
Office of Inspector General

The Year 2000 Computer Program and Computer Security Challenges

Department of Transportation

Report Number: FE-1998-187

Date Issued: August 25, 1998





Memorandum

**U.S. Department of
Transportation**

Office of the Secretary
of Transportation

Office of Inspector General

Subject: ACTION: The Year 2000 Computer Program
and Computer Security Challenges, DOT
Report Number: FE-1998-187

Date: August 25, 1998

From: 
John E. Meche
**Deputy Assistant Inspector General for Financial,
Economic, and Information Technology**

Reply To JA-20:x61496
Attn Of:

To: Acting Chief Information Officer
Federal Aviation Administrator

On August 6, 1998, at a hearing before the Subcommittee on Technology, House Committee on Science, U.S. House of Representatives, we provided our observations on the Federal Aviation Administration (FAA) Year-2000 computer program and computer security issues within FAA and the Department of Transportation (DOT). Subsequently, we also issued an advisory memorandum to the Deputy Secretary of Transportation on DOT's quarterly Year-2000 progress report to the Office of Management and Budget (OMB). Our statement and advisory memorandum are attached for your information.

Results-in-Brief

FAA made substantial progress on its Year-2000 problems within the last 6 months. To its credit, FAA initiated procurement of new Host computers and reviewed over one million lines of the Host microcode. FAA contractors did not identify any Year-2000 problems with the Host microcode that would preclude transition into the next millenium. FAA also reached out to aviation industry representatives at the national and international levels, which increased awareness of Year-2000 issues. While this was welcomed news, FAA cannot rest on these achievements.

FAA was reporting that it was on schedule to fix all known Year-2000 problems by September 30, 1998. We found FAA had six systems currently under development that had not been assessed for Year-2000 problems. FAA also was reporting that 102 of its mission-critical systems will not be tested and implemented by OMB's milestone date of March 31, 1999, including 19 percent of its Air Traffic Control systems. Additionally, where FAA had multiple units of the same systems, the systems were reported as renovated when only one of the units was fixed.

Concerning computer security, DOT had not obtained assurances of compliance with DOT security requirements from outside users of its computer networks, and only 1 of the 20 major DOT networks had been certified as secure. We also found FAA plans to put its primary and backup Host replacement computers in the same room. A single event within the computer room, such as a fire, could render both computers inoperable.

Recommendations

We recommend that FAA: (1) complete Year-2000 assessments of the six systems being developed, and ensure repair work is completed for all required elements including code modification, system replacement, and interfaces; (2) reevaluate the FAA master schedule and make a concerted effort to accelerate the implementation schedule for all systems to March 31, 1999, or as soon thereafter as possible; and (3) provide for physical separation of the primary and backup Host replacement computers.

We recommend that DOT: (1) ensure outside users of DOT computer networks are in compliance with DOT security requirements; (2) develop schedules to certify computer systems and install network security evaluation tools; and (3) establish policy concerning the ordering and receipt of replacement parts needed to fix Year-2000 problems on the same systems with multiple units.

We request that written comments be provided, within 30 days, to include specific actions taken or planned for each recommendation.

We will continue to monitor the Year-2000 project and computer security issues. We appreciate the courtesies and cooperation of FAA and DOT representatives. If we can answer any questions or be of further assistance, please call me or Rebecca Leng at (202) 366-1496.

2 Attachments

Before the Subcommittee on Technology, House Committee on Science

U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EDT
Thursday
August 6, 1998
Report Number: FE-1998-187

**The Year 2000 Computer Program
and Computer Security Challenges
at the Federal Aviation Administration**

**Statement of John L. Meche
Deputy Assistant Inspector General for
Financial, Economic, and Information
Technology
U.S. Department of Transportation**



Madam Chairwoman and Members of the Subcommittee:

We appreciate the opportunity to testify today on the Federal Aviation Administration (FAA) Year-2000 computer program, and computer security issues within FAA and the Department of Transportation (DOT). Our testimony will include:

- Progress FAA has made on its Year-2000 efforts since our testimony before this Subcommittee on February 4, 1998,
- Status of the Year-2000 program and computer network security,
- Challenges ahead for the Year 2000 and telecommunications networks, and
- Actions FAA and DOT should undertake to solve their Year-2000 and computer security problems.

Before addressing these areas, I will summarize our overall message and findings.

Six months ago, we testified before this Subcommittee on FAA's Year-2000 computer problems. At that time, FAA was 7 months behind the Office of Management and Budget (OMB) schedule for assessing its computer systems for Year-2000 problems, and had not completed its assessments. Most witnesses were disappointed with FAA's work at that time, especially pertaining to the Host computers used in the En-route Centers to direct high altitude traffic.

Today the Year-2000 picture is much brighter.

To its credit, FAA took decisive actions concerning the Host and many of its other computers. FAA initiated procurement of new Host computers, while simultaneously reviewing over one million lines of Host microcode for Year-2000 problems. The new Host computers currently are scheduled to be operational by October 1999. **Equally significant, FAA contractors did not identify any Year-2000 problems with the Host microcode that would preclude transition to, and uninterrupted entry into, the next millenium.** FAA's work has significantly reduced the risk associated with the Host computers. In addition to its own internal Year-2000 work, FAA reached out to aviation industry representatives at the national and international levels. FAA has increased awareness of Year-2000 issues facing the aviation industry. While this is welcomed news, FAA cannot rest on these achievements.

FAA is reporting that it is on schedule to achieve the next major OMB milestone—fixing all known Year-2000 problems by September 30, 1998. Significant progress was reported in the last 2 weeks of July. With less than 60 days to go, FAA still has to complete repairs on 53 mission-critical systems, 11 of

which are complex Air Traffic Control systems. There are three areas where FAA needs more attention. First, FAA needs better documentation to support the completeness of the renovation work, especially with replacement parts and system interfaces. Second, FAA needs to determine whether six of the new systems under development are Year-2000 compliant. And third, FAA needs to begin testing the systems.

With about 500 days to the Year 2000, FAA still has significant challenges ahead. **For example, 102 of FAA's mission-critical systems will not be tested and implemented by OMB's milestone date of March 31, 1999. This includes 19 percent of the mission-critical systems for air traffic control.** We have been urging FAA since October 1997 to accelerate its implementation schedule. While a great deal of progress has been made, FAA's current schedule, in our opinion, is still cutting it too close. It is imperative that FAA make a concerted effort to accelerate implementation of the 102 systems to March 31, 1999, or as soon thereafter as possible. This would provide for a cushion if problems are identified when fielding these systems, and allow FAA time to go through the repair and testing process again before the end of 1999.

One area external to FAA that is receiving attention in the aviation industry is awareness of Year-2000 issues. While FAA has had successes with its outreach to industry, continued proactive attention is needed by FAA with national and international industry representatives.

Computer security is becoming more important.

Although this hearing is focused primarily on FAA, discussion of computer security would not be complete without including the Department's computer networks because they are interconnected.

In April 1997, we reported the Department's computer systems lacked firewalls (commercial security software protection) to prevent unauthorized access by Internet users. Since then, the Department installed firewalls in DOT Headquarters and FAA to secure these entry points ("front doors"). While the front doors have been reasonably secured, unauthorized access to departmental networks still can be gained through "back doors." These back doors are network access points that were not intended to be primary entrances, and therefore, are not controlled by firewalls. We found additional efforts are needed to ensure these back door users are in compliance with DOT security requirements.

During our current computer security work, although only in the early stage, we found that 1 of the 20 major networks in DOT has been certified as secure. The one secure system is a Coast Guard system. We also found that network

administrators could make better use of commercially available network security evaluation tools in the identification of network security weaknesses and intruders.

Focusing on FAA, the President's Commission on Critical Infrastructure Protection reported the current networks supporting the National Airspace System (NAS) operations are relatively immune from intruders because of the use of older technologies and the system's physical isolation. However, we found FAA, as part of its NAS modernization, plans to use a common network to support both administrative and NAS operational needs, which could lead to additional exposure for the NAS. During our review, we also found that the primary and backup Host computers are located in the same room. A single event within the computer room, such as fire, could render both computers inoperable.

A comprehensive computer security program needs effective leadership. The Department does not have a permanent Chief Information Officer (CIO) and FAA is currently seeking a CIO. Until DOT and FAA have a permanent CIO, it will be difficult to establish and maintain a comprehensive computer security program.

Our testimony today will identify actions FAA and DOT should take to gain the confidence that there will be no significant Year-2000 and computer security issues. They include the need to:

- complete Year-2000 assessments of the six systems being developed, and ensure repair work is completed for all required elements including code modification, system replacement, and interfaces;
- reevaluate the FAA master schedule and make a concerted effort to accelerate the implementation schedule for all systems to March 31, 1999, or as soon thereafter as possible;
- enhance departmental computer security by (1) ensuring back door users are in compliance with DOT security requirements; (2) developing schedules to certify systems and install network security evaluation tools; and (3) providing for physical separation of primary and backup Host replacement computers.

We are working closely with the Federal Aviation Administrator and the Department's Acting Chief Information Officer to enhance Year-2000 and computer security programs. We will continue to monitor these issues, and advise the Federal Aviation Administrator, the Secretary, and the Congress of progress and problems.

Background

The nation's transportation system is becoming more and more dependent on information technology. DOT's ultimate goal, as stated in its strategic plan, is to:

Improve mission performance, data sharing, system integrity, communications, and productivity through deployment of information systems which are secure, reliable, compatible, and cost effective now and beyond the Year 2000.

This statement addresses the challenges facing DOT in two information technology areas—the FAA Year-2000 computer program, and the Department's computer network security.

FAA Year-2000 Accomplishments and Challenges

OMB established a five-phase approach for addressing Year-2000 computer problems. Milestones established by OMB are:

Table 1 – Year-2000 Phases and Milestones

YEAR-2000 PHASES	TASKS	OMB TARGETS
Awareness/Assessment	Determine Scope of Year-2000 Problems	June 1997
Renovation	Fix Year-2000 Problems	September 1998
Validation	Test the Fix	January 1999
Implementation	Install Year-2000 Compliant Systems	March 1999

FAA reported it completed the assessment phase in February 1998, about 8 months after the OMB milestone. Today, FAA is reporting that it is back on schedule, and will complete all repairs of its known Year-2000 computer problems by September 30, 1998.

FAA's Year-2000 Accomplishments

At the joint hearing before this Subcommittee and the Subcommittee on Government Management, Information and Technology on February 4, 1998, we made eight recommendations addressing assessment work, the Host computer Year-2000 evaluation, and the overall Year-2000 program management (see Exhibit A for details). We are pleased to report that FAA has taken action on all of our recommendations.

One of the most serious concerns discussed in the last hearing was the continued service of the Host computer into and beyond the Year 2000. The Host computer is a key part of the system that enables air traffic controllers to direct high altitude air traffic from En-route Centers. Two important questions needed to be answered: Can FAA make the Host computer Year-2000 compliant, and can FAA find replacement parts to keep it running until it is replaced with new systems? We recommended FAA make a prompt decision on the Host computer replacement and repair strategy, have an independent review of plans to fix and certify the existing Host computer, and develop a suitable contingency plan to continue operations in case both the Host repair and replacement efforts are not completed by the Year 2000.

In response to our recommendations, and in full recognition of the vulnerability of the Host computer, FAA initiated procurement of Host replacement machines. FAA is performing initial testing, and developed a preliminary schedule to install the replacement machines in all 20 En-route Centers by October 1999. In a parallel effort, FAA hired contractors to review the existing Host computer for Year-2000 problems, and repair them if necessary. The contractors concluded they were "unable to identify any microcode Y2K [Year 2000] problem associated with the operational processing of flight and radar data functionality."

Even with the accelerated plan to have new Host computers installed by October 1999, and comfort gained from the contractors' results, FAA still plans to continue its date roll back testing on the existing Host computer as a contingency in case replacement efforts are delayed and the existing Host computer experiences unexpected Year-2000 problems. In our opinion, FAA's work has significantly reduced the risk of Host computer service disruption into and beyond the Year 2000.

Status of Actions to Fix Year-2000 Problems

FAA identified 159 mission-critical systems requiring repair work to make them Year-2000 compliant. Table 2 shows FAA has made significant progress in repairing its mission-critical systems, most of which were reported as completed in the last 2 weeks of July.

Table 2 – System Repair Progress

Organization	5/15/98	7/15/98	7/23/98	7/31/98
Air Traffic Control Systems	14	31	40	50
Others	6	6	43	56
Totals	20	37	83	106

With less than 60 days to go, FAA still faces a significant challenge to complete all repair work by OMB's September 30 milestone. For example, among the 53 systems yet to be fixed are 11 complex Air Traffic Control systems. In our continuing oversight of FAA's Year-2000 program, we identified two additional areas that need more attention by FAA:

- o Better support is needed for renovation work.

DOT guidance specified three critical elements to be accomplished when claiming repair of a Year-2000 problem is complete: (1) modifying program code, (2) replacing hardware and commercial off-the-shelf software, and (3) developing software to facilitate data exchange with interfacing systems. We found there was limited documentation to support the work done that resulted in reporting systems as fully renovated, especially in the areas of replacement parts and systems interfaces.

Among the repaired systems we sampled, there was evidence that replacement parts had been ordered; however, there was no indication whether the parts were delivered and installed. Installing replacement parts generally is not challenging. However, the success of the repair is contingent on vendors' capability to make timely delivery. FAA needs to receive and install replacement parts in time for testing so that it can determine whether the repaired system will function with other systems as intended.

More work is needed concerning system interfaces (the process by which systems exchange data with each other). For the repaired systems we sampled, interface systems were identified. However, there was little documentation indicating what needed to be done to ensure successful interfaces. FAA recently disclosed it had not determined interfacing requirements for 38 mission-critical systems, 9 of which were reported as fully renovated. Based on our work, some of the systems may not have been completely fixed and reported in accordance with departmental guidance. We are currently working with FAA management to determine whether repair work has been completed for all required elements—i.e., code modification, system replacement, and interfaces.

- o FAA needs to know if all new systems currently under development are Year-2000 compliant.

In our February 4 testimony, we reported that FAA had not yet concluded whether 23 major projects under development were Year-2000 compliant. We recommended FAA determine whether or not systems currently being purchased were Year-2000 compliant, and take appropriate action on those that were not. We recently surveyed these major development projects, and found FAA still needs to determine whether four systems currently under development were Year-2000 compliant. Two additional systems were deemed to be Year-2000 compliant based primarily on verbal assurances from vendors. None of these six systems had specific contract language requiring the systems to be Year-2000 compliant. FAA plans to determine whether these six systems are Year-2000 compliant during the testing phase. In our opinion, this is too late to determine whether these systems have a Year-2000 problem.

Significant Challenges Lie Ahead for FAA

- o FAA is behind on OMB's implementation milestone.

Although FAA plans to meet OMB's milestone for fixing all known Year-2000 problems by September 30, 1998, Table 3 on the following page shows 102 of its mission-critical systems will not meet OMB's implementation date of March 31, 1999.

Table 3 – FAA Implementation Schedule

Organization	April – June 1999
Air Traffic Service	42
Acquisition	11
Others	49
Total	102

FAA has 42 systems (19 percent) of its critical Air Traffic Control systems that will not meet the OMB implementation milestone of March 31, 1999. Due to the criticality of Air Traffic Control, and FAA’s poor track record for fielding information technology programs, FAA’s current schedule, in our opinion, is still cutting it too close. It is imperative that FAA make a concerted effort to accelerate implementation of the 102 systems to March 31, 1999, or as soon thereafter as possible. This would provide a cushion if problems are identified when fielding these systems, and allow FAA time to go through the repair and testing process again before the end of 1999.

Upon completing the repair of, and finalizing the test plan for, its mission-critical systems, FAA needs to identify opportunities to further accelerate the implementation schedule in line with the OMB milestones.

- o FAA needs to finalize its test and contingency plans .

Although a specific system may be considered repaired and tested, it is not possible to ensure that systems will work in combination with other systems until all are linked together in a test environment. FAA’s end-to-end testing (from radar to the air traffic control screen) is critical for Year-2000 success because of the interdependency and complexity of the Air Traffic Control systems. The task is further complicated by the fact that local software

changes have been made to the Air Traffic Control systems, which could result in different test results.

As a result, FAA needs a comprehensive test plan and should begin testing the Air Traffic Control systems as soon as possible. As of today, FAA plans to complete its end-to-end test plan and its contingency plan by August 31, 1998. Since we have not seen these plans, we cannot comment on their adequacy.

- o FAA outreach to airlines, airports, and international aviation still need attention.

FAA has reached out to the aviation industry to improve awareness of Year-2000 issues. FAA sponsored three industry days which brought Government, private sector, and international segments of the aviation industry together to discuss and coordinate Year-2000 issues. FAA also established an international Year-2000 office and published an international plan to improve coordination among the international aviation industry. Although these efforts are helpful, FAA has no regulatory control over foreign air traffic control systems, and can only offer suggestions and advice.

In addition to FAA's efforts, the Air Transport Association (ATA) sponsored a Year-2000 review of 150 major airports nationwide. The scope of its review includes developing an operational systems inventory of equipment, such as runway lighting and fuel pump equipment. To date, ATA has looked at about 50 airports and has developed a systems inventory checklist of about 117 systems. The International Air Transport Association (IATA) is performing similar reviews at foreign airports. ATA and IATA are still determining potential risks. Much work still needs to be done.

As part of its outreach to industry, FAA requested aircraft manufacturers and air carriers to respond to specific requests for data. FAA requested aircraft manufacturers to perform self-assessments, prepare Year-2000 action plans, and report any safety-related Year-2000 issues. FAA also asked air carriers to certify that they, and their suppliers, are Year-2000 compliant. We found air carriers are reluctant to provide this type of certification, and that aviation industry representatives would like FAA to define “Year-2000” compliance and what FAA will require to show Year-2000 compliance. FAA needs to continue its proactive attention with the national and international aviation industry.

Department’s Computer Network Security

DOT has about 20 major computer networks which are supported by hundreds of local and wide area networks. Exhibit B is a simplified network diagram depicting how these networks are linked to each other and to the Internet. For discussion purposes, we grouped these network systems into two categories: (1) administrative networks used to support the Department’s processing and transmission of non-air traffic control data, such as payroll, grant payments, and safety statistics/research information, and (2) the National Airspace System (NAS) used to support air traffic control operations.

Need for Comprehensive Computer Network Security

Computer security is becoming important as more computer networks become interconnected. These interconnected systems can provide intruders with the ability to “hack” into computer systems from many different directions and locations. DOT networks are connected with each other, and also with

contractors, state and local Governments, and third party networks through the Internet. The Department has established more than 80 web sites to disseminate information. DOT networks are accessed by thousands of DOT and contractor employees, and potentially by millions of Internet users.

Computer intruders, who are unauthorized users, can enter computer systems from external sources, such as Internet users, as well as from internal sources such as disgruntled employees. A survey performed by the Federal Bureau of Investigation in 1998 reported that insiders constitute the greatest intruder threat. Intruders are becoming increasingly sophisticated with automated tools to probe and exploit network security weaknesses. A control weakness in one network could compromise other networks.

Additional Efforts Are Needed to Secure DOT Administrative and NAS Systems

DOT's Administrative Networks

In April 1997, a contractor, who was retained by us, reported the Department lacked firewalls¹ to prevent Internet users from navigating DOT networks, or using these networks to gain access to other computers. Since then, the Department installed needed firewalls in DOT Headquarters, and in FAA, to secure the entry points (“front doors”) from the Internet to departmental administrative networks. However, our current work has identified additional security is needed:

¹ A firewall is commercial hardware and software which screens communications to and from the Internet. Because software tools and techniques are constantly evolving, firewalls, when properly implemented, provide reasonable, but not complete, assurance that intrusions will be prevented.

- o DOT administrative networks need to be better secured.

While the Department has reasonably secured its “front doors,” unauthorized access to departmental networks can still be gained through “back doors.” These back doors are network connections with contractors, other Federal agencies, dial-up users, and other entities such as industry associations. They were not intended to be primary entrances and, therefore, are not controlled by firewalls. These back doors are identified as shaded areas on the network diagram in Exhibit B.

The Department’s policy is to obtain “Statements of Conformance” from these back door users. These statements would provide assurance from the users that their systems are in compliance with DOT security requirements. We reviewed a sample of three major networks and found conformance statements were not obtained. Accordingly, the Department has no assurance that these back door users are complying with DOT security requirements.

Through these potentially unsecured back doors, intruders could bypass DOT firewall screening and gain unauthorized access to DOT networks. Table 4 on the following page shows DOT’s vulnerability, and that vulnerability has resulted in unauthorized access to its networks.

Table 4 -- DOT Network Exposure

Network	Secured Internet Access		Remote Contractor Access	Other Federal Agency	Dial-up Access	Other Entity Access	Known Unauthorized Access
DOT Administrative	X		X	X	X	X	Yes
FAA Administrative	X		X	X	X	X	Yes
FAA NAS	N/A		X	X	X	X	Yes
<u>Front Doors Reasonably Secured</u>			<u>Back Doors Still Open</u>				

- o DOT administrative networks could be better monitored.

By using a commercial network evaluation tool, we found that departmental electronic mail files were not secure, and could be read or modified by knowledgeable intruders. This weakness was subsequently corrected. However, departmental network administrators need to make better use of commercially available network evaluation tools to determine weaknesses in their network. These tools can determine if sensitive network control files have been manipulated by unauthorized persons.

We found there have been at least 15 intruders into DOT systems since April 1997; however, none was reported to DOT's Acting CIO. Without this information, the Department could not effectively evaluate its network vulnerability and take corrective actions.

- o DOT systems security needs to be certified.

The Department needs to evaluate and test the security of its automated systems every 3 years as required by OMB. This process involves preparing a security plan for the system, evaluating system risks and countermeasures, and testing for the effectiveness of security requirements. The system owner then certifies, in writing, that all security measures are functional. We found 1 of the 20 major networks in DOT has been certified as secure. The one system was a Coast Guard system. We were told these security evaluations have not been completed because of a lack of funds for, or guidance on, testing network security.

FAA's Operational Systems

The President's Commission on Critical Infrastructure Protection specifically identified NAS as a critical national asset that must be protected. The Commission reported the present NAS networks are relatively immune from intruders because of the use of older technologies and the system's physical isolation.

In May 1998, the General Accounting Office (GAO) issued a report recommending FAA enhance NAS security in several areas². Our testimony will focus on two specific issues:

² GAO recommended FAA (a) perform additional physical security inspections of its facilities, (b) complete vulnerability assessments for all Air Traffic Control systems, (c) certify systems' security, and (d) provide more central control over security policy and implementation (GAO/AIMD-98-155).

- o The primary and backup Host computers need to be separated.

Because of the criticality of air traffic control operations, FAA installed two Host computers at each En-route Center. If the primary Host computer fails, the processing is automatically switched to the backup machine. This redundancy was designed to mitigate the impact of system failures. However, we found the primary and backup computers were in the same room, instead of being placed in separate rooms with independent support systems (e.g., fireproof wall, and cooling and ventilation systems). As a result, a single catastrophic event within the computer room, such as fire, could render both the primary and backup computers inoperable.

This physical limitation is the result of cabling constraints in the existing Host computer. As mentioned earlier, FAA plans to replace the Host computer. The new machine does not have the cabling limitation. However, FAA's implementation plan shows it will install both primary and backup replacement machines in the same room. As a result, air traffic control operations in the En-route Centers still will be vulnerable to a single catastrophic event.

- o FAA's computer network security needs to be improved as NAS becomes modernized.

As mentioned earlier, the current networks supporting NAS operations are considered relatively immune from intruders. However, as part of the NAS modernization effort, FAA plans to use a common network to support both administrative and NAS operational needs, which could lead to additional exposure for the NAS because FAA administrative networks are interconnected with outsiders such as Internet users.

Need for Effective Information Technology Leadership

A comprehensive computer security program needs effective leadership. The Clinger-Cohen Act requires agencies to appoint a CIO to promote effective system design; monitor the performance of information technology programs; and advise whether automated systems should be continued, modified, or terminated. However, the Department does not have a permanent CIO, and FAA is seeking a CIO. Until DOT and FAA have a permanent CIO, it will be difficult to establish and maintain a comprehensive computer security program.

Actions Needed to enhance the Year-2000 Program and Computer Security

We offer the following recommendations to enhance FAA's Year-2000 program:

- Complete assessments, by August 31, 1998, of the six systems currently under development to determine whether they are Year-2000 compliant; and ensure repair work is completed for all required elements including code modification, system replacement, and interfaces; and
- Make a concerted effort to accelerate the implementation schedule for all systems to March 31, 1999, or as soon thereafter as possible.

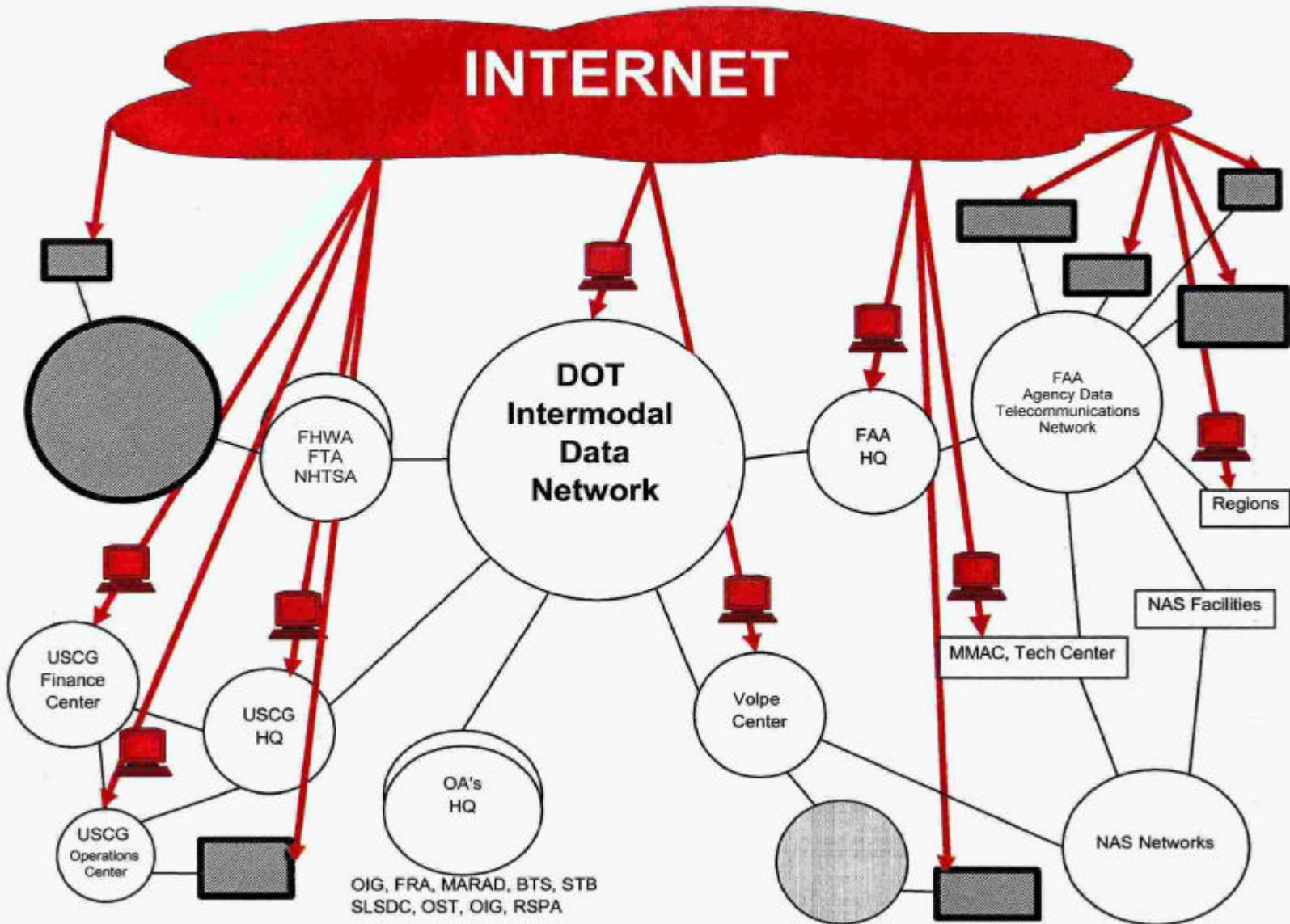
We offer the following recommendations to enhance DOT computer security:

- Obtain Statements of Conformance from entities connected to DOT networks for compliance with DOT security requirements; develop schedules, within 30 days, to certify the security of mission-critical systems and install network security evaluation tools; and provide for physical separation of primary and backup Host replacement computers.

Madam Chairwoman, this concludes our statement. I would be pleased to answer questions.

STATUS OF OIG RECOMMENDATIONS

	Recommendation	FAA
1	Complete assessment work, including quality assurance reviews, on existing systems. Take prompt action to make necessary fixes to newly acquired but not yet operational systems.	Reported completion of assessment work, including the majority of quality assurance reviews on existing systems. Expanded the use of independent quality assurance reviews on newly acquired systems.
2	Expediently appoint a person with strong technical leadership and authority to manage the Year 2000 program.	Appointed a Year-2000 Program Manager directly to the FAA Administration support staff.
3	Make a prompt decision on the HOST computer fixes.	Adopted a two-pronged approach to computer hardware before HOST microcode.
4	Develop a suitable contingency plan for the HOST computer.	In progress. FAA will have a contingency plan by December 31, 1998.
5	Have an independent review of plans to fix and certify the existing HOST computer.	FAA decided it will certify the existing HOST computer.
6	Develop a master schedule for fixing and testing all mission-critical systems.	The FAA Year-2000 project schedule as of May 1998. FAA is developing schedules.
7	Promptly identify and secure resources needed to get the job done by no later than June 1999.	On March 9, 1998, issued a performance plan and action plan from November 1999 to June 1999.
8	Report monthly to the Secretary and Congress on the progress made toward fixing Year 2000 problems.	As of May 1998, FAA is reporting to the Secretary and Congress.



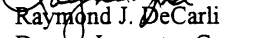


U.S. Department of
Transportation
Office of the Secretary
of Transportation
Office of Inspector General

Memorandum

Subject: INFORMATION: Year 2000 Computer Problem

Date: August 14, 1998

From: 
Raymond J. DeCarli
Deputy Inspector General

Reply To
Attn Of:

To: Deputy Secretary

We reviewed the Department's quarterly report to OMB for August 1998. In performing the review, we worked with the Office of the Chief Information Officer (CIO) and selected Operating Administrations' Year-2000 program offices. In our opinion the report presents a reasonable and fair depiction of the status of DOT's actions to ensure all mission critical computer systems are, or will become, Year 2000 compliant.

There are three areas that warrant explanation and close management attention. They relate to the purchasing of commercial hardware, firmware, and software when multiple units of the same system need renovation; assuring that system interfaces will be operational; and accelerating work on systems not currently scheduled to be renovated, tested, and implemented by March 31, 1999.

- Acquisition of commercial hardware, firmware and software. The report to OMB classifies a system as renovated when software has been updated, commercial replacement parts (hardware, firmware, and software) ordered, received, installed, and tested in one unit of a system. In the DOT environment, there are numerous cases where there are multiple units of the same system. In order to make all units Year-2000 compliant, replacement hardware, firmware, and software must be purchased, installed and tested on all units of these systems. For example, if a system requiring commercial parts is installed and used at 20 different locations, the system is reported as renovated when one of those units (at one location) is renovated. In reality, at the time the system is reported as renovated, only 1 unit has been renovated. The remaining 19 still need commercial parts before they can be renovated.

The ability to renovate the additional units requiring replacement items is dependent on the purchase of the required parts and the vendors' ability to deliver those parts within the timeframes necessary to allow installation and testing of all units. Timely ordering of parts and close monitoring of deliveries is therefore critical. FAA is implementing a system to closely monitor the acquisition of replacement parts. FAA is also drafting a policy requiring all replacement parts be placed on firm orders no later than October 15, 1998; and be on hand no later than November 30, 1998. The CIO Office should establish similar requirements for all OAs that have multiple units of the same system.

- Determination of whether systems interfaces will work on renovated systems. The FAA has not completed sufficient analysis, or made all the changes necessary, to ensure interfaces between systems that have been renovated will work. FAA is aware of this condition and is in process of reviewing interfaces and making the necessary changes. FAA has indicated that it will complete renovation of all interfaces by the end of September 1998. It is essential that necessary interface repairs be identified and addressed promptly.
- Systems not scheduled to be renovated and implemented by March 31, 1999. The report to OMB shows that 63 critical systems will not be renovated and implemented by the March 31, 1999 date established by OMB. Of these systems, 62 are in FAA and 1 in the Coast Guard. The FAA and Coast Guard must accelerate their efforts in order to complete implementation on time.

If I can answer any questions or be of further assistance, please feel free to call me on x66767.

#

cc: FAA Administrator
Commandant, USCG
Acting Chief Information Officer

