



## GOVERNMENT

### GAO beats drum of warning

By Richard Power

In testimony delivered to the U.S. House of Representatives' Subcommittee on Technology in August, Joel C. Willemssen of the U.S. General Accounting Office (GAO) warned of serious problems in the Federal Aviation Administration (FAA), involving both Y2K and computer security issues.

"FAA has made progress in managing its Y2K problem and has completed critical steps in defining which systems need to be fixed and how to fix them. However, with less than 17 months to go, FAA must still correct, test and implement many of its mission-critical systems. It is doubtful that FAA can adequately do all of this in the time remaining. Accordingly, FAA must determine how to ensure continuity of critical operations in the likely event of system failures.

"FAA cannot provide assurance that the air traffic control systems on which it depends are sufficiently resistant to intrusion. FAA's weak computer security practices were detailed in the classified version of a report we made available in May to key congressional committees and appropriate agency officials. An unclassified version of the report is available to the public.

"Underlying weaknesses in FAA's management have allowed the agency's Y2K, computer security, and other information technology problems to persist. Our work over the last two years has identified some of the root causes of, and pinpointed solutions to, these long-standing problems—including an incomplete systems architecture, weak software acquisition capabilities, unreliable cost information, and a problematic organizational culture. Although FAA has initiated efforts in response to some of our recommendations on these issues, most of them have not been fully implemented."

#### Weak practices degrade safety

Willemssen's testimony on the FAA's computer security problems offers many sobering lessons.

Consider the following remarks and ask yourself how well your organization would measure up under such scrutiny.

"In assessing the adequacy of computer security at FAA earlier this year, we found significant weaknesses that compromise the integrity of FAA's air traffic control (ATC) operations. This review resulted in a number of findings to sensitive to discuss in open hearings.

"FAA's ATC network is an enormous collection of interrelated systems that reside at or are associated with hundreds of ATC facilities. The systems and facilities are interconnected by complex communications networks that separately transmit both voice and digital data.

"It is essential that FAA's approach to computer security be comprehensive and include the following three ele-

ments: physical security of the facilities that house ATC systems (e.g., locks, guards, fences and surveillance), information security of the systems (e.g., safeguards incorporated into computer hardware and software) and telecommunications security of the networks linking the systems and facilities (e.g., secure gateways, firewalls and communications-protection devices).

"FAA had significant weakness in every area of computer security that we investigated: physical security, operational systems security, development of new systems and FAA's management structure and implementation of computer security policy.

*ATC physical security management and controls are ineffective:* "The agency's management of physical security at its ATC facilities has been ineffective. Known physical weaknesses exist at many facilities.

*ATC operation systems security is ineffective and systems are vulnerable:* "According to FAA's latest information, less than 10 percent of its operational systems—seven out of 90—have undergone risk assessments. As a result, FAA does not know how vulnerable these operational systems are and consequently has no basis for determining how to best protect them."

*FAA is not effectively incorporating security features into new ATC systems:* "FAA has no security architecture, concept of operations or standards. As a result, implementation of security requirements across ATC development is sporadic and ad hoc. With no security requirements specified during systems design, any attempt to retrofit such features later will be increasingly costly and technically challenging."

*FAA's management structure is not effectively implementing or enforcing computer security policy:* "Civil Aviation Security has not adequately enforced security policies it has formulated, Air Traffic Services has not adequately implemented security policy for operational ATC systems, and Research and Acquisitions has not adequately implemented policy for new ATC system development."

*Problems persist because FAA's management of its information technology is ineffective:* "Our recent reviews have identified some of the root causes...ATC systems architecture is incomplete, ATC software acquisition capabilities are weak, ATC cost information is unreliable and FAA's organizational culture is problematic."

#### Testimony poignant in its obscurity

The unclassified versions of both "Air Traffic Control: Weak Computer Security Jeopardize Flight Safety," (GAO/AIMD-98-155) and its companion study, "Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations" (GAO/AIMD-98-145) tell a compelling story.

As GAO officials testified on these lapses, rescue teams were pulling bodies from the rubble at U.S. embassies in Kenya and Tanzania in the aftermath of terrorist bombings—poignantly illustrating the danger of weak physical security. The lead story of the day, however, was Kenneth Starr's bizarre obsession with sexual alliances and possible perjury in a dismissed civil case. Even news of the terrorist strikes was overshadowed; the drum-beat of the GAO's dire warning of tangible, imminent danger was barely audible.