technical, operational, and management controls, particularly where the risk and magnitude of potential harm is high. NIST guidelines suggest that agencies determine the sensitivity of particular positions, based on such factors as the type and degree of harm that the individual could cause by misusing the computer system and on more traditional factors, such as access to classified information and fiduciary responsibilities. Background screenings (i.e., investigations) help an organization to determine whether a particular individual is suitable for a given position by attempting to ascertain the person’s trustworthiness and

¹²Office of Management and Budget, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (Nov. 28, 2000).

appropriateness for the position. The exact type of screening that takes place depends on the sensitivity of the position and any applicable regulations by which the agency is bound.

In 2000, we testified¹³ that FAA had failed to conduct background investigations on thousands of contractor personnel. Further, according to the testimony, many reinvestigations—which are required every 5 years for top secret clearances—were never completed. Since our 2000 testimony, the agency has made improvements to its background investigation program. For example, according to agency officials, it has completed background investigations for 90 percent of its contractor personnel and has implemented an automated system to track and report when reinvestigations are required.

Although FAA has recently made improvements to its background investigation program, the agency has not always properly designated sensitivity levels for positions involving tasks that could have a major impact on automated information systems. According to the Office of Personnel Management (OPM), positions with major responsibility for the design, testing, maintenance, operation, monitoring, or management of systems hardware and software should be designated as “high risk.”¹⁴ However, FAA has designated some of these types of positions as “moderate risk;” all 20 individuals that we identified as having system responsibilities with potentially significant access were designated as moderate risk or below. Further, OPM recommends a minimum background investigation¹⁵ for moderate risk positions. Nonetheless, FAA had been requiring only a National Agency Check and Inquiry, a less stringent investigation. Without properly designating position sensitivity levels and performing the appropriate background investigations, the agency faces an increased risk that inappropriate individuals could modify critical information and systems or disrupt operations.

¹³GAO, *FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations*, [GAO/T-AIMD-00-330](#) (Washington, D.C.: Sept. 27, 2000).

¹⁴For “high risk” positions, OPM recommends a background investigation, which includes a National Agency Check, credit search, personal interviews of subject and sources, written inquiries, and record searches covering specific areas of a person’s background during the most recent 5 years, and additional record searches during the most recent 7 years.

¹⁵A minimum background investigation is an investigation consisting of a National Agency Check and Inquiry, a credit search, and telephone inquiries to follow-up on written inquiries not returned.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes be implemented, and computer resources be damaged or destroyed.

For the systems we reviewed, FAA did not properly segregate incompatible duties in its computer-related operations. Key duties in a computer environment that are generally segregated include software design, development, and testing; software change control; computer operations; and computer production control. However, on one of the systems that we reviewed, FAA allowed software developers to place application code into the production environment. With access to production systems, software developers could intentionally introduce malicious code. Additionally, FAA did not have mitigating controls; for example, there was no provision for reviewing code on production systems to ensure that only authorized code was placed into production. FAA officials told us that it plans to establish an independent production control group that would place code into production once resources become available for this particular system. Without adequate segregation of duties or appropriate mitigating controls, FAA is at increased risk that unauthorized code could be introduced into the production environment, possibly without detection.

Application Change Controls

It is important to ensure that only authorized and fully tested application programs are placed in operation. To ensure that changes to application programs are necessary, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. In addition, test procedures should be established to ensure that only authorized changes are made to the application's program code.

Application change control procedures that FAA's contractor used were incomplete. At one site, we reviewed change control and quality assurance documentation for 10 of 50 software changes that had been made by FAA's contractor in 2004. We determined that the contractor appropriately followed its own change control process, only omitting a few minor items

in its documentation. However, although the contractor's change control process adequately addressed software testing, it did not include reviewing code after it had been installed on production systems to verify that the correct code had been placed into production. This issue is important, because developers are allowed access to production systems. With no mitigating controls in place, developers could introduce unauthorized code into production systems—without detection.

Information Security Program Is Not Yet Fully Implemented

A key reason for the information security weaknesses that we identified in FAA's air traffic control systems was that the agency had not yet fully implemented its information security program to help ensure that effective controls were established and maintained. FAA has implemented the foundation for an effective information security program with written policy and guiding procedures that designate responsibility for implementation throughout the agency.

FISMA¹⁶ requires agencies to implement an information security program that includes

- periodic assessments of the risk and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel—including contractors and other users of information systems—of information security risks

¹⁶FISMA requires each agency to develop, document, and implement an agencywide information security program to provide information security for the information and systems that support the operations and assets of the agency, including those operated or maintained by contractors or others on behalf of the agency, using a risk-based approach to information security management.

and of their responsibilities in complying with agency policies and procedures;

- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls of every major information system that is identified in the agencies' inventories;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in their 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.

FAA has made progress in implementing information security by establishing an agencywide information security program and addressing many of its previously identified security weaknesses. FAA's *Information System Security Program Handbook* requires each of these FISMA elements, and the agency has initiatives under way in all of these areas. In addition, the Office of Information Systems Security has developed a security management tool to monitor (1) the status of corrective actions, (2) the status of certifications and authorizations¹⁷ for all systems in FAA's inventory, (3) information security-related budgetary allocations and expenditures, and (4) training requirements for key security personnel.

However, we identified instances in which the program had not been fully or consistently implemented for the air traffic control systems. Agency officials recognize that more work is needed to continue to improve their information security program.

¹⁷OMB information security policy requires agency management officials to formally authorize each of their information systems to process, store, or transmit information, and to accept the risk associated with their operation. This authorization (accreditation) decision is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan.

Risk Assessments

Identifying and assessing information security risks are essential steps in determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. Further, OMB Circular A-130, appendix III, prescribes that risk be reassessed when significant changes are made to computerized systems—or at least every 3 years, as does FAA policy. Consistent with NIST guidance, FAA requires that risk assessments include identifying system interconnections, information sensitivity, threats and existing countermeasures and analyzing vulnerabilities.

The risk assessments that we reviewed generally complied with FAA requirements. For the systems we reviewed, FAA provided five risk assessments. Four of the five included the required topics. However, the risk assessment for the fifth one was incomplete and did not always address countermeasures. Inadequately assessing risk and identifying countermeasures can lead to implementing inadequate or inappropriate security controls that might not address the system's true risk, and to costly efforts to subsequently implement effective controls.

Policies and Procedures

Another key task in developing an effective information security program is to establish and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures should help reduce the risk that could come from unauthorized access or disruption of services. Technical security standards provide consistent implementing guidance for each computing environment. Because security policies are the primary mechanism by which management communicates its views and requirements, it is important to establish and document them.

FAA's Office of Information Systems Security has developed systems security policies, with the intent to provide security commensurate with the risks of unauthorized access or disruption of service. For example, FAA has developed policies on an overall information system security program, background investigations, and password management. Further, the agency's *Information System Security Program Handbook* provides detailed information on certification and authorization of information systems. DOT has also developed various technical standards, which address various computing environments. However, FAA's policies and procedures did not address issues such as reviewing and monitoring physical access. In addition, the agency had not yet developed procedures to effectively implement patch management for its air traffic control

systems. Also, as noted earlier, in some instances—such as password management—FAA was not following its own policies and procedures. Without effectively implementing policies and procedures, the agency has less assurance that their systems and information are protected.

Security Plans

The objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place—or planned—to meet those requirements. OMB Circular A-130 requires that agencies develop and implement system security plans for major applications and for general support systems¹⁸ and that these plans address policies and procedures for providing management, operational, and technical controls. Further, Circular A-130 requires that agencies' plans be consistent with guidance issued by NIST. FAA policy requires that security plans be developed, and its *Information System Security Program Handbook* provides guidance on developing security plans. According to both FAA and NIST, plans should include elements such as security controls currently in place or planned, the individual responsible for the security of the system, a description of the system and its interconnected environment, and rules of behavior.

Although the security plans that we reviewed generally complied with FAA policy and guidance, we identified instances where plans were incomplete or not up-to-date. All five of the information system security plans we reviewed were missing information required by FAA. Procedures outlining the individuals responsible for plan reviews and monitoring the status of planned controls were missing in each case. Also, no agency officials were identified to fulfill this responsibility. Although a security plan had been developed for one of FAA's major applications, it was missing such required sections as rules of behavior and controls in place for public access. Another plan did not identify the system owner or the individual who had responsibility for system security. Further, some sections in one of the plans we reviewed were outdated. For example, security controls that existed at the time of our review were not described in the plan. Without complete and up-to-date security plans, FAA cannot ensure that

¹⁸A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications.

appropriate controls are in place to protect its systems and critical information.

Security Awareness Training

Another FISMA requirement for an information security program is that it promote awareness and provide required training for users so that they can understand the system security risks and their role in implementing related policies and controls to mitigate those risks. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees and contractors who use computer resources in their day-to-day operations be made aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. FISMA mandates that all federal employees and contractors who use agency information systems be provided with periodic training in information security awareness and accepted information security practice. FAA has established a policy requiring employees and contractors to take annual security awareness training. Further, FISMA requires agency CIOs to ensure that personnel with significant information security responsibilities get specialized training. OMB and NIST also require agencies to implement system-specific security training.

In December 2000, we reported that FAA had not fully implemented a security awareness and training program. Since then, the agency has established its policy for annual training and has implemented an agencywide security awareness program that includes newsletters, posters, security awareness days, and a Web site. FAA has also implemented a Web-based security awareness training tool that not only meets the requirements of FISMA, but also records whether individuals have completed the training. The training records that we reviewed showed that personnel with significant information security responsibilities had received specialized training.

Despite the agency's progress in security awareness training, we identified shortcomings with the program. For example, although FAA implemented a Web-based training tool, the agency does not require all employees and contractors to use it. As a result, not all contractors and employees receive annual training, training is not appropriately tracked and reported, and the training provided in place of the tool is not always adequate. Although FAA reported in its most recent FISMA report that 100 percent of its employees and contractors had taken security awareness training, it was unable to

provide documentation for more than one-third of selected¹⁹ employees and contractors. Further, the agency does not have an effective tracking mechanism for security awareness training. In some circumstances, management relies on verbal responses from employees and contractors on whether they have completed training, but it has no uniform reporting requirements. Instead they receive responses in different forms, such as telephone conversations, e-mails, and faxes. In instances where the Web-based tool is not used, the awareness training may be inadequate. At one of the sites we visited, this training consisted of a briefing that did not cover information system security and risks. Further, the agency had not developed guidance or procedures for system-specific security training, as required by OMB and NIST.

Without adequate security awareness and training programs, security lapses are more likely to occur. As in our 2000 report, we were able to access sensitive security information on the Internet. FAA agreed that the information we identified was sensitive and took prompt action to remove the specific examples that we had provided. However, 8 months later, one of the examples was available on the Internet again, even though it was marked for “Internal Distribution Only.”

Tests and Evaluations of Control Effectiveness

Another key element of an information security program is testing and evaluating systems to ensure that they are in compliance with policies and that policies and controls are both appropriate and effective. This type of oversight is a fundamental element because it demonstrates management’s commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results improve the security program. Analyzing the results of security reviews provides security specialists and business managers with a means of identifying new problem areas, reassessing the appropriateness of existing controls, and identifying the need for new controls. FISMA requires that the frequency of tests and evaluations be based on risks, but occur no less than annually. Security tests and evaluations are part of FAA’s certification and authorization process, which is required every 3 years or when significant changes to the system occur. According to agency

¹⁹We selected 65 individuals in total from the sites we visited. We did not select a statistical sample. Some selections were random from a listing of employees and contractors on-site, while others were based on the role of an individual, such as a system administrator.

officials, in each of the following 2 years, FAA conducts a self-assessment based on NIST guidance.

Although FAA had conducted system tests and evaluations, documentation and testing were not always adequate. For example:

- In three of the five test plan and results reports we reviewed, most of the test results were not included. Additionally, very little testing was conducted on the network and infrastructure pieces of any of the systems we reviewed.
- As of April 2005, the certifications and authorizations for about 24 percent of the air traffic control systems were either outdated or had not been completed. According to FAA officials, the agency's risk-based approach focused on certifying and accrediting all of its systems; therefore, management accepted an extension beyond 3 years for some systems.
- DOT's IG testified that some of the testing is being conducted only on developmental systems, rather than operational systems.
- FAA's practice was to perform system tests and evaluations annually without regard to criticality. Our tests of critical systems identified many weaknesses. More frequent testing by FAA of these systems may have identified, and FAA could have corrected, many of the information security weaknesses discussed in this report.

Without appropriate tests and evaluations, the agency cannot be assured that employees and contractors are complying with established policies or that policies and controls are appropriate and working as intended.

Remedial Actions

Remedial action plans are a key component described in FISMA. They assist agencies in identifying, assessing, prioritizing, and monitoring the progress in correcting security weaknesses that are found in information systems. According to OMB Circular A-123, agencies should take timely and effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, remedial action plans should be developed for each deficiency, and progress should be tracked for each. FAA policy requires remediation reports to address the results of tests and evaluations.

Although the agency has developed a remedial action tracking system, which included remedial plans, for weaknesses identified through previous reviews in order to help it monitor the progress in correcting security weaknesses, these remedial plans did not address all identified weaknesses, and some deficiencies were not always corrected in a timely manner.

Incident Handling

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they promptly take steps to detect and respond to them before significant damage is done. In addition, accounting for and analyzing security problems and incidents are effective ways for organizations to gain a better understanding of threats to their information and of the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. Problem and incident reports can provide valuable input for risk assessments, can help in prioritizing security improvement efforts, and can be used to illustrate risks and related trends for senior management. DOT has issued a policy for detecting, reporting, and responding to security incidents.

In December 2000, we reported that FAA had not fully implemented an effective intrusion detection capability. Since then, FAA has established a Computer Security Incident Response Center, whose mission is to detect and respond to intrusions on FAA's systems. The Center produces incident reports and provides agency management with various analyses. However, the following weaknesses prevent it from effectively detecting and responding to many potential threats:

- Although the agency has deployed intrusion detection systems, these systems do not cover all segments of the air traffic control system. According to FAA officials, the agency has a risk-based plan to further deploy intrusion detection capabilities.
- One of the intrusion detection systems that we reviewed was configured in such a way that it was unable to detect potential intrusions.

While FAA has made progress, it remains at risk of not being able to detect or respond quickly to security incidents.

Continuity of Operations

Continuity of operations controls, sometimes referred to as service continuity, should be designed to ensure that when unexpected events occur, key operations continue without interruption or are promptly

resumed, and critical and sensitive data are protected. These controls include environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions, along with a plan to recover critical operations should interruptions occur. If continuity of operations controls are inadequate, even a relatively minor interruption could result in significant adverse nationwide impact on air traffic. FAA requires that continuity of operations plans be included as part of its certification and authorization process.

Although FAA has various initiatives under way to address continuity of operations, shortcomings exist. For the systems we reviewed, FAA identified five continuity of operations plans. One plan was incomplete and FAA included the need to complete this plan in its remediation report. While four plans were completed, one of these did not contain accurate information. It described an operating environment to be used as a contingency, yet this environment did not exist at the time of our review. Further, in April 2005, DOT's IG testified that FAA had not made sufficient progress in developing continuity plans to enable it to restore air traffic control services in case of a prolonged service disruption at the en route centers. Until the agency completes actions to address these weaknesses, it is at risk of not being able to appropriately recover in a timely manner from certain service disruptions.

Conclusions

Although FAA has made progress in implementing information security by establishing an agencywide information security program and addressing many of its previously identified security weaknesses, significant information security weaknesses remain that could potentially lead to disruption in aviation operations. These include weaknesses in electronic access controls, for example, in managing networks, system patches, user accounts and passwords, and user rights and in logging and auditing security-relevant events. Weaknesses in physical security, background investigations, segregation of duties, and application change controls increase the level of risk. A key reason for FAA's weaknesses in information system controls is that it has not yet fully implemented an information security program to ensure that effective controls are established and maintained. Effective implementation of such a program provides for periodically assessing risks, establishing appropriate policies and procedures, developing and implementing security plans, promoting security awareness training, testing and evaluating the effectiveness of controls, implementing corrective actions, responding to incidents, and

ensuring continuity of operations. Although FAA has initiatives under way to address these areas, further efforts are needed to fully implement them.

Recommendations for Executive Action

To help establish effective information security over air traffic control systems, we recommend that the Secretary of Transportation direct the FAA Administrator to take the following 12 actions to fully implement an information security program:

- Ensure that risk assessments are completed.
- Develop and implement policies and procedures to address such issues as patch management and the reviewing and monitoring of physical access.
- Review system security plans to ensure that they contain the information required by OMB A-130 and are up to date.
- Enhance the security awareness training program to ensure that all employees and contractors receive information security awareness training, as well as system specific training, and that completion of the training is appropriately reported and tracked.
- Develop a process to ensure that sensitive information is not publicly available on the Internet.
- Conduct tests and evaluations of the effectiveness of controls on operational systems, and document results.
- Perform more frequent testing of system controls on critical systems to ensure that the controls are operating as intended.
- Review remedial action plans to ensure that they address all of the weaknesses that have been identified.
- Prioritize weaknesses in the remedial action plans and establish appropriate, timely milestone dates for completing the planned actions.
- Implement FAA's plan to deploy intrusion detection capabilities for portions of the network infrastructure that are not currently covered.

-
- Correct configuration issues in current intrusion detection systems to ensure that they are working as intended.
 - Review service continuity plans to ensure that they appropriately reflect the current operating environment.

We are also making recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses we identified that are related to network management, patch management, password management, user privileges, auditing and logging, physical security, background investigations, segregation of duties, and application change controls.

Agency Comments and Our Evaluation

In providing oral comments on a draft of this report, the FAA's CIO agreed to consider our recommendations and emphasized several points. He stated that the issues we identified in the three individual systems we examined are not necessarily indicative of the security posture of the air traffic control system as a whole. We acknowledge that we focused our examination on the technical controls of three critical systems. In addition, we reviewed management and operational controls at five sites and FAA headquarters and relied on the OIG's prior work pertaining to air traffic control systems. We concluded that significant information security weaknesses remain that could potentially lead to a disruption in aviation operations.

The CIO also indicated that the implications of the findings in this report should be tempered by the understanding that individual system vulnerabilities are further mitigated by system redundancies and separate access controls that are built into the overall air traffic control system architecture to provide additional protection that is not considered within the context of this review. He was concerned that our report does not always balance the identification of individual system issues with consideration of the relative risk that an issue may pose to the overall system and that the public may be prone to infer from the report that the security risks to the air traffic control system are higher than they may actually be. We acknowledge that FAA may have other protections built into the overall system architecture. However, as noted in this report, the complex air traffic control system relies on several interconnected systems. As a result, the weaknesses we identified may increase the risk to other systems. For example, FAA did not consistently configure network

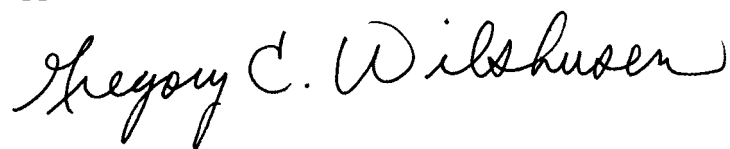
services and devices securely to prevent unauthorized access to and ensure the integrity of computer systems operating on its networks.

In addition, the CIO indicated that all security findings for air traffic control systems, including those from our report, are evaluated and prioritized for action and that FAA has established a sound track record for moving quickly to address priority issues—as demonstrated by the extensive actions the agency has taken on issues identified in our previous reports and in DOT OIG reports. For example, according to the CIO, FAA established an extensive information security training program; deployed intrusion detection systems; and established the Computer Security Incident Response Center as a prevention, detection and reporting capability on a 24x7x365 basis. Finally, he stated that as a result of FAA's information security actions, it achieved 100 percent of the President's Management Agenda goals for certification and authorization of its systems, completed certification and authorization for over 90 percent of its systems in fiscal year 2004, and completed 100 percent of its certifications and authorizations by June 30, 2005. We acknowledge in our report that FAA has made progress in implementing its information security program and has initiatives under way; however, we identified weaknesses in key areas cited by the CIO. For example, as noted in this report, although FAA conducted tests and evaluations as part of its certification and authorization process, some of these were outdated and documentation and testing were not always adequate.

The CIO also provided specific technical comments, which we have incorporated, as appropriate, in the report.

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 to congressional committees with jurisdiction over FAA and executive branch agencies' information security programs, the Secretary of Transportation, the FAA Administrator, the DOT Inspector General, and other interested parties. We also will make copies available to others on request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions regarding this report, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix I.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, stylized 'G' and 'W'.

Gregory C. Wilshusen
Director, Information Security Issues

GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen (202) 512-6244

Acknowledgments

In addition to the person named above, Edward Alexander, Mark Canter, Nicole Carpenter, Jason Carroll, Lon Chin, William Cook, Kirk Daubenspeck, Neil Doherty, Patrick Dugan, Joanne Fiorino, Edward Glagola, Steve Gosewehr, Jeffrey Knott, Carol Langelier, Harold Lewis, Duc Ngo, Eugene Stevens, and Chris Warweg made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548