

INFORMATION SECURITY PROGRAM

Department of Transportation

Report Number: FI-2003-086

Date Issued: September 25, 2003




Memorandum

**U.S. Department of
Transportation**

Office of the Secretary
of Transportation
Office of Inspector General

Subject: **ACTION:** Information Security Program,
Department of Transportation
FI-2003-086

Date: September 25, 2003

From: Alexis M. Stefani 
Principal Assistant Inspector General
for Auditing and Evaluation

Reply to
Attn. of: JA-20

To: Chief Information Officer

This report presents the results of our audit of the information security program at the Department of Transportation (DOT). Responding to requirements of the Federal Information Security Management Act (FISMA), our objective was to evaluate DOT's information security programs and practices. We focused our evaluation on management controls, network and Electronic-government (E-government) security, systems security, protecting national-critical systems, personnel security, and system contingency planning. We also provided input (Exhibit A) to DOT's annual FISMA report by answering questions specified by the Office of Management and Budget (OMB). Our scope and methodology are described in Exhibit B.

INTRODUCTION

FISMA requires Federal agencies to ensure that computer systems and data are adequately protected from losses due to attacks. Protecting computer systems and data presents a challenge to all Federal agencies. Because DOT maintains one of the largest portfolios of information technology (IT) investments in the Federal government, it is critical that DOT protects its systems and sensitive data. In fiscal year (FY) 2003, DOT's information technology budget totaled about \$2.7 billion.¹

DOT has 12 major organizations (Exhibit C) with about 630 computer systems. DOT systems include safety-sensitive air traffic control systems and surface

¹ Excludes budget for U.S. Coast Guard and the Transportation Security Administration which transferred to the Department of Homeland Security in March 2003.

transportation systems, as well as financial systems that disburse over \$50 billion in Federal funds each year. DOT also maintains air traffic control systems that are essential to the Nation's defense, economic security, or public confidence. These “national-critical” systems need to be secured on a priority basis.

During FY 2003, DOT also continued to expand its E-government services, doubling the number of public web sites to more than 400. DOT uses these web sites, which contain millions of web pages, to conduct business, such as accepting hazardous material shipment registrations and payments; and to disseminate information, such as temporary flight restrictions or motor carrier safety records.

RESULTS IN BRIEF

For the last 2 years, DOT reported its information security program as a material internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA). This year, DOT made significant progress toward meeting its commitment to improve information security.

The most noteworthy improvement DOT has made since we began the annual information security review in FY 2001 is in protecting its computer systems from attack by outsiders. For example, DOT enhanced its defense against intrusions from the Internet in FY 2002, and further reduced its vulnerability to attack this year by establishing a Departmentwide security incident response center. This center, with the cooperation of FAA's incident response center, detects, analyzes, and prevents hundreds of potential intrusions from the Internet on a daily basis. Also, this year, DOT appointed a Chief Information Officer (CIO), increased the CIO's resources and influence, and developed a more reliable inventory of systems; all of which further strengthened DOT's information security protection. In addition, air traffic control systems and facilities stayed operational during the recent blackout as a result of quickly switching to their emergency backup systems.

However, DOT still has a long way to go in securing its computer systems from attack by insiders: employees, contractors, grantees, and industry associations. According to the Federal Bureau of Investigation, insiders remain a major threat—about 50 percent of unauthorized activities against all computers were done by insiders during 2003. DOT is not exempted from such a threat. A critical control to mitigate such threats is to perform security certification reviews on individual systems. However, only 33 percent of DOT's systems will have completed such reviews by September 2003. We also found that DOT needs to continue enforcing background checks on contractor employees performing sensitive system work,

and to enhance its contingency planning to ensure business continuity in case key computer system operations are disrupted for a prolonged period of time.

In view of the security weaknesses that still need to be corrected, DOT's information security program remains a material weakness and requires continued senior management attention. In FY 2004, it will be critical for the departmental CIO, with support from the Operating Administrators and their respective CIOs, to continue exercising leadership and providing the direction and oversight to ensure that the Operating Administrations develop adequate plans to correct the remaining weaknesses and execute those plans effectively. DOT's progress correcting the remaining weaknesses will help clarify whether the CIO has adequate authority, resources, and processes to ensure effective IT security and investment management controls.

As a result of this year's assessment, we are making a series of recommendations on pages 14 and 15 of this report to help the Department correct the material weakness. By implementing these recommendations, DOT should not only increase its defense against insider attacks but also enhance the oversight of its multi-billion dollar annual IT investments. The DOT CIO agreed with our findings and recommendations.

FINDINGS AND RECOMMENDATIONS

Management Controls

The Clinger-Cohen Act requires that DOT appoint a CIO responsible to ensure the Department acquires and operates cost effective IT systems, and protects the systems and data from attack. In FY 2002, we reported that DOT had not had a CIO since January 2001 and that the CIO lacked the authority to require the Operating Administrations to implement DOT security guidance. We recommended that DOT appoint a CIO and establish the CIO's authority to approve Operating Administration IT budgets and to provide input to Operating Administrations' CIO performance appraisals.

During FY 2003, DOT made progress by appointing a Departmentwide CIO and obtaining significant budget increases for the Office of the CIO. Although DOT did not give the CIO the authority to approve Operating Administration IT budgets or to provide input into Operating Administrations' CIO performance appraisals as we recommended, it did increase the CIO's influence over IT decisions by forming a departmental Investment Review Board (the Board). The Board, chaired by the Deputy Secretary, with the CIO, the Chief Financial Officer, the General Counsel, and the Assistant Secretary for Administration as official members designated by

the Secretary, has the authority to approve, modify, or terminate major IT investments.²

Creation of the Board, appointment of a CIO, and enhancement of the CIO's influence should improve DOT's oversight of IT investments and security; however, it is too early to judge the effectiveness for two reasons. First, historically, the Operating Administrations have functioned independently on IT matters with little departmental direction. Second, the Review Board only began reviewing IT investments in June for this year. DOT's ability to improve computer security is closely tied to the effectiveness of the IT review process because security needs of IT projects and programs must be considered in making investment decisions. Much of the value added by the CIO will come through his involvement in investment decisions. Under the Clinger-Cohen Act, the CIO is responsible for promoting effective processes to acquire and operate information systems, and to ensure that systems are adequately protected from threats.

During FY 2004, at the request of the Senate Appropriations Committee, we plan to evaluate the effectiveness of the CIO's efforts to coordinate with the Operating Administrations in improving IT security and investment controls. This year, we identified the following opportunities to improve DOT's IT investment review process, which should result in better secured and more cost-effective IT investment.

- Criteria are needed to help the Board select IT investments for review. This year, the Board focused on reviewing “cross-cutting” IT projects concerning more than one Operating Administration. For example, the Board reviewed the progress of implementing a new departmental accounting system, the status of converting the departmental payroll system, and a proposal to consolidate the IT infrastructure in DOT Headquarters. However, the Board reviewed only one Operating Administration-specific investment after we had identified significant cost and schedule problems in the project.

The Board needs to play a more proactive role in identifying high-risk Operating Administration IT investments for review, considering that over 90 percent of DOT's IT budget is appropriated directly to the Operating Administrations. There is also a significant need for increased management oversight of these investments. We have issued several reports on major acquisitions involving extensive software development work that require senior

² Designation of official Board members was specified in the DOT Information Technology Capital Planning and Investment Control Manual, June 21, 2002.

management level attention.³ For example, FAA's Wide Area Augmentation System (WAAS), Standard Terminal Automation Replacement System (STARS), and Local Area Augmentation System (LAAS) have all experienced significant cost overruns (from 31 percent to 227 percent) and schedule delays (from 4 years to 7 years). Congress has also expressed concerns over “the potential for dramatic cost escalation” in FAA's multi-billion-dollar new En Route Automation Modernization (ERAM) project.

The Board needs to issue more specific criteria for identifying IT projects for its review, and direct the Operating Administrations to brief the Board on IT projects that meet the specified criteria.

- We found that more substantive, in-depth reviews of Operating Administration IT budget requests are needed. This year, the Operating Administrations submitted 60 business cases to the CIO Office for review and the Board's approval for budget submission. However, the Board did not start reviewing any IT investment until June this year and the Operating Administrations did not submit budget proposals until August. Due to the short timeframe, the reviews were limited to ensuring that required data were included in the submission, rather than verifying that the data were reliable and reasonable. In our opinion, more substantive, in-depth review of Operating Administration budget proposals is needed to prevent the reviews from being superficial and cursory.

The CIO Office plans to start the budget review process earlier next year. This early start, in conjunction with more experience in reviewing IT investment projects, should enable the Board to provide more insightful oversight of next year's budget requests.

- Establishing the Board with departmental membership represents a significant step forward. However, communications between the departmental Board and the Operating Administrations can be improved. This year, there was inadequate representation from the Operating Administrations when the Board met to discuss “cross cutting” IT investments or investments concerning a particular Operating Administration. For example, when the Board met to discuss annual IT budget requests, FAA was not represented to answer questions even though it was responsible for the largest budget component. Conversely, the departmental CIO Office was not represented when FAA met to make major IT investment decisions.

³ Status of FAA's Major Acquisitions, Report Number: AV-2003-045, June 26, 2003; and DOT Top Management Challenges, Report Number: PT-2003-012, January 17, 2003.

Network and E-government Security

DOT has thousands of computers on its internal networks. These systems contain sensitive information. DOT employees, contractors, grantees, and industry associations access these computers through either the Internet (front doors) or other network connections (back doors). In addition, DOT uses over 400 public web sites to provide E-government services to the public.

In FY 2002, we reported that DOT had enhanced security over the Internet (front door) connection points to DOT's internal networks⁴, but we found hundreds of unsecured telephone line (back door) connections. We also found that web sites operated by DOT were vulnerable to attack, and there was no security assurance for web sites operated by contractors. Further, DOT's process to report computer security incidents was not effective—some major attacks were not reported to the central authority in FY 2002.

During FY 2003, DOT made good progress securing “back door” network connections, reducing DOT's vulnerabilities to attack, and enhancing its security incident response capabilities. For example, the newly established departmental incident response center, with the cooperation of FAA's incident response center, detects, analyzes, and prevents hundreds of potential incidents from the Internet each day. We identified the following progress and remaining problems.

- We still found unsecured telephone line connections this year. These unsecured connections, which were located at one FAA facility, FAA Headquarters, and DOT Headquarters, allowed individuals located outside of DOT premises to make a direct connection to DOT network without password authentication or callback security to validate the calling source, as required by DOT policy. DOT took action by terminating or establishing security mechanisms on 197 dial-up connections. It is currently reviewing the remaining 71 connections. (See Table 1 on page 7.)

⁴ While the E-government web sites are connected to the Internet for public access, other DOT systems, which contain sensitive information, are connected to internal networks only. Entry points to internal networks are protected by security mechanisms, such as firewall security, to allow only authorized personnel to access the data.

Table 1
DOT Corrective Actions on Unsecured Dial-up Connections

-----	Number of Unsecured Dial-up Connections Identified	Corrective Actions	
		Number of Dial-up Connections Terminated or Security Requirement Established	Number of Dial-up Connections Being Reviewed
FAA Facilities	237*	170	67
FAA Headquarters	24	24	0
DOT Headquarters	7	3	4
Total	268	197	71

* 124 dial-up connections at one FAA facility were initially identified during FY 2002, and re-confirmed in FY 2003.

To prevent the problem from recurring, DOT plans to improve the process of authorizing network connections, conduct quarterly compliance reviews, and install additional monitoring devices on DOT networks, if funding permits.

- This year, DOT began evaluating security of contractor-operated web sites. Also, DOT-operated web sites are being regularly scanned to detect and eliminate vulnerabilities. For example, the number of vulnerabilities was reduced from 1,200 to 725 between June and July of this year. The enhanced security successfully protected DOT web servers from recent cyber worm attacks on the Internet.

However, this scanning effort was not enforced on the Operating Administrations' internal networks. We found incidents where software patches were not properly installed on FAA systems and transit financial systems. The CIO Office needs to ensure that Operating Administrations periodically scan their internal networks and timely install software patches.

- DOT enhanced its security incident reporting capability by issuing new guidance and establishing a Departmentwide incident response center to coordinate security reporting. However, DOT still did not report all major security incidents to the central authority—only 17 of 39 major incidents associated with viruses, denial-of-service attacks, or web defacements were reported to the central authority this year.

This occurred because DOT has not defined which incidents should be reported to the central authority. Failing to report these serious incidents could impair the central authority's effort to identify and respond to malicious cyber attacks against Federal government information resources in a timely manner.

The central authority has published clear guidance describing what types of incidents to report.⁵ DOT is revising its guidance to incorporate the central authority's reporting requirements. This action should result in improvement next year.

Systems Security

More than 60,000 insiders—employees, contractors, grantees, and industry associations—have access to DOT computer systems. According to the Federal Bureau of Investigation, insiders remain a major threat—about 50 percent of unauthorized activities against all computers were done by insiders during 2003.

In FY 2002, we reported that DOT systems were vulnerable to abuses or attack because most had not undergone the system security certification review. This review, which is performed by system owners in conjunction with the CIO Office, is a critical and effective security measure to reduce the insider threat. The review will determine whether individual systems are adequately secured commensurate with operational risks. We also found that DOT needed to develop a more reliable systems inventory and security cost estimates.

During FY 2003, DOT made progress by establishing a more reliable system inventory. However, DOT still has a long way to go in securing its computer systems from attack by insiders. In June 2003, OMB established a goal for agencies to increase system certification reviews from 47 percent (Governmentwide average as of September 2002) to 80 percent of their systems this year.⁶ In response, the CIO revised DOT's goal and focused significant attention and resources on completing certification reviews. However, even with additional attention, only 33 percent of DOT's systems will have completed certification reviews by September 2003. With a 33-percent completion rate, DOT is trailing behind the Administration's goal. We identified the following progress and problems:

- DOT conducted over 150 certification reviews this year. As a result, the number of DOT systems certified as adequately secured will have increased from 12 percent to 33 percent for all systems, and from 21 percent to 68 percent for mission-critical systems by the end of September 2003. In June 2003, DOT established a new performance goal to have 90 percent of total systems certified by July 2004. However, Operating Administration plans need to be adjusted to support this new goal, especially FAA which will have

⁵ Federal Computer Incident Response Center Reporting Requirements published at www.fedcirc.gov web site.

⁶ According to OMB, 47% of Government-wide computer systems were reported as having undergone the security certification review as of September 2002. (FY 2002 Report to Congress on Federal Government Information Security Reform, dated March 16, 2003)

to review and certify more than 80 percent of its systems in the next 9 months. The CIO Office is working with the Operating Administrations to implement the new goal, including target completion dates throughout the year. This represents a significant improvement from previous Operating Administration plans, which called for all systems to be certified by September 2006. However, this new commitment will be a challenge to DOT and will require significant resource commitments to complete reviewing two-thirds of the total systems in the next 9 months. (See Table 2 below.)

Table 2
System Security Certification Reviews

Operating Administration	Total Systems	Certified by September 2003	Systems to be Certified by July 2004
FAA	421	70	351
FHWA	25	14	11
FRA	22	6	16
FMCSA	19	6	13
RSPA	25	4	21
BTS	7	3	4
MARAD	12	7	5
FTA	7	7	0
OST	46	46	0
NHTSA	42	42	0
SLSDC	1	1	0
STB	3	3	0
Total	630	209	421
	===	===	===
Percentage	100%	33%	67%

- DOT needs to ensure that systems are tested during certification reviews. One of the key steps in performing a security review is the security testing and evaluation process, which determines the system's compliance with specified security requirements. However, we found little documentation supporting that system security controls had been tested and evaluated.

Specifically, we found that five out of eight systems we reviewed this year did not have adequate evidence to support the results of security testing. Security testing is required for both system security certification reviews and self assessments. Among these five systems, three have been certified as adequately secured and the other two have completed a self assessment, a building block for certification reviews. Our independent review of these systems found instances where controls were not functioning as intended. Further, we found one Federal Transit Administration system, which is used to manage billions of dollars in grant payments, was accredited for operations without having conducted any security testing or evaluation. Without testing or documenting the effectiveness of security controls, management cannot

have reasonable assurance that risks are properly mitigated or that identified security problems are corrected. The lack of testing may explain why we found significant control weaknesses in the systems that had undergone security certification reviews.

Another important step in performing a security certification and accreditation review is for the authorizing official to accept (accredit) the system for operations. Obtaining system accreditation from the correct authorizing official is critical because that official has to accept the risks of system operations. We selected 27 systems for review and found that 4 systems in 3 Operating Administrations (the Office of the Secretary, the Bureau of Transportation Statistics, and the Maritime Administration) were not accredited by authorized officials. DOT needs to perform quality assurance reviews on the Operating Administrations' system testing and accreditation.

- System owners still cannot support their security cost estimates and do not track security spending. During FY 2003, DOT provided training and tools to assist system owners to identify costs associated with implementing security. We examined security cost estimates for five major IT investments in three Operating Administrations (FAA, the Bureau of Transportation Statistics, and the Maritime Administration), totaling \$6.6 million. Again, we found that system owners did not use the DOT guidance and could not support the security cost estimates reported to OMB. Also, they could not provide data for actual security spending. As a result, there is little assurance that costs planned for securing computer systems are reliable or spent as intended.

In addition, we continue finding inconsistent security cost estimate reporting to OMB. The Operating Administrations are required to report their security cost estimates for both budget review (Exhibit 53) and IT investment project review (Exhibit 300). These submissions were reviewed by the CIO Office. However, we found that security cost estimates differed by approximately \$11 million between two submissions. DOT needs to implement comprehensive processes and procedures for security cost preparation and execution.

Protecting National-critical Assets

About 100 computer systems and facilities supporting FAA air traffic control operations are considered national-critical assets because they are essential to the Nation's defense, economic security, or public confidence. These systems are not accessible to the public because they operate on dedicated networks with no direct connections to the Internet, and they are housed within secured compounds. However, if not adequately secured individually, these systems are vulnerable to abuse and attack by insiders—employees, contractors, and industry associations.

In FY 2002, we reported that FAA needed to accelerate security certification reviews of these critical computer systems and facilities, and enhance en route center contingency plans. During FY 2003, FAA continued strengthening its “boundary protection” at network entry points. It also assisted the DOT CIO Office by recommending scanning tools and researching various smart card technologies for Departmentwide use. However, FAA made only limited progress accelerating security certification reviews for these critical systems and facilities, and enhancing en route center contingency plans. We plan to issue a separate report detailing the findings and recommendations to the FAA Administrator and the departmental CIO.

- During FY 2003, FAA increased system certification reviews from 36 to 56 for these critical systems. However, these certification reviews were not adequate to ensure that all significant security vulnerabilities were identified and resolved. These systems are developed in FAA's computer laboratory and deployed to multiple operational sites. FAA's certification reviews focused on evaluating security in the development systems at the computer laboratory, but did not include any operational systems in the field. We found that system security vulnerabilities existed at the operational sites. FAA needs to expand security certification reviews to cover operational systems, because configurations and security controls differ at each operational site.
- FAA also has not enhanced en route center contingency plans to meet the increased need for emergency preparedness. FAA relies on 20 en route centers to direct high altitude traffic, which also provide flight information to other facilities. En route centers are well equipped to deal with short-term emergencies to ensure the public safety. For example, all of the en route centers stayed intact and continued operations during the electricity blackout in September 2003. We plan to issue a separate report on FAA's readiness to deal with other emergencies, such as prolonged service disruptions at a facility or loss of the entire facility.

Personnel Security

Ensuring the integrity and reliability of the people authorized to access DOT systems is important. Training employees and conducting background checks help reduce personnel security risks. In FY 2002, we reported that DOT provided adequate security awareness training to all employees, but did not provide adequate specialized training to employees with significant security responsibilities because it had not completed identifying these individuals. We also reported that 24 percent of the contractor employees we sampled did not

receive background checks and the Operating Administrations did not consistently include background check requirements in contracts.

This year, DOT did a commendable job in improving security training. FY 2003 was the second year that DOT provided Departmentwide security awareness training, including special sessions for senior officials, system owners, and security administrators. DOT also provided specialized training to more than 600 individuals with information security responsibilities. In addition, DOT issued specific guidance for including background check requirements in all system-related contracts. However, as we reported in FY 2002, the lack of background checks on individuals performing sensitive computer work remains a persistent problem in DOT.

- DOT did not conduct background checks on 9 of the 20 contractor employees hired by the CIO Office to perform security certification reviews on DOT systems. This happened because of inadequate background check requests and the practice of waiving checks on temporary personnel. According to DOT policy, individuals should receive background checks in accordance with their job sensitivity. For example, employees and contractors performing sensitive system work are required to receive a high level background check (Background Investigation). However, the CIO office only requested low level background checks (fingerprint check) for its contractor employees because the work only lasted for 6 months.

Unfortunately, the DOT security office did not even perform fingerprint checks on 9 of the 20 contractor employees because they were mistaken as temporarily engaged to perform low risk duties such as janitorial services. As a result, those individuals were given inappropriate access to sensitive information such as system vulnerability assessments and threat analyses without any background checks. After we identified this deficiency, DOT management immediately began fingerprinting these individuals and stopped the practice of waiving fingerprint checks on temporary personnel.

We found similar incidents in the Operating Administrations. For example, 19 DOT and contractor employees performing sensitive work, such as maintaining network security, on the departmental accounting system and the transit grant management system did not receive adequate background checks.

While background checks do not guarantee a person's loyalty or trustworthiness, they provide valuable information to help management determine whether an employee should be given access to DOT systems. This is especially critical to DOT because DOT relies on about 18,000 contractor employees to develop new systems, operate existing systems, and perform

sensitive work such as managing network security, assessing computer vulnerabilities, or analyzing potential threats.

As we reported in FY 2002, FAA has made significant progress in enhancing background checks on its contractors in recent years. However, in spite of multiple audit reports and DOT guidance issued on this subject, the lack of background checks on contractor employees remains a persistent problem in other Operating Administrations. The lack of progress may be due to the fact that responsibilities for background checks are divided among multiple organizations. The CIO, the Office of Security, and individual contracting officers all have a role. The CIO, the Senior Procurement Executive, and the Director of Office of Security and Administrative Management need to work together to develop and enforce a specific plan to fix this problem next year.

System Contingency Planning

Contingency plans allow operations to continue in the event of service disruptions. In response to the increased need for preparedness, DOT has established emergency communications capabilities to allow senior managers to communicate, if DOT Headquarters became nonfunctional. However, DOT has not focused on ensuring business continuity in case key computer system operations are disrupted. This may hinder DOT's readiness to participate in the Administration's Forward Challenge exercise in 2004, which will test agencies' readiness for major IT outages. Specifically,

- DOT requires contingency plans to allow every mission-critical information system to rapidly and effectively deal with potential disruptions of business functions. In spite of today's increased need for emergency preparedness, only 26 percent of DOT systems have established contingency plans.

In addition, existing system contingency plans are often inadequate. For example, we selected 10 system contingency plans for review and found that the business impact analysis—the fundamental first step in planning for contingencies—was not performed for 4 systems. Without this analysis, management does not know how long it could continue business operations without computer systems support, which is critical to effective contingency planning. Also, two systems lacked off-site recovery capabilities. These systems support critical missions of tracking hazardous materials shipment and processing key accounting functions. In addition, management did not install proper equipment or perform tests at the recovery sites for three mission critical systems, which are used to management billions of dollars of grant payments and to compile essential transportation statistics. DOT management took immediate actions to correct the weaknesses by establishing off-site

recovery capabilities for the two systems and agreeing to conduct testing for the other three systems.

- DOT needs to develop guidance on minimum geographic distance for recovery processing sites. When selecting an off-site facility for system recovery processing, the alternate location should be at a reasonable distance away from the primary site to reduce the probability of losing both sites to the same disaster. We found that most DOT system owners use existing facilities operated by DOT or contractors as their recovery sites. While this may be cost-effective, it does not provide adequate risk mitigation because some recovery sites are too close to the primary sites.

For example, we found that geographic distances between the two sites are 10 miles for highway systems, 15 miles for transportation statistic systems, and 25 miles for transit systems. DOT relies on the highway and transit systems to manage more than \$30 billion of annual grant payments. With such close proximity, a single catastrophic event could take both processing sites out of service and seriously damage DOT's capability to support the highway and transit industries. In contrast, the recovery site for the departmental accounting system, which is used to manage \$10 billion of annual contract payment, is about 800 miles away from the primary processing site. DOT needs to provide guidance on minimum acceptable geographic distance between the primary and recovery sites.

RECOMMENDATIONS

1. We recommend that DOT Chief Information Officer implement the following actions to improve oversight of IT investments:
 - a) Develop specific criteria for selecting IT investment projects that should be reviewed by the departmental Investment Review Board, and direct the Operating Administrations to report the status of these investment projects to the DOT CIO Office.
 - b) Verify the reliability and reasonableness of IT budget requests before submission to OMB.
 - c) Ensure appropriate Operating Administrations are invited to attend the departmental Board review meetings, and ensure that DOT CIO Office staff attends the Operating Administrations' review meetings when appropriate.
2. We recommend that DOT Chief Information Officer incorporate corrective action plans and target completion dates for the following items in the FY 2003 Federal Managers' Financial Integrity Act report:

- a) Commit resources to fix the following repeated security weaknesses that we had included in previous security evaluation reports:
 - i. Require the Operating Administrations to provide support for security cost estimates.
 - ii. Work with the DOT Senior Procurement Executive and the Director of Office of Security and Administrative Management to ensure adequate background checks are performed on personnel performing sensitive computer work.
- b) Issue guidance to ensure complete reporting of major security incidents to the Federal Computer Incident Response Center.
- c) Improve the authorization process and perform quarterly compliance reviews of connections to DOT's internal networks; and install additional monitoring devices to detect unsecured telephone line (dial-up modem) connections. In addition, direct the Operating Administrations to perform vulnerability assessments of their computers to ensure timely installation of software patches.
- d) Direct the Operating Administrations to develop and implement plans to meet DOT's new goal of having 90 percent of all systems certified for adequate security by July 2004; perform quality assurance checks of system certification reviews to ensure adequate testing of security controls and proper accreditation by designated officials; and require the Operating Administrations to track security expenditures.
- e) Require FAA to develop and implement a timetable to conduct security certification reviews of air traffic control systems at operational sites.
- f) Direct the Operating Administrations to develop and implement plans to perform business impact analysis, develop contingency plans, and conduct testing to ensure business continuity in case computer system operations are disrupted. In addition, issue guidance on the minimum acceptable geographic distance between the primary and recovery processing sites.

MANAGEMENT COMMENTS

A draft of this report was provided to the DOT Chief Information Officer and the FAA Chief Information Officer on September 23, 2003. They agreed with the report's findings and recommendations. The DOT Chief Information Officer agreed to provide specific action plans and estimated completion dates in DOT's FMFIA submissions to OMB.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, within 30 days, please provide the specific actions taken or planned, including specific target dates for completion on the recommendations. In addition, we would appreciate receiving DOT's FMFIA corrective action plan upon its submission to OMB.

We appreciate the courtesies and cooperation of DOT and the Operating Administrations' representatives. If you have questions concerning this report, please call Ted Alves, Assistant Inspector General for Financial Management and Information Technology Audits, at (202) 366-1992, or Rebecca Leng, Deputy Assistant Inspector General for Information Technology and Computer Security Audits, at (202) 366-1496.

#

EXHIBIT A. OIG INPUT TO FISMA REPORT

For the last 2 years, DOT reported its information security program as a material internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA). This year, DOT made significant progress meeting its commitment to improve information security. The most noteworthy improvement DOT has made since we began the annual information security review in FY 2001 is in protecting its computer systems from attack by outsiders. For example, DOT enhanced its defense against intrusions from the Internet in FY 2002, and further reduced its vulnerability to attack this year by establishing a Departmentwide security incident response center. This center, in conjunction with FAA's incident response center, detects, analyzes, and prevents hundreds of potential intrusions from the Internet on a daily basis. Also, this year, DOT appointed a Chief Information Officer (CIO), increased the CIO's resources and influence, and developed a more reliable inventory of systems, all of which further strengthened DOT's information security protection.

However, DOT still has a long way to go in securing its computer systems from attack by insiders: employees, contractors, grantees, and industry associations. According to the Federal Bureau of Investigation, insiders remain a major threat—about 50 percent of unauthorized activities against all computers were done by insiders during 2003. DOT is not exempted from such a threat. We also found that DOT needs to enhance its contingency planning to ensure business continuity in case key computer system operations are disrupted for a prolonged period of time.

In view of the security weaknesses that still need to be corrected, DOT's information security program remains a material weakness and requires continued senior management attention. In FY 2004, it will be critical for the departmental CIO, with support from the Operating Administrators and their respective CIOs, to continue exercising leadership and providing the direction and oversight to ensure that the Operating Administrations develop adequate plans to correct the remaining weaknesses and execute those plans effectively. DOT's progress correcting the remaining weaknesses will help clarify whether the CIO has adequate authority, resources, and processes to ensure effective IT security and investment management controls.

A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.

Bureau Name	FY03 IT Security Spending (\$ in thousands)
--	--
Agency Total	--

OIG was not required to respond to this question.

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.

Bureau Name	FY03 Programs		FY03 Systems		FY03 Contractor Operations or Facilities	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
BTS	1	1	7	7	1	1
FAA	1	1	421	157	9	9
FHWA	1	1	25	25	7	7
FMCSA	1	1	19	19	6	4
FRA	1	1	22	22	6	6
FTA	1	1	7	7	2	1
MARAD	1	1	12	12	0	0
NHTSA	1	1	42	42	2	2
OST	1	1	46	46	3	3
RSPA	1	1	25	25	0	0
SLSDC	1	1	1	1	0	0
STB	1	1	3	3	0	0
Agency Total	12	12	630	366	36	33
Number reviewed by Office of Inspector General	--	12	--	27	--	2
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes		X	No		--
c. If yes, what methods are used? If no, please explain why.	This year DOT began evaluating contractor operated web sites. DOT used the NIST Self-Assessment guidance 800-26. Several systems located at contractor facilities have been certified and accredited. Others are currently going through certification or self-assessment reviews.					
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes		X	No		--
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	Yes		--	No		--
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.	During FY 2003, DOT revised its system inventory. The revised system inventory showed a reduction in the number of total computer systems (from about 1,200 to 630) and mission-critical systems (from 500 to 220) as a result of transferring two Operating Administrations to the Department of Homeland Security and consolidating systems inventory accounting. FAA accounted for two-thirds of the reduction. We consider the revised system inventory reasonable.					

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.

Bureau Name	FY03 Material Weaknesses			POA&Ms developed? Y/N
	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	
Department of Transportation (Agency Total)	1	1	<p>For the last two years, DOT reported its information security program as a material internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA). Since we began the annual computer security review of DOT's information security program in FY 2001, DOT has made significant progress protecting its systems from attack by outsiders. However, DOT still has a long way to go in securing its computer systems from attack by insiders. A critical and effective security measure to reduce this threat is to perform system certification reviews. However, only 33 percent of DOT systems will have undergone such reviews as of September 30, 2003. We also found that DOT needs to enhance its system contingency planning efforts.</p> <p>In view of the extensive remaining security weaknesses, DOT's information security program remains a material weakness and requires continued senior management attention. We have included recommendations in our annual information security independent evaluation report number (FI-2003-086), dated September 25, 2003 to help the Department correct the material weakn</p>	Yes

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	Yes	No
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	X (1)	--
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	X	--
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	X	--
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	X	--
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	X	--
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.	X (2)	--
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.	X	--
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.	X(3)	--

(1) In July 2003, we brought it to management's attention that not all systems with known security weaknesses had a POA&M. DOT took immediate corrective actions and agreed to have POA&Ms developed for all systems with an IT security weakness by September 30, 2003.

(2) System level POA&Ms are linked directly to the budget submission. However, as we reported this year, system owners can not support system security budget cost estimates and do not track spending to ensure that resources are spent as requested.

(3) DOT has implemented a process to prioritize security weaknesses, however, at this time, it is unknown whether the process has been effectively implemented.

<p>B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?</p>	<p>During FY 2003, The Secretary made progress by appointing a Departmentwide CIO and obtaining significant budget increases for the Office of the CIO. The Secretary also increased the CIO's influence over IT decisions by forming a departmental Investment Review Board (the Board). The CIO is a key member on the Board.</p> <p>Creation of the Board and enhancement of the CIO's influence should improve DOT's oversight of IT investments and security; however, it is too early to judge their effectiveness. Historically, the Operating Administrations have functioned independently on IT matters with little departmental direction. Also, the Review Board did not start reviewing IT investments until June this year. During FY 2004, at the request of the Senate Appropriations Committee, we plan to evaluate the effectiveness of the CIO's efforts to coordinate with the Operating Administrations in improving IT security and investment controls.</p>
<p>B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?</p>	<p>Yes. DOT policy requires Operating Administrations develop business case (Exhibit 300) for major IT investments that are reviewed by the CIO for concurrence. Non-major IT investments (with a lifecycle cost of less than \$150 million) are not subject to the same review process for concurrence. The Operating Administrations can and do make non-major IT investment decisions without CIO review and concurrence.</p>
<p>B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?</p>	<p>The Secretary has delegated the responsibility for developing and maintaining DOT's information security program to the CIO. The CIO Office has issued multiple implementation guidelines, including methodology to certify system security throughout the life cycles of individual systems. During FY 2003, the number of DOT systems certified as adequately secured will increase from 12 percent to 33 percent for all systems, and from 21 percent to 68 percent for mission-critical systems. Nonetheless, DOT is trailing behind the Administration's goal of having 80 percent of systems certified for adequate security by September 2003. To emphasize the importance of this task, DOT recently established a new goal to have 90 percent of all systems certified for adequate security by July 2004. However, Operating Administrations plans need to be adjusted to support this new goal. The CIO office is working with the Operating Administrations to develop work plans to meet this new goal.</p>
<p>B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please describe.</p>	<p>The Secretary delegated the responsibility of overseeing program officials' performance of practicing information security to the CIO. Both the CIO and program officials' performance are subject to our independent evaluation. According to the CIO Office, they conducted compliance reviews on the Operating Administrations' progress in developing security plans and certifying systems for meeting requirements. However, we could not verify the effectiveness of the CIO's compliance reviews because there was no documentation of the discussions or actions taken resulting from the reviews. In addition, DOT needs to improve the quality of security testing. We found that 5 out of 8 systems we reviewed this year did not have any documentation supporting the result of security testing. We recommended corrective actions in our independent evaluation report.</p>

<p>B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.</p>	<p>The creation of the Department of Homeland Security (DHS) has resulted in a major impact on DOT critical infrastructure security responsibilities. Since DHS is now the lead agency, DOT no longer has primary responsibilities for securing the critical infrastructure in the transportation sector. However, DOT is still responsible for securing about 100 air traffic control systems critical to the nation's infrastructure. For other security responsibilities, DOT has integrated its information security program with the continuity of operations program, but not the physical security program. During FY 2003, the CIO Office, in conjunction with DOT emergency staff, established emergency communications capabilities to allow senior managers to communicate, if DOT Headquarters became nonfunctional. The CIO Office is also monitoring the Operating Administrations' development of contingency plans for computer systems. However, as we reported this year, only 26 percent of DOT systems have contingency plans and some of these contingency plans were inadequate or had not been tested.</p>
<p>B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?</p>	<p>DOT has a separate office responsible for the physical security program, which reports to the Assistant Secretary for Administration. Both the Assistant Secretary and the CIO report to the Secretary. These two offices work together on joint projects, such as exploring use of the smart card technology to enhance access security (the Common Access Architecture Project). They also work together on developing the infrastructure in DOT's new Headquarters building.</p> <p>FAA also has divided these security responsibilities. The FAA CIO is responsible for leading system security certifications, and the Associate Administrator for Civil Aviation Security is responsible for leading physical security certifications. Both report to the FAA Administrator. The timetables for system and physical security certification reviews are not coordinated. While completion of system certification reviews has been accelerated to FY 2004, physical security certifications are still scheduled to be completed in FY 2009.</p>

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.

a. Has the agency fully identified its national critical operations and assets?	Yes	X	No	--
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	Yes	X	No	--
c. Has the agency fully identified its mission critical operations and assets?	Yes	X	No	--
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	Yes	X	No	--
e. If yes, describe the steps the agency has taken as a result of the review.	<p>Last year, DOT planned to use the Project Matrix methodology to identify interrelationships of mission-critical systems. DOT later concluded that it is not cost-beneficial to pursue the use of Project Matrix. Instead, DOT issued guidance for establishing and maintaining an inventory of general support systems and major applications. Using this guide, the Operating Administrations are required to record all their systems as either mission critical or non-mission critical, and to document any system information sharing, interfaces, interdependencies and interrelationships. DOT identified 222 mission critical systems and about 400 non-mission critical systems.</p> <p>DOT has identified about 100 mission critical air traffic control systems as essential to the nation's defense, economic security, or public confidence. These systems have national significance and need to be secured on a priority basis. DOT used the same inventory methodology in identifying interdependencies and interrelationships of these national critical systems.</p>			
f. If no, please explain why.	--			

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	During FY 2003, DOT established the Transportation Cyber Incident Response Center (TCIRC) to work with FAA's Computer Security Incident Response Center (CSIRC), and to coordinate Departmentwide reporting of cyber incidents to the central authority (FedCIRC). Reporting to law enforcement authorities is coordinated with the Office of Inspector General. However, DOT external reporting procedure is not consistent with FedCIRC guidance. The Operating Administrations reported a total of 69 incidents during FY 2003, of which 39 were major incidents. As we reported this year, DOT only reported 17 of 39 major incidents associated with viruses, denial-of-services attacks, or web defacements to FedCIRC.			
b. Total number of agency components or bureaus.	12			
c. Number of agency components with incident handling and response capability.	12			
d. Number of agency components that report to FedCIRC.	2 (DOT's TCIRC and FAA's CSIRC)			
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	DOT reported 15 incidents to FedCIRC within 1 to 10 days depending on the criticality of the incident. But 2 incidents were reported to FedCIRC more than 40 days after the occurrences.			
f. What is the required average time to report to the agency and FedCIRC following an incident?	DOT requires the Operating Administrations report serious incidents to TCIRC within 24 hours. DOT has agreed to establish a time requirement for reporting to FedCIRC.			
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	DOT oversees timely patch installation on DOT public-facing web servers through its weekly scanning which identifies the vulnerabilities that need to be patched. However, as we reported this year, the automatic scanning was not consistently performed on DOT's private networks. We found several incidents where DOT computers were vulnerable to attack because management did not install software patches timely.			
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes	X	No	--
i. If yes, how many active users does the agency have for this service?	DOT was given 75 account seats by FedCIRC for using this service. Currently, DOT has created 49 user accounts, but only 3 Operating Administrations (4 users) are actively using this service. Other Operating Administrations obtain software patches from manufactures directly.			
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes	--	No	X
k. Do these configuration requirements address patching of security vulnerabilities?	Yes	--	No	X

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access)

Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement
BTS	2	1	0
FAA	3	1	0
FHWA	28	1	0
FMCSA	1	0	0
FRA	4	1	0
FTA	0	0	0
MARAD	2	0	0
NHTSA	2	1	0
OST	26	12	1
RSPA	1	0	0
SLSDC	0	0	0
STB	0	0	0
Total	69	17	1

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

a. Bureau Name	b. Total Number of Systems	c. Number of systems assessed for risk and assigned a level or risk		d. Number of systems that have an up-to-date IT security plan		e. Number of systems certified and accredited*		f. Number of systems with security control costs integrated into the life cycle of the system		g. Number of systems for which security controls have been tested and evaluated in the last year		h. Number of systems with a contingency plan		i. Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
BTS	7	7	100%	3	43%	3	43%	7	100%	7	100%	2	29%	1	14%
FAA	421	180	43%	126	30%	70	17%	206	49%	164	39%	70	17%	70	17%
FHWA	25	14	56%	14	56%	14	56%	25	100%	14	56%	7	28%	7	28%
FMCSA	19	19	100%	6	32%	6	32%	19	100%	6	32%	6	32%	0	0%
FRA	22	22	100%	6	27%	6	27%	22	100%	6	27%	0	0%	0	0%
FTA	7	7	100%	7	100%	7	100%	7	100%	7	100%	3	43%	0	0%
MARAD	12	12	100%	7	58%	7	58%	12	100%	7	58%	5	42%	0	0%
NHTSA	42	42	100%	42	100%	42	100%	42	100%	42	100%	42	100%	17	40%
OST	46	46	100%	46	100%	46	100%	46	100%	46	100%	8	17%	8	17%
RSPA	25	25	100%	25	100%	4	16%	25	100%	25	100%	20	80%	0	0%
SLSDC	1	1	100%	1	100%	1	100%	1	100%	1	100%	1	100%	0	0%
STB	3	3	100%	3	100%	3	100%	3	100%	3	100%	3	100%	0	0%
Agency Total	630	378	60.0%	286	45.4%	209	33.2%	415	65.9%	328	52.1%	167	26.5%	103	16.3%

Based on our sample test, we did not identify any major discrepancies that would cause us to question the reliability of the performance measures reported by the CIO Office.

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.

Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
YES	YES	The CIO Office collects system security certification review information and POA&M data from the Operating Administrations on a quarterly basis. As we reported this year, the CIO Office needs to perform quality assurance reviews of data collected from the Operating Administrations. We found incidents that systems were certified as adequately secured without adequate security testing or evaluation. The lack of adequate testing may explain why we found significant control deficiencies in systems that had undergone security certification reviews.	YES. In FY 2002, DOT created an SES position—Associate CIO for Information Security. During FY 2003, the position was renamed as the Associate CIO for IT Programs with added responsibilities of capital planning and investment controls and enterprise architecture. The Associate CIO spent 60 percent of her time on security this year.	YES

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?

Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
62,565	62,565	100.0%	681	678	99.6%	DOT has done a commendable job in providing general security awareness training to more than 60,000 employees. FY 2003 is the second year that DOT provided Departmentwide security awareness training, including sessions directed to senior management, program officials, and system users. DOT also provided specialized training sessions such as network security to more than 600 individuals assigned with information security responsibilities.	\$ 413,374.00

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?

Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
BTS	3	Yes	Yes	Yes
FAA	24	Yes	Yes	Yes
FHWA	6	Yes	Yes	Yes
FMCSA	3	Yes	Yes	Yes
FRA	2	Yes	Yes	Yes
FTA	3	Yes	Yes	Yes
NHTSA	7	Yes	Yes	Yes
OST	10	Yes	Yes	Yes
RSPA	2	Yes	Yes	Yes

EXHIBIT B. SCOPE AND METHODOLOGY

During Fiscal Year 2003, we fulfilled the requirements under FISMA by reviewing DOT major financial systems, FAA air traffic control systems, and the newly established capital planning and investment control process for managing IT projects. In addition, we reviewed DOT's FISMA submission and performed sample reviews to ensure the reasonableness of key performance measures reported. We also provided input to DOT's FISMA report by answering questions specified by OMB.

We used the audit methodologies recommended by the General Accounting Office and the President's Council on Integrity and Efficiency, and guidelines issued by other Government authorities such as the National Institute of Standards and Technology. We used commercial scanning software to assess DOT's network and web vulnerabilities.

We performed our work throughout FY 2003 and focused on reviewing FISMA reporting between May 2003 and September 2003 at DOT and its Operating Administrations' Headquarters located in Washington, D.C. The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States.

We previously issued two audit reports on DOT's information security program in response to the legislative mandate of the Government Information Security Reform Act--DOT Information Security Program, Report Number FI-2002-115, September 27, 2002; and DOT Information Security Program, Report Number FI-2001-090, September 7, 2001.

EXHIBIT C. DOT COMPONENTS

Bureau of Transportation Statistics

Federal Aviation Administration

Federal Highway Administration

Federal Motor Carrier Safety Administration

Federal Railroad Administration

Federal Transit Administration

Maritime Administration

National Highway Traffic Safety Administration

Office of the Secretary

Research and Special Programs Administration

Surface Transportation Board

Saint Lawrence Seaway Development Corporation

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

THE FOLLOWING INDIVIDUALS CONTRIBUTED TO THIS REPORT.

<u>Name</u>	<u>Title</u>
Rebecca Leng	Deputy Assistant Inspector General for Information Technology and Computer Security
Nathan Custer	Project Manager
Philip deGonzague	Project Manager
Michael Marshlick	Senior Computer Scientist
Ping Sun	Senior Computer Scientist
James Mallow	Senior Auditor
Henry Lee	Computer Scientist
Gary Klauber	Computer Scientist
Cynthia Tims	Information Technology Specialist
Mitchell Balakit	Information Technology Specialist
Bradley Kistler	Information Technology Specialist
Jean Yoo	Information Technology Specialist