GAO

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

161182

Accounting and Information
Management Division

B-280997

September 14, 1998

The Honorable Constance A. Morella
Chairwoman, Subcommittee on Technology
Committee on Science
House of Representatives

Subject: Responses to Questions on FAA's Computer Security and Year 2000 Program

Dear Ms. Chairwoman:

In response to your August 14, 1998, letter, we are providing the enclosed responses to your questions following our August 6, 1998, testimony on the Federal Aviation Administration's (FAA) management of technology issues (GAO/T-AIMD-98-251). These responses cover two areas–FAA's computer security and Year 2000 program.

If you or your staff have further questions or would like to discuss our responses in more detail, please call me at (202) 512-6253. I can also be reached by e-mail at *willemssenj.aimd@gao.gov*.

Sincerely yours,

Joel C. Willemssen
Director, Civil Agencies Information Systems

Enclosure

161182

RESPONSES TO QUESTIONS ON COMPUTER SECURITY AND THE YEAR 2000 COMPUTING CRISIS

Question 1: Why are risk assessments so essential in the design of new Air Traffic Control (ATC) systems?

GAO Response: Risk assessments identify and evaluate system vulnerabilities and are the basis for specifying future ATC systems security requirements. Without knowing the specific vulnerabilities of its new ATC systems, FAA cannot adequately protect them from attack. We recently reported that leading information security organizations use risk assessments to identify and manage security risks confronting their organizations.[1]

Question 2: To what computer security standards is the FAA building its ATC systems?

GAO Response: FAA does not have a common set of security standards to which all new ATC systems are being built. As a result, implementation of security requirements across ATC development efforts is sporadic and ad hoc.

Question 3: What role should the National Airspace System Infrastructure Management System play in protecting critical airspace infrastructure?

GAO Response: The National Airspace System Infrastructure Management System, FAA's future remote monitoring and maintenance system, will play a vital role in protecting the future ATC network since it will provide connectivity to many systems. Therefore, it is essential that this system have adequate access controls to protect against unauthorized access and an intrusion detection capability to detect unauthorized access should it occur. FAA has made progress in building security features into this system and the process it used to derive security requirements is reasonable. However, although the National Airspace System (NAS) Infrastructure Management System is to be a critical system in the future ATC network, it is only one of many future systems, and not all future development efforts are using a similar approach to address systems security. Therefore, it is essential that all future ATC systems address systems security in a comparable manner.

[1] Executive Guide: Information Security Management – Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Question 4: Will FAA be able to adapt its systems security to protect it from evolving threats?

GAO Response: FAA will be better positioned to protect its systems from the evolving threat if it strengthens its current computer security program. In May 1998, we issued a report that specified a series of recommendations to do just that.[2] These recommendations addressed ATC facilities' physical security, operational systems information security, and future systems modernization security. In addition, we recommended that FAA establish an effective management structure for developing, implementing, and enforcing ATC computer security policy. FAA's ability to adapt its systems security to an appropriate level will depend on how effectively it implements these recommendations.

Question 5: What is FAA doing, and what has been accomplished to date, relative to the planning requirements of Presidential Decision Directive 63 for a comprehensive National Airspace System Security Program? In your opinion, will the November 18 due date of the Directive be met?

GAO Response: According to the Department of Transportation's Commissioner on the President's Commission on Critical Infrastructure Protection, as of September 4, 1998, FAA had not provided an official written response on how it plans to comply with instructions in Presidential Decision Directive 63 to develop and implement a comprehensive NAS security program. As our May 1998 report points out, FAA is ineffective in all critical areas of computer security and must strengthen a number of areas to implement a comprehensive NAS security program. It is unrealistic to expect that all these actions will be completed by November 18, 1998; therefore, it is essential that FAA identify and complete those actions that are needed immediately, and complete lower priority actions later.

[2] Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

Question 6: Why were 15 mission-critical air traffic control systems dropped from the list of systems needing repair prior to the July 31 milestone? How was it determined that they no longer needed to be repaired?

GAO Response: Of the 15 mission-critical air traffic control systems removed from the list of systems needing repair prior to the July 31 milestone, FAA reported that

–13 were removed because they were found to be Year 2000 compliant, and thus did not require repair,
–1 was removed because FAA determined that this system would be replaced, instead of repaired, and
–1 was removed because FAA later determined that the system had no Year 2000 issues.

Question 7: When does the FAA plan to run end-to-end tests of all key business processes and supporting systems? How long will this testing take?

GAO Response: FAA plans to perform NAS end-to-end testing beginning in January 1999 and ending by March 31, 1999.

Question 8: Has the FAA included key user groups like the air traffic controllers and professional technicians in the formulation of Year 2000 contingency plans?

GAO Response: When we testified before your committee, on August 6, 1998, FAA had not yet included key user groups in the formulation of its Year 2000 contingency plans. In fact, the National Air Traffic Controllers' Association (NATCA) had expressed concerns about FAA's contingency planning, stating that contingency plans for certain FAA facilities did not adequately define the role of air traffic controllers.

Recently, however, the Year 2000 program manager decided not to issue the Year 2000 NAS Continuity and Contingency Plan in final form by August 31, as planned. Instead, the agency delayed the plan's issue date until December 1998 in order to coordinate with system users.

Question 9: Do the FAA's contingency plans include the possibility of complete systemwide breakdown?

GAO Response: FAA's Draft Year 2000 NAS Continuity and Contingency Plan, dated August 10, 1998, did not include the possibility of a complete systemwide breakdown. However, a Year 2000 program official told us that the agency recently decided to revise its draft plan to incorporate the comments of system users, including the concern that the continuity plans do not currently include the possibility of multifacility breakdowns. FAA now expects to release its continuity and contingency plan in December 1998.

Question 10: Historically, the FAA's track record for completing large computer and software-intensive projects has been very poor. Is it realistic to expect a higher success rate for the agency's Y2K program?

GAO Response: Over the past 15 years, FAA's ATC modernization has experienced cost overruns, schedule delays, and performance shortfalls of large proportions. Because of its complexity, cost, and problem-plagued past, we designated the ATC modernization as a high-risk information technology initiative in 1995 and 1997. Our recent evaluations of the modernization identified some of the root causes of FAA's problems and pinpointed solutions to these longstanding problems. For example, we found that FAA (1) lacked a complete systems architecture–or overall blueprint–to guide systems development and evolution, (2) had weak software acquisition capabilities, (3) used unreliable cost information, and (4) suffered from an organizational culture that did not reflect a strong commitment to focus on its mission. Generally, these issues demonstrate that FAA lacks the organizational structure and process discipline needed to manage complex information technology initiatives.

This structure and discipline are also required to successfully address the Year 2000 computer crisis, a complex management problem. For FAA, it involves managing the repair or replacement and testing of hundreds of complex, software-intensive, and integrated systems. Such an effort requires sound configuration management practices for systems being repaired and mature acquisition processes for systems being replaced. It also involves unprecedented amounts and levels of testing–including unit testing, integration testing, system acceptance testing, and end-to-end testing. As a result, the Year 2000 problem poses a significant challenge to FAA.

Question 11: In terms of a percentage, what is the chance that the FAA will not complete all of its Year 2000 renovation and testing activities before time runs out?

GAO Response: While it is difficult to respond in terms of a percentage, in our August testimony[3] we stated that FAA must still correct, test, and implement many of its mission-critical systems, and that it is doubtful that FAA can adequately do all of this in the time remaining. We made this statement because of the number of systems requiring renovation, the complexity of the agency's renovation and validation efforts, and unresolved issues such as data exchanges and end-to-end testing. When nonmission-critical systems are factored in, FAA's chance of completing all renovation and testing activities is even less likely. Thus, it is critical that FAA prioritize its systems and focus on renovating and thoroughly testing the highest priority systems.

Question 12: Since IBM basically has stated that the life-span of the Host computer system expires in September of this year and GAO has reported that replacement parts for the outdated equipment is virtually non-existent, is it overly optimistic to expect the Host to continue to operate until they are replaced in an additional 12 to 24 months from now?

GAO Response: If the Host replacement is successfully deployed on schedule, it is reasonable to expect that the Host will continue to operate until all replacements are in place. Whereas FAA estimates that the Host and Oceanic Computer System Replacement will be operating in 20 en route centers by October 1999, the agency anticipates that its current inventory of spare parts together with parts to be cannibalized from Host processors located at its training and technical support centers will allow it to maintain existing Host systems through 2001.

(511261)

[3] FAA Systems: Serious Challenges Remain in Resolving Year 2000 Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

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