United States General Accounting Office

GAO

Report to the Committee on Governmental Affairs, U.S. Senate

May 1998

AIR TRAFFIC CONTROL

Weak Computer Security Practices Jeopardize Flight Safety

GAO/AIMD-98-155

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-276735

May 18, 1998

The Honorable Fred Thompson
Chairman
The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

Security at our nation's airports has received great attention in recent years due to several commercial aircraft explosions; however, securing our nation's airports alone does not ensure safe air travel. It is also critical to secure the Federal Aviation Administration's (FAA) air traffic control (ATC) computer systems that provide information to air traffic controllers and aircraft flight crews to ensure safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruption of air traffic or even loss of life due to collisions. Since malicious attacks on computer systems are an increasing threat, it is essential that FAA ensure the integrity and availability of ATC information and protect it from unauthorized users.

Given the paramount importance of computer security of ATC systems, you asked us to determine (1) whether FAA is effectively managing physical security at ATC facilities and systems security for its current operational systems, (2) whether FAA is effectively managing systems security for future ATC modernization systems, and (3) the effectiveness of FAA's management structure and implementation of policy for computer security. We issued a "Limited Official Use" report to you detailing the results of our review on April 29, 1998. This unclassified version of that report summarizes the weaknesses we found in FAA's ATC computer security program and our recommendations for corrective actions.

Results in Brief

FAA is ineffective in all critical areas included in our computer security review—facilities physical security, operational systems information security, future systems modernization security, and management structure and policy implementation.

In the physical security area, known weaknesses exist at many ATC facilities. For example, a March 1997 inspection of a facility that controls aircraft disclosed 13 physical security weaknesses, including unauthorized personnel being granted unescorted access to restricted areas. FAA is

unaware of weaknesses that may exist at other locations. For example, FAA has not assessed the physical security controls at 187 facilities since 1993 and therefore does not know how vulnerable they are.

Second, FAA is similarly ineffective in managing systems security for its operational systems and is in violation of its own policy. An October 1996 information systems security assessment concluded that FAA had performed the necessary analysis to determine system threats, vulnerabilities, and safeguards for only 3 of 90 operational ATC computer systems, or less than 4 percent. FAA officials told us that this assessment is an accurate depiction of the current state of operational systems security. Further, according to the team that maintains FAA's telecommunications networks, only one of the nine operational ATC telecommunications networks has been analyzed. Without knowing the specific vulnerabilities of its ATC systems, FAA cannot adequately protect them.

Third, FAA is also not effectively managing systems security for future ATC modernization systems. It does not consistently include well formulated security requirements in specifications for all new ATC modernization systems, as required by FAA policy. Further, it does not have a well-defined security architecture, a concept of operations, or security standards all of which are needed to define and ensure adequate security throughout the ATC network.

Finally, FAA's management structure and implementation of policy for ATC computer security is not effective. Security responsibilities are distributed among three organizations, all of which have been remiss in their ATC security duties. The Office of Civil Aviation Security is responsible for developing and enforcing security policy, the Office of Air Traffic Services is responsible for implementing security policy for operational ATC systems, and the Office of Research and Acquisitions is responsible for implementing policy for ATC systems that are being developed. The Office of Civil Aviation Security has not adequately enforced FAA policies that require the assessment of physical security controls at all ATC facilities and vulnerabilities, threats, and safeguards for all operational ATC computer systems. In addition, the Office of Air Traffic Services has not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards. Finally, the Office of Research and Acquisitions has not implemented the FAA policy that requires it to formulate requirements for security in specifications for all new ATC modernization systems.

Background

FAA's ATC network is an enormous, complex collection of interrelated systems, including navigation, surveillance, weather, and automated information processing and display systems that reside at, or are associated with, hundreds of ATC facilities. These systems and facilities are interconnected by complex communications networks that separately transmit both voice and digital data. As stated in our 1997 report on high-risk issues,[1] while the use of interconnected systems promises significant benefits in improved government operations, it also increases vulnerability to anonymous intruders who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations. Since this interconnectivity is expected to grow as systems are modernized to meet the projected increases in air traffic and to replace aging equipment, the ATC network will become even more vulnerable to such network-related threats.

The threat to information systems is also growing because of the increasing availability of strategies and tools for launching planned attacks. For example, in May 1996 we reported that tests at the Department of Defense showed that Defense systems may have experienced as many as 250,000 attacks during 1995, about 65 percent of these succeeded in gaining access, and only about 4 percent were detected.[2]

Since intruders can use a variety of techniques to attack computer systems, it is essential that FAA's approach to computer security be comprehensive and include (1) physical security of the facilities that house ATC systems (e.g., locks, guards, fences, and surveillance equipment), (2) information security of the ATC systems (e.g., safeguards incorporated into computer hardware and software), and (3) telecommunications security of the networks linking ATC systems and facilities (e.g., secure gateways, firewalls, and communication port protection devices).

For years, the need for federal agencies to protect sensitive and critical, but unclassified, federal data has been recognized in various laws, including the Privacy Act of 1974, the Computer Security Act of 1987, and the Paperwork Reduction Act of 1995, and was recently reemphasized in the Clinger-Cohen Act of 1996. The adequacy of controls over computerized data is also addressed indirectly by the Federal Managers'

[1] High-Risk Series: Information Management and Technology (GAO/HR-97-09, Feb. 1997).

[2] Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

Financial Integrity Act (FMFIA) of 1982 and the Chief Financial Officers Act of 1990. For example, FMFIA requires agency managers to evaluate their internal control systems annually and report to the President and the Congress any material weaknesses that could lead to fraud, waste, and abuse in government operations. In addition, a considerable body of federal guidance on information security has been developed by both the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Objectives, Scope, and Methodology

The objectives of our review were to determine (1) whether FAA is effectively managing physical security at ATC facilities and systems security for its current operational systems, (2) whether FAA is effectively managing systems security for future ATC modernization systems, and (3) the effectiveness of FAA's management structure and implementation of policy for computer security.

To determine whether FAA is effectively managing physical security at ATC facilities, we

- reviewed FAA Order 1600.6C, Physical Security Management Program, to determine ATC facility security inspection and accreditation requirements;
- reviewed data from FAA's Facility Inspection Reporting System (FIRS) to determine the accreditation status of category I and II towers, terminal radar approach control (TRACON) facilities, and air route traffic control towers (en route centers) and their last inspection date;[3]
- verified the accuracy of the FIRS accreditation data with each of the nine regional FIRS program managers by requesting accreditation reports for each facility that FIRS reported as being accredited;
- for those facilities that were not accredited, requested dates of their initial comprehensive physical security inspection[4] and follow-up inspections from each of the nine regional FIRS program managers to determine why ATC facilities were not accredited;
- verified the initial and follow-up inspection dates by requesting and reviewing documentation for each inspection conducted from April 16, 1993, to July 31, 1997, and then provided our analyses to Office of Civil

[3]Category I facilities are those that are critical to national security and the National Airspace System (NAS). Category II facilities are other FAA-staffed facilities. We did not review security measures at airports.

[4]FAA calls this initial physical security inspection an initial physical security survey, and it includes an evaluation of the local threat, physical security controls, security documentation, and required corrective actions.

Aviation Security Operations officials, who in turn verified it with each region;

- reviewed the Department of Justice's June 28, 1995, report, Vulnerability Assessment of Federal Facilities, to identify new physical security requirements for federal facilities;
- reviewed physical security assessments for three locations to determine FAA's ATC compliance with Department of Justice blast standards and to identify additional physical security weaknesses at key ATC facilities;
- reviewed the Facility Security Risk Management Mission Need Statement for Staffed Facilities, Number 316, June 23, 1997, to determine physical security deficiencies and FAA's plans to improve physical security; and
- interviewed officials from the Offices of Civil Aviation Security, Operations and Policy and Planning, and Airways Facility Services to determine physical security requirements, to determine whether FAA is in compliance with 1600.6C, to identify reasons for noncompliance, and to identify who develops, implements, and enforces ATC physical security policy.

To determine whether FAA is effectively managing systems security for its current operational systems, we

- reviewed federal computer security requirements specified in the Computer Security Act of 1987 (Public Law 100-235); Paperwork Reduction Act of 1995 (Public Law 104-13), as amended; OMB Circular A-130, appendix III, "Security of Federal Automated Information Resources;" the 1996 Clinger-Cohen Act; and An Introduction to Computer Security: The NIST Handbook to identify federal security requirements;
- reviewed FAA Order 1600.54B, FAA Automated Information Systems Security Handbook, and FAA Order 1600.66, Telecommunications and Information Systems Security Policy, to determine ATC system risk assessment, certification, and accreditation requirements;
- reviewed Volpe National Transportation Systems Center NAS AIS Security Review, October 1, 1996, to determine how many ATC operational systems were assessed, certified, and accredited as of October 1, 1996;
- requested and reviewed accreditation reports, security certification reports, risk assessments, contingency plans, and disaster recovery plans for six operational ATC systems;[5]
- reviewed the White House Commission on Aviation Safety and Security's final report to the President, February 12, 1997, to determine recommendations to improve ATC computer security;

[5]The six operational ATC systems we selected were not intended to be a representative sample. However, each is critical to controlling aircraft, and collectively they represent systems from different environments in which aircraft are controlled.

- reviewed the Federal Aviation Administration Air to Ground Communications Vulnerabilities Assessment, June 1993, to determine ATC communication systems vulnerabilities;
- reviewed the Report to Congress, Air Traffic Control Data and Communications Vulnerabilities and Security, Report of the Federal Aviation Administration Pursuant to House-Senate Report Accompanying the Department of Transportation and Related Agencies Appropriations Act, 102-639, June 1, 1993, to determine what ATC security vulnerabilities FAA disclosed to the Congress in 1993;
- interviewed the telecommunications integrated product team to determine what operational communication systems have been assessed, certified, and accredited and reviewed the team's 1994 and 1997 strategic plans to determine communication system risks and planned security improvement initiatives;
- interviewed the Director of Spectrum Policy and Management to determine the extent to which intruders are accessing ATC frequencies;
- interviewed FAA's Designated Approving Authority (DAA) to determine FAA's policy for accrediting ATC systems; and
- interviewed the Office of Civil Aviation Security Operations officials and Airways Facilities Services officials to determine who develops, implements, and enforces ATC operational systems security policy and to determine whether an incident reporting and handling capability exists.

To determine whether FAA is effectively managing systems security for future ATC modernization systems, we

- requested and reviewed risk assessments and acquisition specifications for six ATC systems that are being developed to determine if security requirements based on detailed assessments existed;[6]
- interviewed three integrated product teams (IPT) to determine what security policy/guidance each follows in developing ATC systems;
- reviewed the NAS Information Security Mission Need Statement, April 22, 1997, to determine information security deficiencies, future system vulnerabilities, and FAA's plans to improve information security;
- interviewed the NAS Information Security (NIS) group to determine its plans to improve ATC information security and reviewed its NAS Information Security Action Plan; and
- reviewed the President's Commission of Critical Infrastructure Protection's (PCCIP) final report, Critical Foundations, Protecting America's Infrastructures, October 1997, and its supplemental report,

[6]The six ATC systems currently being developed that we selected were not intended to be a representative sample. However, each will be critical to controlling aircraft in the future, and collectively they represent systems from different environments in which aircraft are controlled.

Vulnerability Assessment of the FAA National Airspace Systems (NAS) Architecture, October 1997, to determine future ATC systems security vulnerabilities.

To determine the effectiveness of FAA's management structure and implementation of policy for computer security, we

- reviewed FAA Order 1600.6C, Physical Security Management Program (dated April 1993), Order 1600.54B, FAA Automated Information Systems Security Handbook (dated February 1989), and Order 1600.66, Telecommunications and Information Systems Security Policy (dated July 1994), to determine what organizations are assigned responsibility for developing, implementing, and enforcing ATC computer security policy[7] and
- interviewed officials from the Offices of Civil Aviation Security, Air Traffic Services, and Research and Acquisitions to determine what organizations are responsible for developing, implementing, and enforcing ATC computer security policy.

In addition, we interviewed the Associate Administrators for Civil Aviation Security and for Research and Acquisitions and the Director of Airway Facilities under the Associate Administrator for Air Traffic Services to determine why ATC computer security policies have not been adequately implemented and enforced.

We performed our work at FAA headquarters in Washington, D.C., from April 1997 through January 1998 in accordance with generally accepted government auditing standards.

ATC Physical Security Management and Controls Are Ineffective

ATC systems used to control aircraft reside at, or are associated with, a variety of ATC facilities including towers, TRACONs, and en route centers. FAA policy, dated April 1993, required that these facilities be inspected by April 1995 and that annual or triennial follow-up inspections be conducted depending on the type of facility to determine the status of physical security at each facility. These inspections determine whether the facility meets the physical security standards established in FAA policy and are the basis for accrediting ATC facilities (i.e., concluding that they are secure).

[7]We did not conduct a complete assessment of Orders 1600.6C, 1600.54B, or 1600.66 since two of these orders were undergoing major revisions at the time of our review.

FAA is not effectively managing physical security at ATC facilities. Known physical security weaknesses exist at many ATC facilities. For example, an inspection of a facility that controls aircraft disclosed 26 physical security findings including (1) fire protection systems that failed to meet minimum detection and suppression standards and (2) service contract employees that were given unrestricted access to sensitive areas without having appropriate background investigations. FAA recently confirmed its physical security weaknesses when it performed detailed assessments of several key ATC facilities following the Oklahoma City bombing to determine physical security risks and the associated security measures and costs required to reduce these risks to an acceptable level.[8] For example, an assessment of a facility that controls aircraft concluded that access control procedures are weak to nonexistent and that the center is extremely vulnerable to criminal and terrorist attack.

In addition, FAA is unaware of physical security weaknesses that may exist at other FAA facilities. For example, FAA has not assessed the physical security controls at 187 facilities since 1993 and therefore does not know how vulnerable they are. Until FAA inspects its remaining facilities, it does not know if they are secure and if the appropriate controls are in place to prevent loss or damage to FAA property, injury to FAA employees, or compromise of FAA's capability to perform critical air safety functions.

ATC Operational System Security Is Ineffective and Systems Are Vulnerable

FAA policy requires that all ATC systems be certified and accredited.[9] A risk assessment, which identifies and evaluates vulnerabilities, is a key requirement for certification and accreditation. We recently reported that leading information security organizations use risk assessments to identify and manage security risks confronting their organizations.[10]

FAA has not assessed, certified, or accredited most operational ATC systems. A review conducted for FAA's Office of Civil Aviation Security in October 1996 concluded that FAA had not conducted risk assessments on 83 of 90, or over 90 percent, of all operational ATC systems. FAA officials told us that this assessment is an accurate depiction of the agency's

[8]A key part of these assessments was to conduct a blast analysis of FAA facilities.

[9]System certification is the technical evaluation that is conducted to verify that FAA systems comply with FAA security requirements, identify security deficiencies, specify remedies, and justify exceptions. Certification results are one factor management considers in deciding whether to accredit systems. Accreditation is the formal declaration from management that the appropriate security safeguards have been properly implemented and that residual risk is acceptable.

[10]Executive Guide: Information Security Management — Learning From Leading Organizations (Exposure Draft) (GAO/AIMD-98-21, Nov. 1997).

knowledge regarding operational systems security. As a result, FAA does not know how vulnerable these operational ATC systems are and consequently has no basis for determining what protective measures are required. Further, the review concluded that of the 7 systems assessed, only 3 resulted in certifications because 4 systems did not have the proper certification documentation.[11] Accordingly, less than 4 percent of the 90 operational systems are certified. In addition, FAA has not assessed most ATC telecommunication systems. For example, FAA's officials responsible for maintaining the nine FAA-owned and leased communication networks told us that only one has been assessed. Such poor security management exists despite the fact that FAA's 1994 Telecommunications Strategic Plan stated that "vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety." FAA's 1997 Telecommunications Strategic Plan continues to identify security of telecommunication systems as an area in need of improvement.

Office of Civil Aviation Security officials told us that they were not aware of a single ATC system that was accredited. We found similar results when we reviewed six operational systems to determine if they were assessed, certified, or accredited. Risk assessments had been conducted and certification reports written for only two of the systems, while none of the systems had been accredited. The Associate Administrator for Civil Aviation Security, who is responsible for accrediting systems, told us that FAA has decided to spend its limited funds not on securing currently operating systems, but rather on developing new systems and that FAA management is reluctant to acknowledge information security threats.

FAA claims that because current ATC systems often utilize custom-built, 20-year-old equipment with special purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited. While these configurations may not be commonly understood by external hackers, one cannot conclude that old or obscure systems are, a priori, secure. In addition, the certification reports that FAA has done reveal operational systems vulnerabilities. Furthermore, archaic and proprietary features of the ATC system provide no protection from attack by disgruntled current and former employees who understand them.

[11]The documentation did not exist or was not signed by appropriate authorities.

FAA Is Not Effectively Managing Security for New ATC Systems

Essential computer security measures can be provided most effectively and cost efficiently if they are addressed during systems design. Retrofitting security features into an operational system is far more expensive and often less effective. Sound overall security guidance, including a security architecture, security concept of operations, and security standards, is needed to ensure that well formulated security requirements are included in specifications for all new ATC systems.

FAA has no security architecture, security concept of operations, or security standards. As a result, implementation of security requirements across ATC development efforts is sporadic and ad hoc. Of the six current ATC system development efforts that we reviewed, four had security requirements, but only two of the four developed their security requirements based on a risk assessment. Without security requirements based on sound risk assessments, FAA lacks assurance that future ATC systems will be protected from attack. Further, with no security requirements specified during systems design, any attempts to retrofit security features later will be increasingly costly and technically challenging. An FAA June 1993 report to the Congress on information security states that because FAA lacks a security architecture to guide the development of ATC security measures, technical security requirements will be retrofitted or not implemented at all because the retrofit "could be so costly or technically complex that it would not be feasible."[12]

In April 1996, the Associate Administrator for Research and Acquisitions established the National Airspace Systems (NAS) Information Security (NIS) group to develop, along with other security initiatives, the requisite security architecture, security concept of operations, and security standards. The NIS group has developed a mission need statement that asserts that "information security is the FAA mission area with the greatest need for policy, procedural, and technical improvement. Immediate action is called for, to develop and integrate information security into ATC systems throughout their life cycles." FAA has estimated that it will cost about $183 million to improve ATC information security. The NIS group has developed an action plan that describes each of its proposed improvement activities. However, over 2 years later it has not developed detailed plans or schedules to accomplish these tasks.

As FAA modernizes and increases system interconnectivity, ATC systems will become more vulnerable, placing even more importance on FAA's

[12]Report to Congress, Air Traffic Control Data and Communications Vulnerabilities and Security, Report of the Federal Aviation Administration Pursuant to House-Senate Report Accompanying the Department of Transportation and Related Agencies Appropriations Act, 102-639, June 1, 1993.

ability to develop adequate security measures. These future vulnerabilities are well documented in FAA's information security mission need statement and also in reports completed by the President's Commission on Critical Infrastructure Protection.[13] The President's Commission summary report concluded that the future ATC architecture appears to have vulnerabilities and recommended that FAA act immediately to develop, establish, fund, and implement a comprehensive systems security program to protect the modernized ATC system from information-based and other disruptions, intrusions, and attacks. It further recommended that this program be guided by the detailed recommendations made in the NAS vulnerability assessment.

FAA's Management Structure Is Not Effectively Implementing and Enforcing Computer Security Policy

FAA's management structure and implementation of policy for computer security has been ineffective: the Office of Civil Aviation Security has not adequately enforced the security policies it has formulated; the Office of Air Traffic Services has not adequately implemented security policy for operational ATC systems; and the Office of Research and Acquisitions has not adequately implemented policy for new ATC systems development. For example, the Office of Civil Aviation Security has not enforced FAA policies that require the assessment of physical security controls at all ATC facilities and vulnerabilities, threats, and safeguards for all operational ATC computer systems; the Office of Air Traffic Services has not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards; and the Office of Research and Acquisitions has not implemented the FAA policy that requires it to include, in specifications for all new ATC modernization systems, requirements for security based on risk assessments.

FAA established a central security focal point, the NIS group, to develop additional security guidance (i.e., a security architecture, a security concept of operations, and security standards), to conduct risk assessments of selected ATC systems, to create a mechanism to respond to security incidents, and to provide security engineering support to ATC system development teams. The NIS group includes members from the Offices of Civil Aviation Security, Air Traffic Services, and Research and Acquisitions.

[13]The President's Commission on Critical Infrastructure Protection (PCCIP) was established in July 1996, in Executive Order 13010, to assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. As a supplement to the transportation assessment, the PCCIP conducted a vulnerability assessment of the NAS architecture.

Establishing a central security focal point is a practice employed by leading security organizations. In order to be effective, the security focal point must have the authority to enforce the organization's security policies or have access to senior executives that are organizationally positioned to take action and effect change across organizational divisions. One approach for ensuring that a central group has such access at FAA would be to place it under a Chief Information Officer (CIO) who reports directly to the FAA Administrator. This approach is consistent with the Clinger-Cohen Act,[14] which requires that major federal departments and agencies establish CIOs who report to the department/agency head and are responsible for implementing effective information management.

FAA does not have a CIO reporting to the Administrator. Although the NIS group has access to certain key Associate Administrators (e.g., the Associate Administrator for Civil Aviation Security and the Associate Administrator for Research and Acquisitions), it does not have access to the management level that can effect change across organizational divisions (e.g., FAA's Administrator or Deputy Administrator). Thus, there is no assurance that the NIS group's guidance, once issued, will be adequately implemented and enforced, that results of its risk assessments will be acted upon, and that all security breaches will be reported and adequately responded to. Until existing ATC computer security policy is effectively implemented and enforced, operational and developmental ATC systems will continue to be vulnerable to compromise of sensitive information and interruption of critical services.

In addition, OMB Circular A-130, Appendix III, requires that systems, such as ATC systems, be accredited by the management official who is responsible for the functions supported by the systems and whose mission is adversely affected by any security weaknesses that remain (i.e., the official who owns the operational systems). At FAA, this management official is the Associate Administrator for Air Traffic Services. However, FAA's ATC systems authorizing official is the Associate Administrator for Civil Aviation Security, who does not own the operational ATC systems.

Conclusions

Since physical security is the agency's first line of defense against criminal and terrorist attack, failure to strengthen physical security controls at ATC towers, TRACONs, and en route centers places property and the safety of the flying public at risk. Information system security safeguards, either those now in place or those planned for future ATC systems, cannot be fully

[14]The 1996 Clinger-Cohen Act, Public Law No. 104-106, section 5125, 110 Stat. 684 (1996).

effective as long as FAA continues to function with significant physical security vulnerabilities. Also, because FAA has not assessed physical security controls at all facilities since 1993, it does not know how vulnerable they are.

Similarly, FAA does not know how vulnerable its operational ATC systems are and cannot adequately protect them until it performs the appropriate system risk assessments and certifies and accredits ATC systems. In addition, FAA is not effectively incorporating security controls into new ATC systems. FAA has taken preliminary steps to develop security guidance by forming the NIS group and estimating the cost to fill this void. However, until this group develops the guidance and the ATC development teams apply it, new ATC system development will not effectively address security issues.

Until FAA's three organizations responsible for ATC system security carry out their computer security responsibilities adequately, sensitive information is at risk of being compromised and flight services interrupted. Moreover, central security groups assigned to assist these organizations can only be successful if they have the authority to enforce their actions or a direct line to top management to ensure that needed changes can be implemented across organizational divisions. At FAA this central security group has neither. Finally, FAA's designated ATC system accrediting authority is inconsistent with federal guidance and sound management practices since this designee is not responsible for the daily operations of ATC systems.

Recommendations

Given the importance of physical security at the FAA facilities that house ATC systems, we recommend that the Secretary of Transportation direct the FAA Administrator to complete the following tasks:

- Develop and execute a plan to inspect the 187 ATC facilities that have not been inspected in over 4 years and correct any weaknesses identified so that these ATC facilities can be granted physical security accreditation as expeditiously as possible, but no later than April 30, 1999.
- Correct identified physical security weaknesses at inspected facilities so that these ATC facilities can be granted physical security accreditation as expeditiously as possible, but no later than April 30, 1999.
- Ensure that the required annual or triennial follow-up inspections are conducted, deficiencies are promptly corrected, and accreditation is kept current for all ATC facilities, as required by FAA policy.

Given the importance of operational ATC systems security, we recommend that the Secretary of Transportation direct the FAA Administrator to complete the following tasks:

- Assess, certify, and accredit all ATC systems, as required by FAA policy, as expeditiously as possible, but no later than April 30, 1999.
- Ensure that all systems are assessed, certified, and accredited at least every 3 years, as required by federal policy.

To improve security for future ATC modernization systems, we recommend that the Secretary of Transportation direct the FAA Administrator to ensure that

- specifications for all new ATC systems include security requirements based on detailed security assessments by requiring that security requirements be included as a criterion when FAA analyzes new systems for funding under its acquisition management system and
- the NIS group establishes detailed plans and schedules to develop a security architecture, a security concept of operations, and security standards and that these plans are implemented.

We further recommend that the Secretary report FAA physical security controls at its ATC facilities, operational ATC system security, and the lack of information security guidance (e.g., a security architecture, a security concept of operations, and security standards) as material internal control weaknesses in the department's fiscal year 1998 FMFIA report and in subsequent annual FMFIA reports until these problems are substantially corrected.

Finally, we recommend that the Secretary of Transportation direct the FAA Administrator to establish an effective management structure for developing, implementing, and enforcing ATC computer security policy. Given the importance and the magnitude of the information technology initiative at FAA, we are expanding on our earlier recommendation that a CIO management structure similar to the department-level CIOs as prescribed in the Clinger-Cohen Act be established for FAA[15] by recommending that FAA's CIO be responsible for computer security. We further recommend that the NIS group report to the CIO and that the CIO direct the NIS group to implement its plans. In addition, we recommend

[15]Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization (GAO/AIMD-97-30, Feb. 3, 1997) and Air Traffic Control : Immature Software Acquisition Processes Increase FAA System Acquisition Risks (GAO/AIMD-97-47, Mar. 21, 1997).

that the CIO designate a senior manager in Air Traffic Services to be the ATC operational accrediting authority.

We made two additional recommendations pertaining to operational ATC systems security in our "Limited Official Use" report.

Agency Comments and Our Evaluation

The Department of Transportation provided written comments on a draft of our "Limited Official Use" report. In summary, the department recognized that facility, systems, and data security are critical elements in FAA's management of the nation's ATC systems and that adequate physical security controls are important to ensure the safety of employees and ATC systems. The department agreed that required FAA inspections should be completed and said that immediate action had been directed to inspect and, where appropriate, accredit the 187 facilities identified in the draft report, that inspections had already been completed for about 100 of these facilities, and that completion of the remaining inspections was expected by June 1998.

However, the department did not state what, if any, specific action it would take on the remaining 14 recommendations. Further, while the department did not dispute any of the facts presented, it offered alternative interpretations of some of them. For example, the department did not agree that FAA's management of computer security has been inappropriate or that ATC systems are vulnerable to the point of jeopardizing flight safety. In addition, the department stated that the report does not present a complete picture regarding decisions guiding FAA resource allocation in that it does not recognize the basis for FAA decisions to allocate resources to other concerns facing FAA, rather than to correcting computer security vulnerabilities. We do not agree with these alternative interpretations.

As discussed in the report, FAA's management of facility, systems, and data security is ineffective for the following reasons:

- Known physical security weakness persist at many ATC facilities, and FAA is unaware of weaknesses that may exist at another 187 facilities.
- FAA has not analyzed the threats and vulnerabilities, or developed safeguards to protect 87 of its 90 operational ATC computer systems and 8 of its 9 operational ATC telecommunications networks.
- FAA does not have a well-defined security architecture, a security concept of operations, or security standards, and does not consistently include

well formulated security requirements in specifications for new ATC systems.

- None of the three organizations responsible for ATC security have discharged their respective security responsibilities effectively: the Office of Civil Aviation Security has not adequately enforced FAA policies that require the assessment of (1) physical security controls at all ATC facilities and (2) vulnerabilities, threats, and safeguards of all operational ATC computer systems; the Office of Air Traffic Services has not implemented FAA policies that require it to analyze all ATC systems for security vulnerabilities, threats, and safeguards; and the Office of Research and Acquisitions has not implemented FAA policy that requires it to formulate requirements for security in specifications for all new ATC modernization systems.

FAA has recognized for several years that its vulnerabilities could jeopardize, and have already jeopardized, flight safety. In its 1994 Telecommunications Plan, FAA states that vulnerabilities that can be exploited in aeronautical telecommunications potentially threaten property and public safety. Vulnerabilities that have jeopardized flight safety are discussed in our "Limited Official Use" report.

Finally, making judicious decisions regarding resource allocation requires a thorough understanding of relative levels of risk, as well as reliable estimates of costs. As we have reported, FAA has not fully assessed its security vulnerabilities and threats and does not understand its security risks. Further, since it has not formulated countermeasures, it cannot reliably estimate the cost to mitigate the risks. As a result, FAA has no analytical basis for its decisions not to allocate resources to security. In recent years, FAA has invested billions of dollars in failed efforts to modernize its ATC systems while critical security vulnerabilities went uncorrected.

The department's comments and our detailed evaluation of them are presented in our "Limited Official Use" report.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from its date. At that time, we will send copies to the Secretary of Transportation; the Director, Office of Management and Budget; the Administrator, Federal Aviation Administration; and interested congressional committees. Copies will be available to others upon request. If you have any questions about

this report, please call me at (202) 512-6253. I can also be reached by e-mail at *willemssenj.aimd@gao.gov*. Major contributors to this report are listed in appendix I.

Joel C. Willemssen
Director, Civil Agencies Information Systems

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Dr. Rona B. Stillman, Chief Scientist for Computers and Telecommunications
Keith A. Rhodes, Technical Director
Randolph C. Hite, Senior Assistant Director
Colleen M. Phillips, Assistant Director
Hai V. Tran, Technical Assistant Director
Nabajyoti Barkakati, Technical Assistant Director
David A. Powner, Evaluator-in-Charge
Barbarol J. James, ADP/Telecommunications Analyst

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested