United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
10 a.m.
Monday,
March 15, 1999

# YEAR 2000 COMPUTING CRISIS

# FAA Is Making Progress But Important Challenges Remain

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

GAO/T-AIMD/RCED-99-118

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

We appreciate the opportunity to testify on the Federal Aviation Administration's (FAA) efforts to address the Year 2000 problem. With fewer than 300 days remaining until January 1, 2000, this critical issue 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 effectively 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 five topics: (1) FAA's progress to date, (2) the agency's self-reported data showing that much remains to be done, (3) challenges FAA faces in ensuring its internal systems will work, (4) risks associated with external organizations—focusing specifically on airports and international entities, and (5) the critical need for business continuity and contingency plans that identify how aviation operations will continue should systems fail.

In brief, FAA and its employees have worked hard over these past months and continue to show dedication in tackling the monumental Year 2000 problem. Looking back to where the agency was only a year ago, FAA has made tremendous progress. However, much remains to be done to complete validating and implementing FAA's mission-critical systems, and the agency continues to face challenges in making these internal systems Year 2000 compliant. Additionally, the risk of failures by external organizations, such as airports and foreign air traffic control systems, could seriously affect FAA's ability to provide aviation services—which could have a dramatic effect on the flow of air traffic across the nation and around the world. To mitigate the risk that critical internal or external systems will fail, FAA needs sound business continuity and contingency plans.

## FAA Has Made Substantial Progress in Its Year 2000 Program

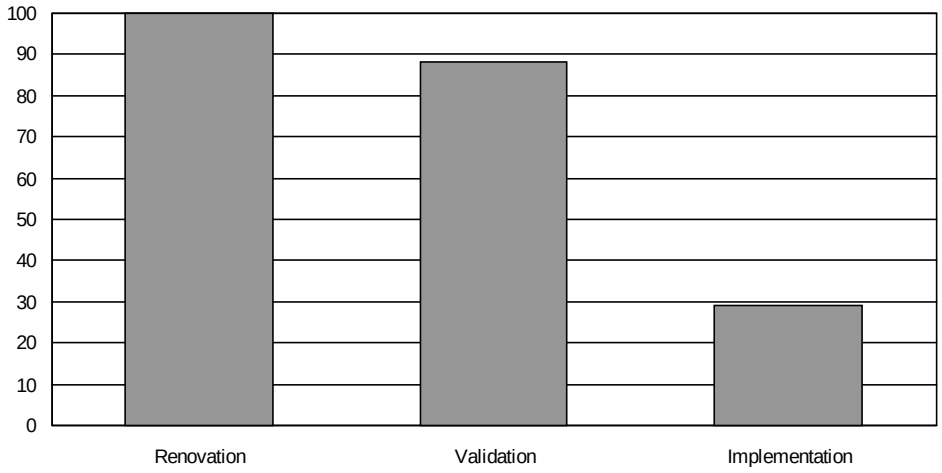
Over the past year, FAA has made substantial progress. In January 1998, FAA had no central Year 2000 program management; an incomplete inventory of mission-critical systems; no overall strategy for renovating, validating, and implementing mission-critical systems; and no milestone dates or schedules. At that time we recommended that FAA provide its Year 2000 program manager with the authority to enforce policies; outline FAA's overall strategy for addressing the Year 2000 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 Year 2000 business continuity and contingency plans to ensure the continuity of critical operations.

FAA has now addressed these recommendations. The agency has a strong Year 2000 management structure; an overall Year 2000 strategy; detailed standards and guidance for renovating, validating, and implementing mission-critical systems; a database of schedules and milestones for these activities; and a draft Year 2000 business continuity and contingency plan. Additionally, FAA reported that it completed 99 percent of its mission-critical systems repairs by the Office of Management and Budget's (OMB) September 1998 deadline and 74 percent of its systems testing by OMB's January 1999 deadline.

## Self-Reported Data Show FAA Still Has Much to Do

While the governmentwide deadline for completing systems implementation is at the end of this month, FAA's self-reported data demonstrate that much work remains to be done in a limited amount of time. Specifically, FAA must still finish implementing 141 mission-critical systems. Figure 1 details the overall reported status of FAA's mission-critical systems as of March 8, 1999.

**Figure 1: Percentage of Mission-Critical Systems That Have Completed Key Year 2000 Phases as of March 8, 1999**

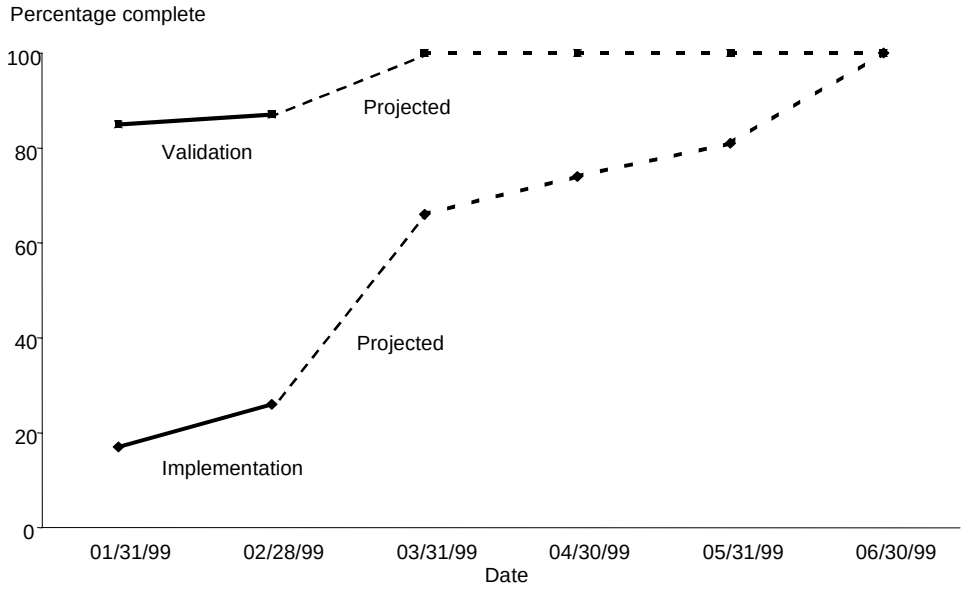



Source: FAA.

As of March 8, 1999, FAA's internal systems database showed that 50 of its 423 mission-critical systems had not yet been validated. These include 25 systems that have been repaired, 5 replacement systems, and 20 systems that were determined not to need repair or replacement. FAA intends to complete validation of all mission-critical systems by March 31, 1999.

Much more remains to be done to complete the implementation of mission-critical system repairs and replacements. While FAA determined that 224 of its 423 mission-critical systems do not require changes to be made, the remaining 199 systems (47 percent) must be modified, replaced, or newly installed. As of March 8, 1999, FAA reported that it had implemented 58 of these 199 systems. The agency plans to implement an additional 74 systems by March 31, and the remaining 67 systems by June 30, 1999. Figure 2 details FAA's schedule for completing the validation and implementation of its mission-critical systems.

**Figure 2: Percentage of Mission-Critical Systems Completing Validation and Implementation Over Time**




Source: FAA.

## Many Critical Air Traffic Control Systems Still Await Validation and Implementation

FAA has identified 26 mission critical systems as posing the greatest risk to the National Airspace System (NAS)—the network of equipment, facilities, and information that supports U.S. aviation operations--should their repairs experience schedule delays or should the systems not be operational on January 1, 2000. FAA ranked mission-critical air traffic control systems based on their impact and criticality to the NAS, their overall functionality, and an evaluation of the risk associated with solving the Year 2000 problem.

As of March 8, 1999, five of these critical systems had not yet been validated, and 14 had not yet been implemented. Twelve of the 14 that have not yet been implemented--providing critical functions ranging from

communications to radar processing to weather surveillance—are not scheduled to be implemented until after March 31, 1999.[1]

## FAA's Year 2000 Efforts Face Significant Challenges

FAA faces several challenges in completing its Year 2000 activities. These challenges include

- ensuring that systems validation efforts are adequate,
- implementing multiple systems at numerous facilities,
- completing data exchange efforts, and
- completing end-to-end testing.

## Support for Systems' Validation Is Not Always Sufficient and Complete

FAA's Year 2000 program office has developed standards for testing and implementing mission-critical systems that require system owners to prepare and obtain approval on a validation plan that includes test plans and procedures, funding requirements, test management roles, and schedules. The system owners are then required to test the system according to this plan, complete a checklist of required validation activities, and prepare a Year 2000 validation results report. Once this report has been approved within the relevant FAA business line, a contractor for FAA's Year 2000 program office performs an independent verification and validation (IV&V) review of key validation documents. The system is then considered ready to be implemented.

In reviewing validation plans, reports, and supporting test documentation for six mission-critical air traffic systems[2] that were reported as having completed validation, we found that the validation of three systems was

[1]The 12 systems are (1) the Automated Radar Terminal System (ARTS-IIIE), (2) the Host Environment, (3) the En Route Automated Radar Tracking System, (4) the Graphic Weather Display System, (5) the U.S. Notices to Airmen System, (6) the Aeronautical Mobile Communications Services, (7) the Integrated Communications Switching System (ICSS) Litton-types 2 and 3, (8) ICSS type III-Denro, (9) Terminal Doppler Weather Radar, (10) the Remote Maintenance Monitoring System, (11) Heating, Ventilation and Air Conditioning Systems, and (12) Mejoras Al Enlace De Voz Del ATS, a satellite-based communications system in the Caribbean and Central American regions.

[2]In choosing systems for our case studies, we attempted to cover a range of air traffic control functions in different environments. We selected validated systems from three different critical core functions (surveillance, communications, and weather processing) that operated in one or more of the different air traffic control environments (en route, terminal, tower, and flight service station). Two of the systems (FSAS and ICSS-Litton type 2,3) were also chosen because they were identified by FAA as among the 26 most at-risk systems.

supported.[3] However, one system's testing was found to be insufficient, and two systems lacked the documentation necessary to ensure that testing was adequate.

## ARTS-IIIA Validation Testing Is Insufficient

The Automated Radar Terminal System (ARTS)-IIIA is the critical data processing system used in about 55 terminal radar approach control facilities. These systems provide essential aircraft position and flight plan information to controllers. The ARTS-IIIA system continues to rely on a 1960s-vintage computer (a UNIVAC 8303 Input Output Processor), which was originally produced by UNIVAC but is now supported by the Lockheed Martin Corporation. Home computers available today have 250 times the memory of this archaic processor. In 1989 and 1990, we reported on the flight safety risks associated with this system and recommended that FAA assess other alternatives for meeting air traffic requirements.[4] However, FAA did not act on our recommendation, stating that it had a plan—which included continuing with the old processors. Ten years later, these processors are still in operation.

FAA validated the ARTS-IIIA system based on source code analysis, testing, and vendor inquiries performed by Lockheed Martin, whose representatives told us that they retained some of the experts who had worked on the UNIVAC 8303 processor in the 1960s. Source code analysis was used to identify all date processing code in the system. Testing was performed after problematic code was repaired, and vendor inquiries were used to determine the Year 2000-compliance status of all commercial-off-the-shelf (COTS) hardware, firmware, and software in the ARTS-IIIA system. Because of its criticality, we focused on the ARTS-IIIA subsystem that uses the UNIVAC 8303 processor and processes radar data. We found shortcomings in the source code analysis, testing, and vendor assessment of the UNIVAC processor, which form the basis for FAA's decision to validate this system.

Specifically, the analysis of the ARTS-IIIA source code, which includes code written in UNIVAC Ultra assembly language, depended upon using a common text search utility to search for 10 specific character strings that

[3]These systems are the Voice Switching and Control System, the Display System Replacement, and the Low Level Windshear Alert System version FA-10240.

[4]Air Traffic Control: Computer Capacity Shortfalls May Impair Flight Safety (GAO/IMTEC-89-63, July 6, 1989) and Air Traffic Control: Inadequate Planning Increases Risk of Computer Failures in Los Angeles (GAO/IMTEC-90-49, July 16, 1990).

included “DECADE,” “LEAP,” “YEAR,” “DATE,” and “DAY.” However, computer programs written in assembly language do not use only common English words such as “YEAR” and “DATE” for names of date fields. Instead, assembly language programs often use cryptic names such as DATCHK (for “date check”) or CURDAT (for “current date”). Thus, FAA’s analysis may not have found all date processing code in the Ultra assembly language programs that run in the UNIVAC processor. FAA officials stated that the code analysis was sufficient because they believe there are no date-related items in the code. We believe that the criticality of this system warrants a more thorough analysis.

The ARTS-IIIA system testing consisted of two phases. The first phase, performed at FAA’s Technical Center, involved evaluating data file transfers between the ARTS-IIIA memory and the peripheral equipment during simulations rolling the date forward through key dates—including from December 31, 1999 to January 1, 2000. The second phase, key site testing, involves performing Year 2000-rollover and functional evaluations at a site. FAA’s test documentation showed that these tests focused primarily on off-line programs, such as an editing application. The test documentation does not show any tests designed to validate the radar tracking functionality of the UNIVAC 8303 Input Output Processor at critical dates. Therefore, FAA’s testing to date validated data exchanges between the ARTS-IIIA memory and the peripheral devices in Year 2000, but not the critical functionality of tracking real radar data. FAA officials responded that they did not test the radar tracking functions because they did not make any modifications to these applications. However, the Lockheed Martin’s test report showed that there are date calculations in operational segments of the ARTS-IIIA system. Therefore FAA should test these functions. FAA officials stated that they plan to test the radar tracking functions during end-to-end testing.

Further, FAA’s use of vendor inquiries to assure the Year 2000 compliance of COTS hardware, firmware, and software was insufficient, given the criticality of the ARTS-IIIA system. The list of COTS hardware includes the UNIVAC 8303 input-output processor, which is no longer produced. FAA officials told us that they did not request or obtain a statement from the manufacturer that the processor was Year 2000 compliant. Instead, FAA relied on Lockheed Martin’s finding--based on analysis by an engineer that had worked on the UNIVAC processor since the 1960s--that there were no Year 2000 issues associated with the processor. Given the criticality of this processor, FAA’s Year 2000 program manager agreed that a statement of the processor’s Year 2000 compliance would be nice to have. A Lockheed

Martin representative agreed to look into the possibility of providing such a statement.

Because of shortcomings in the source code analysis, testing, and vendor certification of the UNIVAC processor's Year 2000 compliance, FAA's validation of the ARTS-IIIA system may be premature. A statement from the vendor that the UNIVAC 8303 processor is Year 2000 compliant together with FAA's planned end-to-end testing of radar tracking functions should provide greater assurance that the system will work through the Year 2000 date change as anticipated.

## Two Systems' Tests Lack Supporting Documentation

The Integrated Communications Switching System (ICSS)[5] supports ground-to-ground voice communications between air traffic controllers in adjacent facilities and air-to-ground voice communications between air traffic controllers and pilots. We reviewed ICSS test results and found that they lacked sufficient details to determine if all required testing was actually conducted. Specifically, for 1 of 2 key components, we could not determine whether required tests for processing 5 of 11 critical dates had been performed and passed.[6] If they were not tested, the risk that the system could experience unanticipated failures on these specific dates is increased. FAA testing documents also did not specify which version of ICSS had been tested and deemed Year 2000 compliant. As a result, the version of ICSS that was successfully tested may not be the version that is implemented in air traffic control facilities. If it is not, there is an increased risk of Year 2000-induced communications failures between air traffic controllers.

The test results for the Flight Service Automation System (FSAS), which provides essential weather information and flight planning services to general aviation pilots, also did not show whether the required tests for processing 6 of the 11 critical dates had been performed and passed. As a result, to the extent that the tests were not performed, FSAS is also at risk of failing unexpectedly on these dates, potentially affecting the flight planning capabilities of the general aviation community—a group that comprises over 95 percent of all flights within the United States. In

[5]There are multiple versions of ICSS in FAA's mission-critical systems inventory. We reviewed the validation information on ICSS-Litton types 2 and 3.

[6]FAA's compliance checklist requires the following 11 dates to be checked to ensure that they roll over to the next day correctly: 12/31/1998, 9/9/1999, 9/30/1999, 12/31/1999, 1/1/2000, 2/28/2000, 2/29/2000, 3/1/2000, 12/31/2000, 1/1/2001, and 12/31/2027.

responding to a draft of this testimony late last week, an FAA official stated that he was confident that all of the dates had been tested and agreed to provide the supporting documents this week.

Further, the validation plans for both ICSS and FSAS were not completed prior to testing, in accordance with FAA standards. For example, FAA conducted FSAS validation testing through June 1998, but the plan for conducting the validation test was written in July 1998. Not having a plan before testing compromises the integrity and objectivity of the tests and raises the risk that critical testing will be overlooked.

## The Number of FAA Air Traffic Control Facilities Complicates Systems Implementation

FAA's ability to implement system repairs and replacements in a timely manner is complicated by the agency's highly decentralized nationwide configuration of air traffic control facilities. FAA intends to deploy about 75 mission-critical air traffic control systems to one or more of its roughly 654 air traffic facilities.[7] Concurrently rolling out numerous systems changes to multiple sites will be time-consuming, labor-intensive, and filled with difficult implementation challenges.

FAA's Year 2000 program manager acknowledged that schedules are tight and there is no room for any schedule delays. He estimated that FAA has to complete roughly 4500 "events" by June 30, 1999—each one entailing the activation of a single system in a single site. To aid in this monumental task, FAA has established system implementation schedules for managing system changes at its facilities.

## Data Exchange Efforts Are Ongoing

In order to ensure that systems will successfully navigate the Year 2000 date change, systems' data exchanges must be assessed and any necessary modifications must be made. If not addressed, data exchanges could cause the failure of an otherwise compliant system.

Last month, FAA reported that it had 1,127 data exchanges in its inventory. After evaluating each, the agency determined that 119 data exchanges required modification. FAA reports that these data exchanges are

[7]These facilities include the Air Traffic Control System Command Center, Automated Flight Service Stations, Flight Service Stations, Alaskan Rotational Flight Service Stations, Air Route Traffic Control Centers, Airport Traffic Control Towers, Terminal Radar Approach Control facilities, Radar Approach Control facilities, and Combined Center/Radar Approach Control facilities.

associated with 42 different systems. As of last week, 33 of these systems have been validated and 12 have been implemented. FAA plans to complete implementing modifications to the data exchanges on its mission-critical systems by June 30, 1999.

While most of these systems' data exchanges requiring modification are between internal FAA systems, 10 systems also exchange data with outside entities. Specifically, three systems exchange data with other federal agencies, such as the National Aeronautics and Space Administration and the National Transportation Safety Board; three exchange data with other entities, such as foreign air traffic control providers; and two systems exchange data with both other federal agencies and other entities. Data exchanges with external entities are more at risk because FAA cannot control the schedule and priorities of these organizations. We are continuing to review FAA's progress in resolving Year 2000 issues associated with data exchanges.

## End-to-End Testing Underway

Integrated, end-to-end testing of multiple systems that have individually been judged Year 2000 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.

In August 1998, we reported that FAA's draft end-to-end test program plan was not sufficiently detailed to provide an understanding of how the agency planned to accomplish this testing.[8] Since that time, however, FAA has developed a detailed end-to-end testing strategy and plans.

FAA's end-to-end testing strategy related to the NAS focuses on systems that directly support navigation, surveillance, weather, maintenance, and air traffic control functions. While most of the systems that support these functions are owned and managed by FAA, some tests include external systems with which FAA systems interface, including commercial voice and data telecommunications systems, National Weather Service systems, and international air traffic control systems.

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

FAA established plans for, and is in the process of conducting, three types of Year 2000 end-to-end testing: system integrity testing, operational demonstration, and field site testing. The system integrity test involves testing groups of systems that together make up a core function to ensure that data are processed correctly. FAA has identified groups of systems that support weather processing, communications, flight- and radar-data processing, and remote maintenance monitoring. The results of these tests are to be analyzed to ensure that inputs and outputs are processed correctly across interfaces.

FAA has completed two system integrity tests using systems that have passed individual systems testing, although these systems have not necessarily completed all of the steps necessary to complete validation. FAA plans to complete a third system integrity test by the end of this month.

The end-to-end operational demonstration simulates having aircraft pass through all phases of flight using recorded data and tests the activities associated with these phases—such as weather briefings, clearances, aircraft tracking, rerouting, handoffs, and transfers. This test focuses on FAA's ability to continue intersystem and interfacility data communications through the Year 2000 date change. FAA officials stated that they completed this test last month, again using systems that had passed individual systems testing but that had not necessarily completed all validation activities.

Field site testing involves a demonstration of core NAS functions using equipment at operational air traffic control facilities in order to demonstrate that functional components at selected sites are reliable under Year 2000 conditions. FAA plans to complete this testing in April 1999.

FAA officials reported that they have encountered no Year 2000 problems thus far in any of their end-to-end tests and plan to issue a report on the results of all three types of end-to-end testing in June. We are continuing to review FAA's end-to-end testing results.

## Risks Associated With External Partners Could Affect Aviation Operations

In addition to the risks that its internal systems will malfunction or fail, FAA is at risk that external systems will fail, thereby affecting its operations. Two prime areas of concern are airports and international partners.

### Many Airports May Not Complete Year 2000 Activities in Time

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 Year 2000-induced failures and malfunctioning.

We recently reported on the status of airports' efforts to address the Year 2000 computing problem, based on a survey of 413 airports.[9] While the nation's airports are making progress in preparing for the year 2000, such progress varies among airports. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of 14 core airport functions.[10] Although most of those not planning to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

According to FAA and airport officials, adequate safeguards are in place to ensure the safety and security of the National Airspace System through the Year 2000 date change. Specifically, FAA requires an airport to suspend or restrict operations if it is unable to provide safety and security functions. Yet, airport officials stated that they would be unlikely to suspend or restrict operations should an automated system malfunction or fail,

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

[10] Our questionnaire focused on 14 core airport functions: access control, administration, airfield operations, airport services, baggage handling, communications, environmental systems, facilities maintenance, fuel services, ground support and ramp services, navigational aids, parking, ramp operations, and weather services.

because the airport could usually resort to manual operations. However, they also noted that if manual procedures are substituted for operations normally controlled by automated equipment, an airport's efficiency—its ability to handle its normal number of scheduled flights per day—could decrease and cause flight delays. Delays at one airport could cause delays at other airports and eventually reduce the efficiency of the entire National Airspace System.

## International Activity 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 Year 2000 international management team has been active. FAA is sharing information with its foreign counterparts and assisting them in addressing Year 2000 issues, such as business continuity and contingency planning. FAA is also actively working with the International Civil Aviation Organization to obtain Year 2000 status information on its international counterparts, and is prioritizing countries based on perceived risk in order to determine the level of end-to-end testing to be performed with these countries. FAA intends to complete international end-to-end testing with several countries by October 1, 1999, and plans to test interfaces with other countries after this date at their request.

FAA's Year 2000 international manager stated that FAA will provide status information on individual countries to the State Department to help develop travel advisories for at-risk countries. The State Department intends to issue such travel advisories later this year.

## Comprehensive Business Continuity and Contingency Planning Is Crucial

Because of the risk of anticipated and unanticipated failures—whether from internal systems or due to reliance on external partners and suppliers—a comprehensive business continuity and contingency plan is crucial to continuing core operations. FAA drafted a Year 2000 Business Continuity and Contingency Plan in December 1998 and is currently reviewing it. The agency plans to release four more iterations of this plan by the end of the year, with the next version due out in April 1999.

We reviewed the draft plan and found that it does not yet fully address several broad failure scenarios that could affect aviation operations, including simultaneous Year 2000-related failures of systems across the country, widespread power outages, or failures of interfacility telecommunications. The plan relies on FAA's current way of handling such problems at a single facility—by having adjoining facilities support the failed facility. This approach may not be appropriate should Year 2000-induced failures affect adjoining facilities. However, FAA's Year 2000 program manager stated that the agency plans to determine whether current contingency plans are sufficient to address widespread outages.

FAA is also working to address a concern with its plan that was voiced by the National Air Traffic Controllers Association (NATCA) over 8 months ago. At that time, NATCA officials stated that the contingency plans for certain FAA facilities do not adequately define the role of the air traffic controller. NATCA officials explained that should some "worst case" Year 2000 scenario occur—such as a critical facility's losing all power—FAA contingency plans require surrounding facilities to take over the air traffic control responsibilities of the failed facility. However, the contingency plans do not specify how the surrounding facilities would assume or perform these responsibilities. For instance, it is not clear which controllers would pick up which sectors of airspace, or even what information would be available to them.

Last month, FAA's air traffic operations division requested that regional air traffic division managers work with facility managers and NATCA representatives to ensure that facility contingency plans contain sufficient detail to fully inform air traffic controllers of their respective roles and responsibilities, and to provide them with the necessary information to meet those responsibilities. This effort is to be completed by April 30, 1999.

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.

**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 Rate**
**Postage & Fees Paid**
**GAO**
**Permit No. GI00**