

STATEMENT OF MARTIN T. POZESKY, ASSOCIATE ADMINISTRATOR FOR SYSTEM ENGINEERING AND DEVELOPMENT, FEDERAL AVIATION ADMINISTRATION, BEFORE THE HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY, SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS, CONCERNING COMPLIANCE WITH THE COMPUTER SECURITY ACT. JULY 10, 1990.

Mr. Chairman and Subcommittee Members:

It is a pleasure to appear before you today to discuss the FAA's response to the recent GAO report on computer security as well as our overall compliance with the Computer Security Act of 1987. Accompanying me today is our National Program Manager for Automated Information Systems Security, Steven D. Smith.

As a safety regulatory agency, the FAA takes seriously its responsibility to provide a safe and efficient air transportation system. Critical to our success is a massive array of computer systems for our communication, navigational, and radar facilities used to safely control the flow of aircraft in the national airspace system (NAS).

As this Subcommittee well knows, the FAA is approaching the end of the National Airspace System Plan (NAS PLAN), which charted the procurement and installation of major equipment systems over a 10-year period. The NAS Plan is well on its way to full implementation--first deliveries have been made in more than 80 percent of NAS Plan projects. We are at a crossroads in committing ourselves to developing systems and equipment that will extend our leadership in world aviation well into the 21st century. The security of our new systems as well as compliance

with the Computer Security Act remains a high priority, since the security of each system can only enhance aviation safety. As requested in your letter of invitation, I have attached to my prepared statement, as Appendix A, a time schedule showing planned versus actual implementation for our sensitive information systems.

While we do not concur with all of the GAO findings with respect to the FAA's compliance posture with the Computer Security Act, we believe that their report will be of valuable assistance in making additional improvements to our computer security programs. We concur with their finding that our computer security efforts were strengthened by the planning process required by the Computer Security Act. The planning process helped focus efforts on specific areas of concern, including risk analysis and software security controls. It further heightened senior management awareness of the need for computer security in both administrative and operational systems.

Specifically, GAO identified six computer security control areas, involved in the control of air traffic, as having less than full implementation. I would like to briefly outline for you the status of each of those areas identified in the GAO report as being not fully implemented.

1. DATA INTEGRITY AND VALIDATION CONTROLS: All active systems handling operational (air traffic control related) information

currently have data integrity controls in place, i.e. data must be presented at a specific rate and in a particular format to be accepted. If the specific rate and particular format are not presented correctly, data will be rejected and systems will await re-transmission or next transmission of data. Data integrity checks have been in place throughout the life cycle of current NAS operational systems. Data validation and integrity checks are also included within the plans for the Advanced Automation System (AAS), which is designed to upgrade air traffic control computer technology.

2. PRODUCTION, INPUT/OUTPUT CONTROL: These are nothing more than procedural controls in place to ensure air traffic control requirements are met. These requirements are coordinated with the operational service prior to completion of the deployment readiness review process. Some of the older systems were not subject to these controls and reviews. All future systems must comply with the deployment readiness review process.

3. RISK/SENSITIVITY ASSESSMENT: The FAA currently uses either the Los Alamos Vulnerability Assessment package or short form risk analysis package to accomplish this. Virtually every NAS operational site and system has been evaluated and every generic type of NAS operational system has received a risk analysis.

4. SECURITY SPECIFICATIONS: All NAS Plan systems currently being developed are evaluated throughout the developmental process to ensure compliance with security control requirements. Some older systems are still operational and were developed prior to the requirement of security controls. These systems are generally being phased out and replaced with updated systems which meet the security requirements necessary for compliance with current automated information systems security orders.

5. DESIGN REVIEW AND TESTING: This area is also covered through the deployment readiness review process. FAA airway facilities staff play an important part in the integration of the systems to ensure total systems integrity.

6. CERTIFICATION/ACCREDITATION: The FAA has developed system accreditation guidelines which are currently being implemented throughout the Agency. All NAS systems will be accredited by the end of fiscal year 1991.

As you know, the Computer Security Act required Federal agencies to identify each computer system which contained sensitive information and to prepare a plan for the security of each system. We received guidance through OMB Bulletin No. 88-16 and attendance at an implementation seminar conducted by the National Institute of Standards and Technology, in July 1988.

The OMB Bulletin No. 88-16 in essence stated that the key to the security plan submission process was in the identification of systems, where agencies must draw logical boundaries around such systems for planning and reporting purposes. The bulletin also indicated that agencies should aggregate systems which have essentially the same function, characteristics, and security needs.

Pursuant to OMB guidance and existing agency documentation, the FAA identified and submitted security plans to the Office of the Secretary of Transportation for submission to the National Institute of Standards and Technology. Our NAS security is based on a total systems approach. However, in order to adequately identify and plan for security, we grouped the NAS applications into five separate security plans which performed similar functions. These functions are consistent with those identified in the existing and more comprehensive NAS Plan.

The FAA has numerous applications which are processed on similar computers with similar functions. For example, the En Route and Terminal Air Traffic Control System consists of applications associated with the control of aircraft in the en route and terminal environment. Specific applications covered by this plan include the central flow control complex, central altitude reservation facility, Automated Radar Tracking System, traffic management processor, flight service automation system and the Host Computer (IBM-3084). Since all of these applications perform

similar functions at multiple sites they were aggregated into one system security plan.

Our security system plans were either identified as general ADP support systems or special purpose major applications. General ADP support systems, included those used for management of FAA resources, administrative data processing, and systems used for training and engineering support not related to air traffic control. Special purpose major applications included all operational systems involved in air traffic control. The agency identified a total of 13 system plans which fell into one of the two major categories. Five security plans were submitted for the major NAS applications systems and eight for the general ADP support systems.

The agency's overall computer security plan was revitalized with the signing of FAA Order 1600.54B on February 7, 1989. It was developed to ensure the protection of all sensitive and nonsensitive automated information systems. The order assigned responsibilities and provided detailed guidance to ensure that the proper safeguards are in place for every operational and administrative automated system. The scope of the order includes all hardware, software and telecommunications that are owned, operated, or under the authority of the FAA.

The order also established guidelines and procedures on contingency planning, risk analysis and certification of sensitive

systems/applications. It also recommended the necessary environmental safeguards to protect all information from unauthorized disclosure and established specific guidelines for connectivity of telecommunications for FAA systems worldwide.

In an effort to make the accreditation process of computer systems as straight forward as possible, the agency published the Automated Information System Security Accreditation Guidelines in November 1989. Efforts to establish a methodology for certification of sensitive systems and applications has been supplemented by contractor support. Finally, in an on-going effort to promote computer security awareness, the Automated Information Security Branch in the Office of Civil Aviation Security has conducted numerous briefings on the accreditation process, conducted classes on risk assessments and provided written, video and other guidance throughout the agency.

Because of the FAA's reliance on computer technology to maintain and enhance aviation safety, I want to assure this Subcommittee that the FAA is committed to ensuring that proper computer security safeguards are in place to protect the NAS system.

Mr. Chairman, that completes my prepared statement. I would be pleased to answer any questions you may have.