United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Committee on Science, and the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Thursday,
September 9, 1999

# YEAR 2000 COMPUTING CHALLENGE

# FAA Continues to Make Important Strides, But Vulnerabilities Remain

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO
Accountability * Integrity * Reliability

GAO/T-AIMD-99-285

Ms. Chairwoman, Mr. Chairman, and Members of the Subcommittees:

We appreciate the opportunity to testify today on the Federal Aviation Administration's (FAA) efforts to address the Year 2000 (Y2K) problem. With a little over 100 days remaining until January 1, 2000, the Y2K computing problem is at the forefront of the world's information technology challenges and is especially crucial to FAA.

Hundreds of critical computer systems make FAA's operations possible. FAA uses these systems to control air traffic, target airlines for inspection, and provide up-to-date weather conditions to pilots and air traffic controllers. However, many of these systems could fail to perform as needed when using dates after 1999 unless proper date-related calculations can be ensured. Should systems fail or malfunction, hundreds of thousands of people could be affected through customer inconvenience, increased airline costs, grounded or delayed flights, or degraded levels of safety.

My statement today will focus on four topics: (1) FAA's progress to date, (2) challenges FAA faces in ensuring that its internal systems will work, (3) risks associated with external organizations—focusing specifically on airports, airlines, and international entities, and (4) the critical need for business continuity and contingency plans that identify how aviation operations will continue should systems fail. Our review of FAA's Y2K program was performed in accordance with generally accepted government auditing standards from March through September 1999. We performed our work at FAA headquarters and facilities in Washington, D.C., and at facilities in Atlanta, Georgia; Dallas, Texas; and Denver, Colorado. We obtained comments on a draft of this testimony from FAA officials and incorporated these comments where appropriate.

In brief, FAA and its employees have made excellent progress in tackling the monumental Y2K problem. The agency is now reporting that all of its systems are ready for the year 2000. However, FAA's work is not yet done. The agency continues to face challenges in ensuring that its internal systems will work as intended through the Y2K date change. These challenges involve managing modifications to compliant systems, independent verification of systems' compliance, and systems testing. FAA must also mitigate risks posed by external organizations, including airports, airlines, and foreign air traffic control systems. These factors could impede FAA's ability to provide reliable aviation services, which could seriously affect the flow of air traffic across the nation and around the world. In the event that critical internal or external systems do not

work as intended, FAA must have a comprehensive and tested business continuity and contingency plan ready to implement and train its staff in how to do so.

## FAA Has Made Excellent Progress in Its Y2K Readiness

Over the past year and a half, FAA has made substantial progress. In January 1998, the agency had no central Y2K program management; an incomplete inventory of mission-critical systems; no overall strategy for renovating, validating, and implementing mission-critical systems; and no milestone dates or schedules.[1] At that time, we recommended that FAA provide its Y2K program manager with the authority to enforce policies; outline FAA's overall strategy for addressing the Y2K date change; complete inventories of all information systems and interfaces; set priorities; establish plans for renovating, validating, and testing all converted and replaced systems; and develop Y2K business continuity and contingency plans to ensure the continuity of critical operations.

FAA has addressed our recommendations. The agency established a strong Y2K program office, and tasked it with providing leadership—guidance and oversight—to FAA's business lines and aviation industry partners. The program office established (1) an overall Y2K strategy, (2) detailed standards and guidance for renovating, validating, and implementing mission-critical systems, (3) a database of schedules and milestones for these activities, and (4) a Y2K business continuity and contingency plan. The agency has also worked to repair or replace systems with date-related problems, test these systems, and implement these repairs and replacements in air traffic control facilities throughout the nation.

Recently, the Department of Transportation (DOT) announced that—as of June 30—100 percent of FAA's systems were fully Y2K compliant. Specifically, DOT stated that FAA had completed Y2K work on 424 mission-critical systems and 204 nonmission-critical systems. The department also reported that data verifying the compliance of all FAA systems had been examined and approved by Science Applications International Corporation (SAIC), an independent verification and validation (IV&V) contractor. DOT also noted that its Inspector General had examined a sample of systems and approved FAA's work.

[1] *FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically* (GAO/AIMD-98-45, January 30, 1998).

Last month, FAA revised its Y2K project plan to identify key efforts for the remaining months before January 1, 2000. One key activity involves ensuring that systems that have been certified Y2K compliant maintain this status through a change-control process. Other activities include testing contingency plans and training systems users in how to implement them, if necessary. According to FAA, the agency is also having two independent contractors analyze selected compliant systems' code for any date problems.

## Evidence Supports Systems Implementation

To manage the deployment of hundreds of systems' Y2K-related changes in facilities across the nation, FAA's Y2K program office established implementation standards. These standards require system owners to complete a system's Y2K certification, and, as applicable, test the system at key sites and deploy it nationally. When the system is implemented at every facility, system owners are then required to prepare a Y2K implementation results report. Once this report has been approved within the relevant business line, FAA's IV&V contractor reviews it and other key implementation documents. Upon successful completion of this review, the system is considered implemented.

When we last testified on this topic in March 1999,[2] FAA estimated it had yet to complete roughly 4,500 implementation "events"—each one entailing the activation of a single system at a single site. FAA subsequently reported that it completed this task on June 30, 1999.

To evaluate this effort, we reviewed implementation evidence for 18 mission-critical air traffic systems[3] that were installed at one or more of 8 different facilities—totaling 49 implementation events in all. In evaluating implementation evidence, we reviewed hard copy and automated maintenance records to determine if the Y2K modification had been completed, and sought to identify compliant version numbers on system

[2] *Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain* (GAO/T-AIMD/RCED-99-118, March 15, 1999).

[3] In choosing systems, we attempted to cover a range of air traffic control functions in different environments. We selected implemented systems from three different critical core functions (surveillance, weather information processing, and communications) that operate in one or more of the different air traffic control environments (en route, terminal, tower, and flight service station). Seven of these systems were also chosen because they were among the 26 systems identified by FAA as posing the greatest risk to the National Airspace System.

consoles where possible. To the extent they were available, we also interviewed local technicians who implemented the modifications. We did not validate the effectiveness of the Y2K repairs.

We found sufficient documentation supporting the implementation of these systems in all cases where this evidence was required. Of the 49 events, 39 required an entry in the maintenance records and 10 did not. The 39 events that required an entry were all documented in the facilities' maintenance records. Additionally, we viewed compliant version numbers on backup console screens for 18 of the events. In some cases, we could not view the console screens because the system was on-line supporting air traffic control operations and would have had to be taken off-line for us to see version numbers.

Of the 10 events that did not require an entry in the maintenance records, 5 were associated with leased systems, 2 were associated with prototype systems, and 3 were associated with systems that were not in operation at the facilities. FAA technicians explained that leased systems are maintained, monitored, and operated by a contractor—and thus are not tracked in FAA's maintenance records. Similarly, the prototype systems we evaluated were maintained and managed by the National Aeronautics and Space Administration, and so were also not tracked in FAA's maintenance records. Of the three systems that were not in operation at the facilities we visited, two had been decommissioned and one was maintained and managed at a distant location.

## FAA's Year 2000 Efforts Face Important Challenges

FAA faces several challenges that could affect its activities through the Y2K date change. These include addressing

- changes to compliant systems that could introduce new Y2K problems,
- independent verification efforts that were not documented, and
- end-to-end testing efforts that were not comprehensive.

## Changes to Compliant Systems Increase Risks of Y2K-Related Failures

As noted in our January 1999 testimony, changes made to systems after they have been certified as Y2K compliant can introduce new Y2K problems.[4] To address this risk, we suggested the federal government adopt a strong Y2K change management policy—one that limits new software and systems changes. As an example of such a policy, we noted that the Social Security Administration had issued a moratorium on new systems changes on commercial-off-the-shelf and mainframe products from July 1, 1999 through March 31, 2000, and on programmatic applications from September 1, 1999 through March 31, 2000. We, therefore, suggested that the Office of Management and Budget (OMB) consider directing agencies to implement such a policy.

In response to our suggestion, in May, OMB issued a memo to federal department heads stating the importance of considering the potential effect of changes to information technology systems on Y2K readiness, and urging agency heads to adopt a policy that only allows system changes where absolutely necessary. OMB also requested that agency heads summarize how they would implement such guidance in their quarterly Y2K progress reports.

In its August 1999 quarterly report to OMB, DOT responded that it had a formal policy in place that required critical software and hardware modifications to be supported by formal, documented change control procedures. DOT also stated that on July 23, 1999, its Deputy Chief Information Officer (CIO) issued a memorandum calling for all operating administrations to examine any decision to proceed with new requirements or modifications to Y2K-compliant systems and to defer such modifications until after the Y2K date change, if possible.

Prior to the Deputy CIO's memo, on May 28, FAA established a policy calling for system owners to assess whether any completed modification to a Y2K-compliant system might affect the system's compliance or its ability to process dates, and to disclose this information in a Y2K Certified System Change Report to their lines of business and the Y2K program office. According to the policy, if, as a result of this assessment, a modification were determined to have an impact on date processing or Y2K compliance, the system would have to be revalidated, recertified Y2K compliant, and reimplemented.

[4] *Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions* (GAO/T-AIMD-99-50, January 20, 1999).

Although FAA recognized the criticality of controlling systems changes and established a policy for doing so, the agency has not yet effectively implemented this policy. As of August 24, FAA Y2K program officials told us that they had received three Y2K Certified System Change Reports and that they were following up on another four system modifications identified by the Inspector General that did not have supporting change reports. However, when we requested a list of all system modifications logged in FAA's Maintenance Management System (MMS)—the agency's national database of systems modifications, maintenance actions, and interruptions—from July 1, 1999 (the day after FAA's systems were deemed fully compliant) through August 23, 1999, the resulting printout was 535 pages long. Our preliminary review of this information identified 967 completed system modifications[5] that should have been linked to Certified Y2K Systems Change Reports.[6] For example, on August 15, one facility reported modifying its Digital Bright Radar Indicator Tower Equipment. In another instance, a facility made modifications to its Automated Radar Terminal System. Both of these systems help air traffic controllers maintain adequate separation between aircraft.

Beyond the completed modifications, we identified an additional 239 modifications that had been initiated and were in process. These also should generate change reports when they are completed. For example, on August 3, one facility initiated–but has not yet completed–a software upgrade to its Terminal Doppler Weather Radar.

When asked about the large number of modifications that were not linked to the required change reports, FAA's acting Y2K program manager[7] stated that the program office recently realized that the change-control policy did not specify a deadline by which system owners must file their change reports. The Y2K manager explained that system owners might have

[5]We focused on modifications that had been completed (and so would require a change report), and eliminated entries that stated that (1) the modification was not applicable to the subject facility, (2) this was a delayed entry and the modification had been made prior to June 30, or (3) the change only applied to systems documentation. We also eliminated duplicate entries.

[6]Multiple system modifications may be linked to a single System Change Report because the maintenance management system lists each facility's modifications separately, and several facilities could be implementing the same change.

[7]In July 1999, FAA's Y2K program manager accepted a different position in the agency; the deputy program manager is serving as acting program manager.

delayed filing change reports because of this lack of a deadline. Yesterday, the Y2K program office modified the policy to require change reports no later than 2 weeks after the system owner assesses the Y2K impact of any system modification.

Additionally, officials in FAA's air traffic services line of business reviewed samples of the 535 pages of systems modifications and stated that they believed many of the modifications had been made prior to June 30, but that the technician did not reflect that in the entry. They stated that they will follow up on every entry in the MMS database to ensure that all modifications are tracked for Y2K compliance, and that in the future, they plan to use the MMS database to help them track all system modifications, including new modifications.

In addition to its change control policy, FAA's Y2K program office allowed each business line to determine if a policy implementing a moratorium on changes to Y2K compliant systems was appropriate for its organization. One organization, the office of the Associate Administrator for Research and Acquisitions (ARA)—which is responsible for developing new air traffic control systems—issued a policy calling for a moratorium on new system changes to certified systems from November 17, 1999 through January 7, 2000, and from February 1, 2000 through March 8, 2000. This policy also establishes a waiver process for mission-critical, safety-related, or other essential modifications required during the moratorium period, and states that waivers will be granted wherever a contract schedule would be affected by the moratorium. The FAA office responsible for operating the National Airspace System (NAS)—the network of equipment, facilities, and information that supports U.S. aviation operations—has drafted a similar policy.

FAA's ARA organization plans to waive the moratorium for at least one system change scheduled to occur during that time frame. The new Standard Terminal Automation Replacement System (STARS), which is to replace aging radar data processing systems, is scheduled to begin operating at the first two facilities in December 1999 and January 2000. The ARA Y2K program manager stated that he plans to grant this system a waiver to allow it to meet its schedule.

Another major change affecting the NAS is scheduled to take place on December 30. This change, called the 56-day national database update, involves updating boundaries between facilities, navigational aids, weather locations, and airways structures throughout the national airspace. This

change coincides with worldwide updating of aeronautical information by the International Civil Aviation Organization (ICAO), the international organization responsible for aviation standards. This updating process occurs regularly throughout the year and, according to an FAA official, has, on occasion, experienced problems. While this change is not expected to affect the Y2K status of systems, any change so soon before the date rollover complicates the process of identifying and correcting problems. FAA officials stated that they explored the possibility of delaying the 56-day update, but decided not to do so because of the safety implications resulting from not updating critical aviation information.

## Lack of Documentation Supporting IV&V Contractor's Efforts Raises Questions About Compliant Systems

As we previously reported, when OMB and the President's Council on Year 2000 Conversion began collecting information on the Y2K progress of federal agencies, they had little assurance that they were receiving accurate information because progress was predominantly based on agency reports that had not been consistently reviewed or verified.[8] In fact, we had found cases in which agencies' reported compliance status was inaccurate. To address this issue, we recommended that the Council require agencies to develop an independent verification strategy. According to OMB, all agencies are now required to independently verify their validation process, and senior managers at all large agencies are now relying on independent verification to provide a double-check that their mission-critical systems will, in fact, be ready for the year 2000.

To respond to this requirement, many agencies hired IV&V contractors to assist in their Y2K work. Such contractors provide quality assurance services ranging from reviewing systems' documentation to independent testing of Y2K repairs. IV&V contractors often perform verification and validation services and summarize their results, together with any qualifications they may have, in the form of interim and final reports.

FAA contracted with SAIC to perform an independent review of each system's documentation throughout key Y2K program phases (assessment, renovation, validation, and implementation) and to report its findings in monthly status reports. The task order stated that SAIC would not be asked to certify that FAA systems were actually Y2K compliant.

[8]GAO/T-AIMD-99-50.

In reviewing FAA's systems, SAIC used standard checklists identifying required documents for each phase, and reported any concerns to the Y2K program office during daily meetings.[9] FAA's acting Y2K program manager stated that agency officials saw these checklists during the meetings, and that the checklists often contained handwritten notes about concerns and how they were resolved. However, when SAIC completed its work and turned its files over to FAA, these handwritten checklists had been removed. Instead, SAIC provided electronic files that lacked a complete history of the concerns and the reviewer's signature.

Without this history, it is difficult to determine if all of the system-specific concerns raised during SAIC's independent review had been addressed. For example, when we reviewed Y2K documentation for the Display System Replacement system,[10] we found that SAIC had reported that there were several unexplained problems that needed to be addressed and retested during the validation phase. Later, SAIC approved the system for implementation, but there is no explanation of how the validation problems were resolved. Similarly, SAIC identified missing and incomplete information on FAA's mission-critical heating, ventilation, and air conditioning (HVAC) system[11] during renovation. SAIC later approved the system's validation and implementation, but we were unable to find any documentation supporting how their renovation concerns had been resolved.

Further, because FAA did not require it, SAIC did not originally provide written interim or final reports summarizing the outcome of its activities, including any issues or crosscutting concerns. Without interim or final IV&V reports, FAA did not have summary evidence that IV&V concerns and issues were raised and satisfactorily addressed. In response to our concern about the lack of an IV&V summary report, FAA's acting Y2K program manager stated that while she was comfortable that all of SAIC's concerns had been addressed, she recognized the value of having a summary

[9]FAA's acting Y2K program manager stated that the agency's daily and weekly meetings with SAIC and the data sheets that were discussed during the meetings satisfied the requirement for monthly status reports.

[10]The Display System Replacement displays radar data to controllers in the en route environment.

[11]HVAC systems are needed to maintain critical air traffic control equipment in normal operating condition.

statement. FAA obtained such a summary statement from SAIC on September 7, 1999.

## End-to-End Testing Valuable, But Not Comprehensive

Integrated, end-to-end testing of multiple systems that have been individually deemed Y2K compliant ensures that the systems that collectively support a core business function will operate as intended. Without such testing, systems individually deemed compliant may not work as expected when linked with other systems in an operational environment. This testing should include not only those owned and managed by an organization, but also any external systems with which they interface.

FAA's end-to-end testing strategy related to the National Airspace System focused on systems that directly support navigation, surveillance, weather, maintenance, and air traffic control functions.[12] FAA conducted three types of Y2K end-to-end testing: system integrity testing, operational demonstration, and field-site testing.

FAA's system integrity tests involved testing groups of systems supporting weather processing, communications, flight- and radar-data processing, and remote maintenance monitoring, to ensure that data were processed correctly across interfaces. To date, FAA has completed five system integrity tests and reported that there were no Y2K-related problems in any of the tests.[13] One of these tests was performed in response to our concern, raised in March 1999, that FAA did not validate the radar tracking functions of its Automated Radar Terminal System (ARTS)-IIIA—a critical data processing system used in about 55 terminal radar approach control facilities.[14] In this system integrity test, FAA compared ARTS-IIIA radar tracking information with two independent tracking systems and found no Y2K-related problems. The information from the three sources was consistent.

[12]FAA also performed system-specific testing prior to certifying each systems' Y2K compliance.

[13]FAA officials stated that they performed a sixth system integrity test, but that the test results report has not yet been completed.

[14]GAO/T-AIMD/RCED-99-118.

FAA's end-to-end operational demonstration simulated having aircraft pass through all phases of flight using recorded data, and tested the activities associated with these phases—such as weather briefings, clearances, aircraft tracking, rerouting, handoffs, and transfers. This test focused on FAA's ability to continue intersystem and interfacility data communications through the Y2K date change. FAA officials reported that they completed this test in February, with no Y2K-related problems.

FAA's field-site testing involved a demonstration of core NAS functions using equipment at operational air traffic control facilities in order to demonstrate that functional components at selected sites were reliable under Y2K conditions. FAA ran this demonstration in a "split environment." That is, the agency used redundant equipment for this demonstration while still controlling live air traffic with its primary air traffic control systems. FAA completed this testing in April and reported it a success.

While these three types of tests are important in demonstrating FAA's Y2K progress in successively increasing increments, the tests were not comprehensive. Specifically, of 21 mission-critical systems[15] that FAA identified as posing the greatest risk to the national airspace system if not operational on January 1, 2000, 13 were not included in any end-to-end testing. These include four weather systems, four communications systems, and five facilities systems. For example, neither the Graphical Weather Display System (GWDS) nor the Terminal Doppler Weather Radar (TDWR) was included in any of the end-to-end tests. Both of these systems are critical to obtaining aviation weather information; GWDS provides graphical weather information to flight service stations while TDWR detects windshear events and reports these events to air traffic controllers.

Additionally, the agency's broadest end-to-end test, the field-site test, was limited in that it took place during low traffic conditions. Further, FAA did not exercise every system or interface in this test. For example, FAA was unable to use the critical Voice Switching and Control System—used for communications between air traffic controllers and pilots—because it could not be set up to operate in both a primary and redundant environment. Also, FAA did not test critical backup systems, such as the Direct Access Radar Channel, which is essential should the Host Computer System—the primary information processing system in an en route

[15]FAA originally identified 26 systems as posing the greatest risk to the national airspace system, but 5 have since been decommissioned.

center—fail. Finally, because FAA's demonstration focused on air traffic control systems, it did not constitute an end-to-end test of all of the key components of the NAS—including mission-critical systems operated by airlines and airports.

FAA officials agreed that their end-to-end tests were not comprehensive, but stated that they had tested many of their most important systems and functions and, therefore, do not plan to conduct additional end-to-end testing. Given the significance of the systems and functions that have not yet been tested end-to-end, FAA should consider performing additional testing in the time remaining before the Year 2000 date change.

## Risks Associated With External Partners Could Affect Aviation Operations

In addition to the challenges FAA faces in ensuring its internal systems will work through the Y2K date change, the agency is at risk that critical external systems will fail, thereby affecting its operations. Three prime areas of risk are airports, airlines, and international partners.

### Many Airports Expected to Complete Y2K Activities Late This Year

The successful operation of the NAS depends, in part, on the equipment that airports use to carry out their operations. This equipment helps provide safe, secure, and efficient aircraft operations and other services to the public; it includes controls for functions such as runway lighting, monitoring access to secured areas, handling baggage, providing emergency communications, and fueling aircraft. Because much of this equipment is automated, it is at risk of Y2K-induced failures and malfunctioning. While airport officials expressed confidence that they could resort to manual operations if automated systems fail, they noted that manual operations could decrease an airport's efficiency—its ability to handle its normal number of scheduled flights per day—thereby causing flight delays. Delays at one airport could have a ripple effect, causing delays at other airports and eventually reducing the efficiency of the system nationwide.

We raised concerns about the Y2K status of our nation's airports in January 1999, when we reported that nearly two-thirds of 334 airports responding to our survey did not plan to complete their Y2K efforts by FAA's recommended June 30 deadline.[16] We also noted that while most of these were small airports, 26 of them were among the nation's 50 largest airports.

More recently, the International Civil Aviation Organization (ICAO) required member countries to report on the Y2K status of their civil aviation systems—including air traffic control systems, airports, and airlines—by July 1, 1999. FAA collected Y2K information on 113 U.S. airports, submitted it to ICAO on June 29, and is continuing to update this information.[17] According to FAA's latest information, about 20 percent of the 113 airports reported that they had completed their Y2K preparations. Another 58 percent estimated that they would complete Y2K efforts by September 30, and the remaining 22 percent of airports either planned on a later date or did not provide an estimated completion date. Among the group planning to complete their Y2K efforts after September 30, but by November 30, are five of the nation's largest international airports.

FAA is also collecting information on the Y2K status of 566 domestic airports' safety systems and 459 airports' security systems—systems that FAA certifies—but this information is not yet complete. FAA officials stated that the agency is requiring information on airports' safety systems by October 15, but had not set a deadline for information on security systems. The agency will continue this information-collection effort through the end of 1999.

To help ensure the safety of airports' systems, on July 1, 1999, FAA proposed a requirement that airports test critical safety equipment early on January 1, 2000. The purpose of this proposed requirement was to have airports test equipment—such as emergency communications systems and fire trucks—that may not be in use during the Y2K date change. Several airports provided comments to FAA on this proposed rule change, and the agency is now evaluating those comments before proceeding to issue the new requirement.

[16] *Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem* (GAO/RCED/AIMD-99-57, January 29, 1999).

[17] On August 31, FAA requested that we treat information on specific airports and airlines as "For Official Use Only" information, meaning that we are unable to report site-specific information in a public forum.

## Many Airlines Expected to Complete Y2K Activities Late This Year

Airlines, another key element of the National Airspace System, also rely heavily on automated systems to provide safe and efficient air transportation. These systems support communications, navigation, flight management, aeronautical information processing, and weather information processing, as well as transponders and engine management.

Responding to ICAO's request for Y2K information on airlines, FAA collected Y2K information on 146 international airlines in April and May 1999, submitted it to ICAO on June 29 and is continuing to update this information. According to FAA's latest information, about 33 percent of the 146 airlines reported that their systems were Y2K compliant. Another 35 percent planned to complete their Y2K efforts by September 30, and the remaining 32 percent either planned on a later date or did not provide any date. Among the group planning to complete their Y2K efforts after September 30, but by December 31, 1999, are four of the nation's major airlines.

FAA is also collecting Y2K status information from over 14,000 FAA-certified air carriers and operators. The agency distributed a questionnaire to certificate-holders in April 1999, and is currently following up with nonrespondents. In addition, FAA inspectors are beginning to ask questions of certificate-holders about their Y2K status. FAA officials stated that they will continue with these efforts through the Y2K date change.

## International Activity and Coordination Is Continuing

American international carriers operate in over 90 countries and at over 200 foreign airports; similarly, over 125 foreign carriers cross FAA-controlled airspace. FAA lacks the authority and resources to ensure compliance of any foreign air traffic control system, but it nevertheless retains responsibility for ensuring safe, reliable aviation services for American travelers into 2000 and beyond.

FAA's international Y2K management team has been active. FAA is sharing information with its foreign counterparts and assisting them in addressing Y2K issues, such as business continuity and contingency planning. FAA is also actively working with ICAO to obtain Y2K status information on its international counterparts, and is prioritizing countries based on perceived risk in order to determine the level of testing to be performed with these countries. FAA reports that it has completed international testing with several countries, and plans to continue these tests throughout 1999.

FAA's Y2K international manager stated that FAA will provide status information on individual countries to the State Department to help develop consular information sheets—previously called travel advisories—regarding ICAO member countries. Both the departments of Transportation and State intend to issue information on individual countries later this month.

## Comprehensive Business Continuity and Contingency Planning Is Crucial

Because of the risk of anticipated and unanticipated Y2K failures—whether from internal systems or due to reliance on external partners and suppliers—comprehensive business continuity and contingency plans are crucial to continuing core operations. We have issued guidance on this topic,[18] and OMB adopted this guidance as the standard that federal agencies are to use in developing their business continuity and contingency plans.

In accordance with this requirement, FAA drafted a Y2K business continuity and contingency plan in December 1998, and released iterations of this plan in April and July 1999. FAA's plan defined its approach to business continuity and contingency planning and focused on developing risk matrices for each of the agency's core business functions. These risk matrices, developed in conjunction with subject matter experts, identify risks, business impact, mitigation strategies, potential triggers, and contingency plans within each core business area.[19] The latest version of the plan also describes FAA's "Day One" strategy—plans and procedures for the time frame immediately before and after the date rollover, business resumption model, and plans for testing the contingency plan and training people in how to use it.

For the portion of the plan that affects the NAS, the "Day One" strategy is a plan for reducing risk from December 31, 1999 through January 1, 2000. This includes the establishment of business resumption teams made up of experts who will be available to address problems, as well as a communications structure for coordinating responses to any problems that arise.

[18] *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19, August 1998). This product was available as an exposure draft in March 1998.

[19] The information in these risk matrices is considered "For Official Use Only" and therefore cannot be discussed in this testimony.

To test and improve the NAS portion of its business continuity and contingency plan, FAA has initiated rehearsal exercises. One such exercise took place last month, and another is scheduled for next month. During these exercises, experts in various facets of aviation operations work through different failure scenarios, determining how they would react and what further activities should be undertaken to better prepare the agency for such failures. These scenarios range from minor to major failures, and include failures of the national infrastructure. FAA officials stated that they will use suggestions generated during these exercises to improve their contingency plans. This is an extremely valuable exercise but, for it to be effective, FAA must follow through and act on key suggestions.

FAA is also planning to train key systems users on the NAS portion of the business continuity and contingency plan. The air traffic services line of business is developing a training curriculum and intends to train air traffic controllers and systems specialists in the months preceding the date rollover. Because FAA's business continuity and contingency plan provides a Y2K focus not included in the agency's existing contingency plans, such training is crucial.

This concludes my statement, and I would be happy to respond to any questions that you or other members of the Subcommittees may have at this time.

## Contact and Acknowledgements

If you have any questions regarding this testimony, please contact Joel Willemssen at (202) 512-6408 or by e-mail at *willemssenj.aimd@gao.gov*.
Individuals making key contributions to this testimony include Nabajyoti Barkakati, William Bumgarner, Cynthia Jackson, Colleen Phillips, and Glenda Wright.

## 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

PRINTED ON RECYCLED PAPER

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

**Official Business**
**Penalty for Private Use $300**

**Address Correction Requested**

**Bulk Mail**
**Postage & Fees Paid**
**GAO**
**Permit No. GI00**