INFORMATION SECURITY PROGRAM

Department of Transportation

Report Number: FI-2005-001
Date Issued: October 1, 2004

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

Memorandum

Subject: ACTION: Audit of Information Security Program, Department of Transportation FI-2005-001

Date: October 1, 2004

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 the Federal Information Security Management Act (FISMA) of 2002, our audit objectives were to (1) assess DOT's progress in correcting weaknesses identified in last year's FISMA review, and (2) provide input to DOT's annual FISMA report by answering questions specified by the Office of Management and Budget (OMB). Our input to DOT's annual FISMA report is in Exhibit A.

This year, we tested a subset of DOT systems that had undergone system security certification reviews to determine whether DOT has complied with Government standards in assessing system risks, identifying security requirements, testing security controls, and accrediting systems as able to support business operations. In addition, we reviewed the reasonableness of DOT's continued reduction of computer systems in its inventory (from 630 to 485) during fiscal year (FY) 2004.

Our review was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Our scope and methodology are described in Exhibit B.

INTRODUCTION

FISMA requires Federal agencies to identify and provide security protections commensurate with the risk and magnitude of harm resulting from the loss of, misuse of, unauthorized access to, or modification of information collected or maintained by or on behalf of an agency. Because DOT maintains one of the largest portfolios of information technology (IT) investments of Federal civilian agencies, it is critical that DOT protects its systems and sensitive data. In FY 2004, DOT's information technology budget totaled about $2.7 billion.

DOT has 12 Operating Administrations (OA) (listed in Exhibit C) with 485 computer systems. DOT is also responsible for operating the air traffic control system, which has been designated as part of the Nation's critical infrastructure by the President (Homeland Security Presidential Directive 7, December 2003). DOT systems include safety-sensitive air traffic control and surface transportation systems, as well as financial systems that disburse over $50 billion in Federal funds each year.

RESULTS IN BRIEF

For the last 3 years, DOT has reported its information security program as a material internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA).[1] During FY 2004, DOT made a concerted effort to correct weaknesses identified in previous years. The most noteworthy improvements DOT has made since we began the annual information security review in FY 2001 include:

- Increased oversight of IT investment management and security controls. During FY 2004, the departmental Investment Review Board expanded its review of OA investment projects and directed OAs to evaluate cost saving opportunities by consolidating systems of common interests, such as grant management. The Office of the Chief Information Officer (CIO office) also performed more in-depth reviews of IT budget requests submitted by OAs than in prior years.

- Strengthened protection of DOT's network infrastructure against internal and external attacks. During FY 2004, DOT expanded its vulnerability checks to cover not only its public web sites but also computers on OA private networks. The CIO office also issued guidelines for configuring computers in a secure manner to prevent vulnerabilities.

- Improved integrity, confidentiality, and availability of DOT program operations that depend on computer systems support. During FY 2004, DOT

[1] A material internal control weakness is a significant deficiency in an agency's overall information systems security program or management control structure, or within one or more information systems that (1) significantly restricts the capability of the agency to carry out its mission, or (2) compromises the security of its information, information systems, personnel, or other resources, operations, or assets. The risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. (OMB Guidance on "FY 2004 Reporting Instructions for the Federal Information Security Management Act," M-04-25, August 23, 2004.)

increased the percentage of systems completing the security certification review from 33 percent to over 90 percent.

Although DOT has made significant progress, this report identifies security issues that require continued management attention. The most significant remaining issues are summarized below:

The CIO office and OAs need to better coordinate IT budget requests in order to more clearly describe the sources and uses of IT funds. This may require changes in how budget funds are allocated between the CIO office and the OAs. For example, an important DOT initiative is to consolidate multiple systems maintained by individual OAs in 11 common business areas. Historically, each OA made its own investment decisions and submitted separate budget requests to fund its system operations. Consolidating systems in these common business areas will require a more centralized approach, and the Department may have to adjust its IT project management and budget submission practices. For example, consolidation efforts may require the CIO office or one OA to take the lead, resulting in shifting budget requests among the OAs.

The FY 2006 budget will need to more clearly describe this consolidation effort and tie together the individual OA requests in each area so that oversight groups such as the Office of the Secretary, OMB, and congressional appropriators can understand the investments being made and the expected benefits of consolidating systems in each business area. At the request of the Senate Appropriations Committee, we are conducting an evaluation of the Department's IT budget submission and progress in enhancing IT investment controls and IT security. The report, which will be issued in the first quarter of FY 2005, will contain the results and specific actions needed to improve IT budget presentations, including the need to clarify project management and budget responsibilities of the CIO office and OAs.

The quality of security certification reviews needs to be improved. The Department has made good progress in completing security certification reviews during FY 2004. However, when we checked a sample of 20 systems, we identified one or more deficiencies in 14 cases. These deficiencies included inadequate assessments of the risks facing the system; lack of evidence that tests were performed and in one case, a test item that had been listed as "passed" failed when we re-tested it; incomplete presentations of remaining weaknesses to responsible senior officials; and approval to operate by senior officials who may not have adequate authority to correct the remaining problems. The CIO office needs to continue its efforts to enhance the quality of OA security certification reviews.

Air traffic control system security must be enhanced. During FY 2004, we issued an audit report concerning security and controls over air traffic control en route computer systems.[2] En route systems are used to control high-altitude (over 18,000 feet) traffic. The report concluded that while air traffic control en route computer systems have limited exposure to the general public, they need to be better protected. Two issues in particular deserve special attention. First, although the Federal Aviation Administration (FAA) had certified that the en route systems we reviewed were adequately secured, the reviews were limited to developmental systems located at FAA's Technical Center computer laboratory. Operational systems deployed to en route centers also need to be reviewed. FAA has agreed to review operational en route systems but, to comply with FISMA requirements, FAA needs to commit to reviewing all operational air traffic control systems—at en route, approach control, and airport terminal facilities—within 3 years. Second, FAA has agreed to identify a cost-effective contingency plan to restore essential air service in the event of a prolonged disruption of service at an en route facility. FAA will use the results of an alternatives analysis, due in December 2004, to identify a cost-effective alternative. FAA needs to commit to making the implementation of a robust contingency plan a priority.

Based on the progress the Department has made and the current status of the security program, we are of the opinion that the DOT's information security program should be considered a reportable condition.[3] We plan to continue reviewing DOT's computer security program, focusing particular attention on FAA's progress in strengthening security over air traffic control systems. DOT, and FAA in particular, needs to make certain that it follows through aggressively to implement corrective actions in order to prevent the security program from deteriorating into a significant deficiency next year. Progress completing certification reviews of air traffic control systems and progress implementing and testing an en route center contingency plan will be key measures of FAA's commitment to address these issues.

We make a series of recommendations on pages 19 through 21 of this report to help the Department further enhance its information security protection and oversight of its multi-billion dollar annual IT investments. The departmental CIO office agreed with our findings and recommendations. We have requested DOT to

[2] OIG Report Number FI-2004-078, "Audit of Security and Controls over En Route Center Computer Systems," August 9, 2004. OIG reports can be accessed on our website: www.oig.dot.gov. The Department has determined that this report contains Sensitive Security Information (SSI) as defined by 49 CFR Part 1520. Accordingly, it is not available for public inspection or copying. The regulations provide that, under the Freedom of Information Act (FOIA) and the Privacy Act, should a document contain both SSI and non-SSI information, the Department may disclose the document with the SSI information redacted, so long as this information is not otherwise exempt from disclosure under FOIA or the Privacy Act.

[3] A reportable condition is a security or management control weakness that does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management. (OMB Guidance on "FY 2004 Reporting Instructions for the Federal Information Security Management Act," M-04-25, August 23, 2004.)

provide written comments describing the specific actions it will take to implement the recommendations.

FINDINGS AND RECOMMENDATIONS

Management Controls

DOT, with an annual IT budget of about $2.7 billion, is responsible for one of the largest IT investment portfolios among civilian agencies. The Clinger-Cohen Act requires DOT to appoint a CIO responsible for ensuring cost-effective IT investments, including proper security protection. In FY 2003, we reported that DOT appointed a CIO and increased the CIO's influence over IT decisions by forming a departmental Investment Review Board (the Board). The Board, chaired by the Deputy Secretary, has the authority to approve, modify, or terminate major IT investments. DOT's ability to improve computer security is closely tied to the effectiveness of the IT review process because security must be considered when making investment decisions. Much of the value added by the establishment of the CIO office will come through its involvement in investment decisions.

Last year, we concluded that it was too early to judge whether these changes would substantially improve DOT's oversight of IT investments and security. Specifically, we were concerned that the Board had focused its reviews on department-wide IT projects, such as implementation of a new departmental accounting system, and had provided little oversight of OA-specific IT investment projects. This was inadequate, considering that over 90 percent of the Department's IT budget is appropriated directly to OAs and a number of their investments had experienced significant cost overruns and schedule delays in recent years. We were also concerned with the lack of substantive, in-depth review of OA information technology budget submissions and poor communications between the Board and the OAs.[4]

Last year, we recommended that the CIO office develop specific criteria for selecting high-risk IT investment projects for the Board to review, provide more insightful oversight of IT budget requests, and ensure proper OA representation at the Board's meetings and appropriate departmental representation at OA meetings. At the request of the Senate Appropriations Committee, we are also evaluating the

[4] Seventy percent (42 out of 60) of the business cases for major IT investments submitted in FY 2003 were initially rejected by the Office of Management and Budget due to a lack of proper alternative analyses, performance evaluations, and life-cycle cost estimates.

Department's progress in enhancing IT investment controls and IT security. The following summarizes the progress and improvements still needed.

The Board Needs a Better Process To Select Projects for Review

The Board has expanded its review of OA-specific IT investments. However, its review has focused on projects that are already considered troubled because they have experienced more than 10 percent cost increases or schedule delays. During FY 2004, the Board reviewed 10 IT projects managed by 7 OAs, including complicated air traffic control modernization projects. These projects were deemed "at risk" and selected for Board review primarily because they had a more than 10 percent increase in cost or schedule targets. However, other high-risk projects were not reviewed because they did not show a more than 10 percent cost or schedule overrun after having been "re-baselined."[5] These projects nonetheless still need senior management's close attention to prevent a recurrence of problems.

In recent years, we have issued several audit reports on FAA's major acquisitions involving extensive software development work that require senior management level attention.[6] We reported that of 20 major acquisitions reviewed, 13 projects had experienced schedule slips of 1 to 7 years, and 14 projects had experienced cost growth of over $4.3 billion (increasing from $6.8 billion to $11.1 billion). Yet, the list of projects reviewed by the Board in FY 2004 did not include many of those we reported as having cost and schedule problems. In response to our work, the Board added three of FAA's major acquisition projects to its watch list—the Wide Area Augmentation System (WAAS), the Standard Terminal Automation Replacement System (STARS), and the Integrated Terminal Weather System (ITWS).

While reviewing troubled projects is important, the Board also needs to monitor projects that have not yet exceeded the 10 percent threshold in order to prevent projects from becoming troubled. A key objective of the Board should be to prevent projects from breaching the threshold (10 percent overruns) and becoming "troubled." This is especially important considering that FAA is beginning new, costly, and complex acquisition programs such as the En Route Automation Modernization Program (ERAM), which will cost billions of dollars to implement, to provide new hardware and software for facilities that manage high altitude traffic. In September 2004, the CIO office updated its criteria for selecting at-risk projects for the Board's review, including projects re-baselined and projects

[5] The original cost estimates and planned implementation schedule displayed in business cases (also called Exhibit 300s) are referred to as "baselines" for project management. The original cost and schedule baseline on the 300 can be changed ("re-baselined") upon approval by the Office of Management and Budget.

[6] OIG Report Number PT-2004-006, "DOT Top Management Challenges," December 5, 2003, and OIG Report Number AV-2003-045, "Status of FAA's Major Acquisitions," June 26, 2003.

showing a negative trend. We will report the progress of using these new criteria in selecting investment projects for the Board's review in next year's report.

Better Cost Estimates for IT Investments Are Needed

This year, both the Board and the CIO office performed more substantive, in-depth reviews of OA information technology budget submissions. During FY 2004, the Department prepared 58 business cases, also called Exhibit 300s by OMB, for major IT investment projects, totaling $2.1 billion. These budget requests were submitted for review much earlier than last year, thus allowing a more substantive review by the CIO office. This early start, in conjunction with more experience in reviewing IT investment projects, helped strengthen DOT's investment management controls. However, we continue to find that cost estimates for IT investment projects lack adequate support despite the existence of departmental guidance.[7]

Project Management and Budget Responsibilities for IT Consolidation Initiatives Need To Be Defined

The Board provided more insightful oversight during the budget review process. However, the CIO office and OAs need to better coordinate IT budget requests in order to more clearly describe the sources and uses of IT funds. This may require changes in how budget funds are allocated between the CIO office and the OAs. For example, an important DOT initiative is to consolidate multiple systems maintained by individual OAs in 11 common business areas. Historically, each OA made its own investment decisions and submitted a separate budget request to fund its system operations. Consolidating systems in these common business areas will require a more centralized approach, and the Department may have to adjust its IT project management and budget submission practices. For example, consolidation efforts may require the CIO office or one OA to take the lead, resulting in shifting budget requests among the OAs.

The FY 2006 budget will need to more clearly describe this consolidation effort and tie together the individual OA requests in each area so that oversight groups such as the Office of the Secretary, OMB, and congressional appropriators can understand the investments being made and the expected benefits of consolidating systems in each business area. At the request of the Senate Appropriations Committee, we are conducting an evaluation of the Department's IT budget submission and progress in enhancing IT investment controls and IT security. The report, which will be issued in the first quarter of FY 2005, will contain the results and specific actions needed to improve IT budget presentations, including the need

[7] OIG Report MH-2004-068, "Investment Review Board's Deliberations on the Motor Carrier Management Information System," June 29, 2004.

to clarify project management and budget responsibilities of the CIO office and OAs.

Better OA Review of IT Investment Projects Is Needed

The communications between the Board and the OAs have improved significantly. During FY 2004, the Board expanded its membership to include OA representatives. The Federal Aviation Administrator has joined the Board as a voting member in reviewing and approving major IT investment projects. In addition, the Board created three additional members who will rotate among the remaining OAs. While the Board benefited from the OAs' input when reviewing major IT investment projects, more needs to be done to ensure that OA investment review boards operate effectively.

DOT guidance authorizes each agency to establish its own Board to review IT investment projects. The departmental Board reviews only major investments—projects exceeding certain dollar thresholds or those deemed to have a significant impact on departmental missions. IT investment projects not meeting these criteria are deemed non-major. These investment projects, totaling $600 million, should have been reviewed by OA Boards in accordance with the DOT policy. However, we found that non-major projects were not being adequately reviewed.

The CIO office needs to ensure that OAs follow departmental guidance when estimating IT project costs and OA Investment Review Boards adequately review and manage all IT investments.

Network and Internet (Web) Services Security

DOT uses over 400 public web sites to provide Internet services to the public and thousands of computers on its private networks to process sensitive information. Together, they form the IT infrastructure to support DOT missions. DOT has made significant strides in securing this infrastructure since we started performing annual computer security audits in FY 2001.

In FY 2001, we reported weaknesses in DOT's firewall security that allowed us to gain unauthorized access from the Internet to about 270 computers located within DOT's private network. In FY 2002, we reported that DOT had strengthened security over the Internet entry points (the "front door"). However, we found hundreds of unauthorized or unsecured telephone line connections to DOT networks (the "back door") and hundreds of vulnerabilities in DOT web sites, which made the web sites vulnerable to denial-of-service attacks or defacement. In FY 2003, we reported that DOT added security to its back-door network connections, established security incidents response centers, and started checking public web sites for potential vulnerabilities. However, we also reported that computers on DOT's private networks were not checked for potential vulnerabilities, and DOT did not report all major security incidents to the responsible Federal authority.

During FY 2004, DOT took corrective actions by requiring OAs to perform vulnerability checks on their network computers, issuing guidance for secure configuration (or setup) of computers, and reporting all major incidents to the Federal authority. However, we identified the following concerns associated with the OAs' vulnerability checks, configuration management, and security assurances from third-party contractors.

Vulnerability Checks Are Incomplete

The OAs' vulnerability checks did not cover all computers on their private networks, and vulnerabilities found were not always corrected in a timely fashion. For example, we found that FAA checked vulnerabilities on major computer servers but not on end-user computers. As a result, tens of thousands of workstations on its networks have not been checked for vulnerabilities. The same limitation also applied to the Merchant Marine Academy's workstations. We also found that there is a lack of prompt corrections of the vulnerabilities identified on public web sites and on the Federal Railroad Administration's private networks.

Configuration Management Controls Need Improvement

Configuration management controls need enhancement and enforcement. Proper configuration is key to preventing computer vulnerabilities.[8] FISMA requires each agency to develop specific IT security configuration requirements that meet its needs and to ensure compliance with them. During 2004, the CIO office issued security baseline standards for configuring computers using these five software packages: server-based Windows, Linux, Solaris, Cisco (router), and wireless devices such as the Personal Digital Assistants (PDA). OAs were required to configure their computers in accordance with these baseline standards by August 1, 2004.

While DOT is moving in the right direction to implement configuration management controls, it needs to issue configuration standards for additional commonly used software and to develop a process to ensure that the controls are implemented. The CIO office needs to develop configuration standards for at least three additional software packages commonly used to support DOT operations—PC-based Windows, the Oracle database, and web applications.

[8] For example, hackers can easily take total (root-level) control of a computer that is not configured with a password-protected system administrator account.

We estimate that three-quarters of the desk top computers on DOT networks use PC-based Windows software to store, process, and transmit data. The Oracle database is used in key application systems, such as the departmental accounting system (Delphi), the Federal Highway Administration's grant management system, FAA's labor distribution system, and the National Highway Traffic Safety Administration's defect investigation system. Web application software is used not only to program web sites, but also to serve as the front-door interface to key DOT systems. Vulnerabilities embedded in web application software could leave DOT systems open to attacks. For example, in FY 2003, we found web application vulnerabilities in the departmental accounting system that could have allowed intruders to access sensitive information. In FY 2004, one of DOT's web sites was defaced due to improper configuration of web application software. Both vulnerabilities have been eliminated. In response to our recommendations, the CIO office issued draft standards for secure configuration of the Oracle database on September 27, 2004 and for web applications on September 29, 2004.

Issuing security configuration standards alone is not enough to ensure computer security. As required by FISMA, agencies must establish an enforcement program to ensure adequate monitoring and maintenance of the established configuration standards. The CIO office needs to periodically verify OA compliance with the issued standards.

Web Service Contractors Did Not Provide Security Assurance

OAs did not obtain security assurance for contractor-operated web sites. DOT has over 400 public web sites, some of which are operated by third-party contractors. In FY 2002, we recommended that DOT require written assurance from third-party contractors that the outsourced DOT web sites are adequately protected from cyber attacks. In response to our recommendations, the Assistant Secretary for Administration issued a memorandum in February 2003 requiring that contractors provide written assurance that all systems operated on behalf of DOT had adequate security protections and that DOT could inspect their operations.[9]

More than a year later, we found DOT has not effectively implemented this requirement. During FY 2004, using commercial scanning software, we scanned 16 OA web sites that were operated by third-party contractors. We identified a total of 57 vulnerabilities (8 high and 49 medium).[10] The summary of the scanning result is shown in Table 1.

[9] DOT memorandum, "Information Security Requirements," February 13, 2003.

[10] High-risk vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium-risk vulnerabilities may provide an attacker with useful information, such as password files that they can then use to compromise a computer system.

Table 1. Scanning Result of DOT Third-Party Websites

Operating Administration*	Vulnerabilities Confirmed and Corrected		Number of Websites Scanned
	High	Medium	
FAA	0	4	1
FHWA	2	21	6
FMCSA	0	7	1
FRA	4	7	3
FTA	0	4	1
OST	1	2	2
RSPA	1	4	2
Total	**8**	**49**	**16**

* See Exhibit C for definitions of acronyms.

While OAs took immediate actions to eliminate all of these vulnerabilities, most could not provide us with security assurance from their contractors. We asked OAs to provide us with the written security assurance and any supporting documentation, such as the vendor's IT security plan, self-assessment results, or independent evaluation reports. The Federal Highway Administration provided us its contractors' IT security plans. The Office of the Secretary, the Federal Transit Administration, and the Federal Motor Carrier Safety Administration provided certification and accreditation packages prepared by DOT for these contractor-operated web sites, but not any contractor-provided assurance. Other OAs did not provide any evidence. Providing security assurance to DOT is part of each contract and should be enforced because the lack of assurance puts the integrity, confidentiality, and availability of DOT business operations at risk.

The CIO office needs to verify the completeness of OAs' vulnerability checks, ensure that timely corrective actions are taken by OAs, finalize software configuration standards for Oracle database and web applications, develop standards for PC-based Windows, check OA compliance with configuration standards, and require OAs to obtain annual security assurance from contractors operating DOT-sponsored web sites or terminate the contractors' services.

System Security

Historically, one of the persistent weaknesses concerning DOT's information security program was the lack of system security certification reviews. They are a critical and effective measure to ensure systems are adequately secured commensurate with their individual operational risks. DOT had trailed behind the Government average by having only 10, 12, and 33 percent of its systems complete such reviews during FY 2001, FY 2002, and FY 2003, respectively. In FY 2003, we also reported cases where systems were certified as secure without having been tested, systems were accredited for operations by personnel not in a position to do so, and estimated security costs were not supported or documented. We recommended that the CIO office perform quality assurance checks of OA security certification reviews.

During FY 2004, DOT made a concerted effort to increase the number of system security certification reviews and reported that 97 percent of its systems had completed such reviews. Meanwhile, DOT reduced its system inventory from 630 systems to 485 (a reduction of 145). FAA reduced its inventory from 421 systems to 285 (a reduction of 136)—94 percent of the total reduction. Table 2 shows the change in inventory between FY 2003 and FY 2004 and the number of systems certified by OA.

Table 2. DOT System Inventory Changes

Operating Administration*	**FY 2003 Total**	**FY 2004 Total**	**FY 2004 Certified**
BTS	7	4	4
FAA	421	285	274
FHWA	25	24	24
FMCSA	19	19	19
FRA	22	22	22
FTA	7	9	9
MARAD	12	12	11
NHTSA	42	38	38
OST	46	54	54
RSPA	25	15	15
STB	3	2	2
SLSDC	1	1	1
Total	**630**	**485**	**473**

* See Exhibit C for definitions of acronyms.

FAA stated that the overall reduction of 136 systems was primarily due to inventory consolidation, system additions, and system retirements. FAA provided documentation supporting the changes from last year. We reconciled FAA's system inventory to last year's record to ensure that all system components were accounted for. In addition, we reviewed the certification work performed on 20 systems to ensure the quality of the work. The following summarizes our review results.

A Significant Amount of Work Remains for Security Certification Reviews

While FAA provided adequate support to reconcile the inventory records between the 2 years, we found that it will require continued management support and monitoring to complete the remaining certification reviews.

- **Inventory adjustments were supported.** Based on our analysis, inventory consolidation accounted for the majority of system reduction. We selected nine systems from the consolidation listing for review and found that they all were properly incorporated as components (sub-systems) of other systems in FAA's inventory.

- **Systems remain to be certified.** Six of the 11 systems remaining to be certified in FAA's inventory record involve local area network systems installed at hundreds of locations. Since there is no assurance that network systems at all these locations have the same configuration or operate the same way, FAA may have to perform certification reviews at all installation sites. This could require a significant amount of work.

Quality of Security Certification Reviews Needs Improvement

Our sample review of 20 systems identified deficiencies in 14 cases. Deficiencies were in the areas of assessing system risk levels, testing security controls, informing senior management of remaining security weaknesses, and approving systems for operations through accreditation as shown in Table 3.

Table 3. Quality of System Security Certification Reviews

Systems Sampled* (Number of Systems)	Inadequate Risk Level Assessment	No Evidence of Security Testing	Failed Our Test	Weaknesses Not Summarized	Weaknesses Not Mentioned	Accredited By Inappro. Official
BTS Statistics Sys (1)	1	--	--	--	1	1
FAA: Air Traffic Control (5)	1	3	N/A	1	4	--
Others (5)	1	--	N/A	3	1	--
FHWA Network (1)	--	--	--	1	--	--
FTA Network (1)	--	--	--	1	--	--
FMCSA Network (1)	--	--	--	--	1	--
MARAD Financial (1)	--	--	1	1	--	--
NHTSA Safety (1)	--	--	--	1	--	1
OST: Network (2)	--	--	N/A	1	1	2
Telephone (1)	--	--	N/A	1	--	1
RSPA Network (1)	--	--	--	1	--	--
Total	**3**	**3**	**1**	**11**	**8**	**5**

* See Exhibit C for definitions of acronyms.
N/A=We did not select these systems for independent tests.

- The system risk level was not properly assessed for 3 of 20 systems we reviewed. This assessment is part of the overall system risk assessment and is critical to determining the level of security protection and degree of testing needed to certify that a system is adequately secured. The National Institute of Standards and Technology and DOT have issued specific guidelines directing OAs to perform such assessments based on the impact on agency business should the system operations be compromised. We found that FAA assigned a low-risk level to, and accordingly required low security protection and testing for, two important systems—an air traffic control surveillance system and a labor distribution system that is used to manage labor forces and costs. However, FAA had not performed the business impact analysis to justify the low-risk rating.

  We also found that the Bureau of Transportation Statistics (BTS) did not assign any risk level or perform any business impact analysis for a critical transportation statistics system. That system is widely used by DOT and the industry to set rates for essential air services and to monitor major trends in the transportation industry. Despite the lack of a risk assessment, BTS reported that the system was adequately secured commensurate with the associated risks.

- There was no evidence of testing for 3 of 20 systems we reviewed. One of the key parts of the security certification review is the security testing and evaluation process, which determines the system's compliance with specified security requirements. We did not find any documented evidence of security control testing for three of the five air traffic control systems we sampled.

For the seven systems outside of FAA and the Office of the Secretary, we randomly selected control items marked as “passed” on the evaluation sheets and subjected them to an independent testing. In one case—a Maritime Administration financial system—the item we tested failed in our presence. The system did not lock the user out after three unsuccessful logon attempts, as indicated in testing documents. This is a basic but important access control.

- Remaining security weaknesses were not summarized so that accrediting officials could easily evaluate remaining risks for 19 of 20 systems we reviewed. The final step in a security certification and accreditation review is for the authorizing official to accept (or accredit) the system as adequately secured commensurate with its associated risks to support business operations. The authorizing officials need to know what remaining risks and corrective actions are planned before approving the system for operations.

  All 20 systems we reviewed have remaining security weaknesses pending corrections, but in only one case were remaining risks clearly summarized in the signed certification letter. In 11 cases, the certification letter mentioned that risks remained and referred the official to an attachment that described the risks. However, the attachment (also called Plan of Actions and Milestones by OMB) is a low-level document detailing individual security weaknesses found and the progress of correction. It does not provide summary information the senior official needs to understand the remaining risks before accrediting the system for operations. In eight cases, the certification letter did not even mention that remaining risks were described in an attachment. Current DOT policy does not require risks to be summarized in the certification letter. However, because accepting the remaining risks is the key element in the accreditation process, we believe the risks should be clearly stated in the letter.

- Systems were not accredited for operations by the appropriate senior official for 5 of 20 systems we reviewed. Federal and DOT guidance requires the senior official who is primarily responsible for using a computer system (the system user) to accredit the system for operations. Obtaining system accreditation from the correct authorizing official is critical because this official has to accept the system risk (impact) on business operations and should also be able to allocate budget resources to secure the system. We found that three Office of the Secretary communication systems and a National Highway Traffic Safety Administration safety system were accredited by technical managers, rather than by senior officials at a high enough level to make budget trade-off decisions to allocate resources to address remaining problems. In addition, the BTS transportation statistics system had not been accredited by the system user organization, even though BTS reported it had been accepted for operations. All BTS provided was a certification statement approved by its CIO stating that the system had passed testing.

During FY 2004, the CIO office performed quality assurance checks on OAs' security certification work on 14 systems, but it did not share the review results with OAs. The CIO office needs to increase the number of quality assurance checks of OA security certification reviews, share the results with OAs to ensure that improvements are communicated widely, and issue guidance to ensure accrediting officials are properly informed of remaining security weaknesses.

We are also recommending that the CIO office require FAA to justify the low risk level of the air traffic control surveillance system and the labor distribution system, examine FAA's procedures for testing air traffic control systems security, modify its policy to ensure that accreditation statements are approved by appropriate senior officials, remove the BTS transportation statistics system from the list of accredited systems, and examine the security certification review process employed by BTS for appropriateness.

Protecting Critical National Infrastructure

The President designated the air traffic control system as part of the critical national infrastructure due to the important role commercial aviation plays in fostering and sustaining the national economy and ensuring the safety and mobility of citizens. FAA is responsible for ensuring that air traffic control facilities, systems, and operations are (1) protected from disruption from man-made or natural events, and (2) able to resume services in a timely manner if services are disrupted. Operational disruptions at any air traffic control facility have the potential to create significant delays and interruption of air service. Prolonged outages at major facilities, such as an en route center, would severely disrupt air traffic, causing significant economic losses and subjecting travelers to delays and inconvenience.

In FY 2003, we reported that FAA's security certification review of air traffic control systems was too limited to provide assurance that operational systems were adequately secure. The reviews covered only the developmental (prototype) systems operating at the FAA computer laboratory. FAA has agreed to develop a timetable to have all operational systems reviewed for adequate security but has not yet established a schedule.

During FY 2004, we issued an audit report concerning security and controls over air traffic control en route computer systems. En route systems are used to control high-altitude (over 18,000 feet) traffic. The report concluded that while air traffic control en route computer systems have limited exposure to the general public, they need to be better protected. We made specific recommendations to enhance system, physical, and network access security; reduce risks of en route service disruptions; strengthen FAA's overall contingency planning; and improve the security review process for air traffic control computer systems.

FAA management concurred with our findings and is taking corrective actions that, when fully implemented, will enhance the integrity and availability of en route computer system operations. In that regard, two important issues deserve special attention. First, although FAA had certified that the en route systems we reviewed were adequately secured, the reviews were limited to developmental systems located at FAA's Technical Center computer laboratory. Operational systems deployed to en route centers also need to be reviewed. FAA has agreed to review operational en route systems, but, to comply with FISMA requirements, FAA needs to commit to reviewing all operational air traffic control systems—at en route, approach control, and airport terminal facilities—within 3 years. Second, FAA has agreed to identify a cost-effective contingency plan to restore essential air service in the event of a prolonged disruption of service at an en route facility. FAA will use the results of an alternatives analysis, due in December 2004, to identify a cost-effective alternative. FAA needs to commit to making the implementation of a robust contingency plan a priority.

We are recommending that the departmental Investment Review Board monitor FAA's implementation of these corrective actions to ensure that FAA (1) completes security certification reviews of all operational air traffic control systems within 3 years and (2) implements and tests a cost-effective contingency plan to restore essential air service in the event of a prolonged service disruption at an en route facility. We plan to continue reviewing air traffic control security issues and FAA's progress correcting the deficiencies. We will report on the air traffic control system's security status in next year's FISMA report.

System Contingency and Continuity Planning

Contingency plans allow business operations that depend on information systems to continue operating during system service disruptions. In FY 2003, we reported inadequate contingency planning for DOT systems (only 26 percent of systems had such plans) and inadequate testing at recovery sites. In addition, we reported that, to reduce the probability of losing both sites to the same disaster, DOT needs to develop guidance on the minimum geographic distance between system primary and recovery processing sites. We found cases where the backup sites were within 10, 15, or 25 miles of the primary sites for systems critical to DOT operations.

During FY 2004, DOT emphasized this area and reported that about 93 percent of systems now have contingency plans. In May 2004, DOT participated in the

Forward Challenge Exercise. The exercise focused on testing the communications capability between the departmental and the OA command centers, in case the DOT Headquarters became uninhabitable. All DOT components participated in the exercise and tested the communications capability with cell phones and e-mails.

We reviewed the contingency plans for eight business application systems within four OAs. These systems are used to support a wide range of business functions. We found that two systems did not have off-site disaster recovery capabilities, and that three of the remaining six systems had no evidence of testing at the designated disaster recovery sites. Table 4 shows the results of that review.

Table 4. Contingency Planning for Selected Systems

Operating Administration*	Systems	Off-site Recovery Capability	Evidence of Testing
FAA	Cost Accounting	No	N/A
FAA	Labor Distribution	Yes	No
FAA	Logistics Support	Yes	Yes
FAA	Aircraft Safety Inspection	Yes	No
FAA	Human Resources	Yes	No
MARAD	Financial Management	Yes	Yes
NHTSA	Crash Investigation	Yes	Yes
BTS	Transportation Statistics	No	N/A

* See Exhibit C for definitions of acronyms.

In addition, we found that policy governing the physical distance between system primary and backup processing sites has not been completed. The CIO office plans to issue this policy by December 2004. However, some OAs plan to invest more money to further equip recovery sites that may not meet the minimum distance requirements.

The CIO office needs to ensure that OAs do not make uneconomic investments in recovery sites that could be superceded by the December 2004 policy and require OAs to develop and test off-site disaster recovery capabilities.

Personnel Security

Another persistent weakness concerning DOT's information security program was the lack of background checks on contractor personnel. Background checks are important because of the large number of contractor personnel (about 18,000) performing sensitive system work, such as air traffic control system development and maintenance, network security, and system security certification reviews. Background checks help to determine whether a particular individual is suitable for a given position. In FY 2003, we reported that DOT did not conduct background checks on contractor employees performing sensitive security work. As a result, contractor personnel were given inappropriate access to sensitive information, such as system vulnerability assessments and threat analyses, without any background checks.

During FY 2004, in response to our recommendations, DOT changed its practices by requiring background checks solely based on the sensitivity of the work and regardless of the contract length. Previously, checks were not performed if the contract term was for less than 6 months. DOT also established new procedures[11] requiring quarterly updates from OAs concerning contractor personnel, such as who began work, who had access to DOT facilities and systems during that quarter, and who previously had access but no longer needed access.

This year, we sampled 122 contractor personnel who were associated with the 20 systems we selected for review for background checks.[12] All individuals had received proper background checks commensurate with the sensitivity of their jobs.

RECOMMENDATIONS

To improve IT management controls, we recommend that the DOT CIO:

1. Require OAs to follow departmental guidance when estimating IT project costs.

2. Periodically review OA review board activities to ensure that they follow existing guidance and adequately manage their IT investments.

To improve network and Internet (web) security, we recommend that the DOT CIO:

3. Periodically verify that the OAs have performed adequate vulnerability checks and taken timely corrective actions on vulnerabilities identified.

4. Issue software configuration standards for PC-based Windows and finalize the configuration standard for the Oracle database and web applications.

5. Periodically check OA compliance with configuration standards.

[11] The Assistant Secretary for Administration memorandum to all heads of Operating Administrations and secretarial offices on May 17, 2004.

[12] In this audit, we limited the review of background checks to contractor personnel working on 20 computer systems. We have a separate audit underway with more comprehensive coverage of this issue.

6. Enforce the requirements that OAs obtain annual security assurance from contractors that host OA web sites or terminate these contractors' services.

To enhance the quality of OA system security certification reviews, we recommend that the DOT CIO:

7. Increase quality assurance checks of OA system certification work and communicate the review results to OAs to ensure that identified weaknesses are corrected timely.

8. Issue guidance requiring that remaining security weaknesses and needed corrective actions be summarized and presented to the responsible senior official when accrediting systems for operations.

9. Require FAA to justify the low-risk level assigned to one air traffic control surveillance system and the labor distribution system, and examine FAA's procedures for testing air traffic control system security.

10. Modify DOT guidance to ensure that accreditation statements are approved by appropriate senior officials, and require the Office of the Secretary and the National Highway Traffic Safety Administration to obtain accreditation approval from higher level senior officials in the user organization for the systems we identified.

11. Remove the BTS transportation statistics system from the list of accredited systems, examine the security certification review process employed by BTS for appropriateness, and obtain a new certification review.

To improve air traffic control system security, we recommend that the departmental Investment Review Board monitor FAA's implementation of the following corrective actions:

12. Complete security certification reviews of all operational air traffic control systems within 3 years.

13. Implement and test a cost-effective contingency plan to restore essential air service in the event of a prolonged service disruption at an en route facility.

To improve system contingency planning, we recommend that the DOT CIO:

14. Review OA disaster recovery plans to ensure all OAs develop and test off-site disaster recovery capabilities for critical business operations.

15. Ensure that OAs do not make uneconomic investments in recovery sites that could be superceded by future policy guidance to be issued governing the minimum distance between system primary and recovery processing sites.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

The CIO office reviewed a draft of this report and provided oral comments. CIO office officials stated that they were pleased that the report recognized the significant progress made this year to improve IT management and strengthen computer security. They also agreed with the report's findings and recommendations and stated they will provide written comments describing the specific actions they will take to implement the recommendations.

ACTION REQUIRED

In accordance with Department of Transportation Order 8000.1C, we would appreciate receiving your written comments within 30 calendar days. Please indicate the specific actions taken or planned for each recommendation and a target date for completion. You may provide alternative courses of action that you believe would resolve the issues presented in this report.

We appreciate the courtesies and cooperation of the Office of the Chief Information Officer and the Operating Administrations' representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1992 or Theodore Alves, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1496.

#

cc: Deputy Secretary
Federal Aviation Administrator
Martin Gertel, M-1

EXHIBIT A. OIG INPUT TO FISMA REPORT

2004 FISMA Report

Agency:	Department of Transportation
Date Submitted:	10/01/2004
Submitted By:	OIG

Contact Information:

Name:	Alexis M. Stefani
E-mail:	alexis.stefani@oig.dot.gov
Phone:	(202) 366-1992

To enter data in allowed fields, use password: fisma

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. **FY04 Programs**		**A.1.b.** **FY04 Systems**		**A.1.c.** **FY04 Contractor Operations or Facilities**		**A.2.a.** **Number of systems certified and accredited**		**A.2.b.** **Number of systems with security control costs integrated into the life cycle of the system**		**A.2.c.** **Number of systems for which security controls have been tested and evaluated in the last year**		**A.2.d.** **Number of systems with a contingency plan**		**A.2.e.** **Number of systems for which contingency plans have been tested**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
BTS	1	1	4	1	1	0	0	0.0%	1	100.0%	1	100.0%	0	0.0%	0	0.0%
FAA	1	1	285	10	12	12	10	100.0%	8	80.0%	7	70.0%	9	90.0%	5	50.0%
FHWA	1	1	24	1	2	2	1	100.0%	1	100.0%	1	100.0%	1	100.0%	1	100.0%
FMCSA	1	1	19	1	4	1	1	100.0%	1	100.0%	1	100.0%	1	100.0%	0	0.0%
FRA	1	0	22	0	2	1	0									
FTA	1	1	9	1	2	1	1	100.0%	1	100.0%	1	100.0%	1	100.0%	1	100.0%
MARAD	1	1	12	1	4	0	1	100.0%	1	100.0%	1	100.0%	1	100.0%	1	100.0%
NHTSA	1	1	38	1	2	1	1	100.0%	1	100.0%	1	100.0%	1	100.0%	1	100.0%
RSPA	1	1	15	1	0	0	1	100.0%	1	100.0%	1	100.0%	1	100.0%	1	100.0%
SLSDC	1	0	1	0	3	0	0									
STB	1	0	2	0	0	0	0									
OST	1	1	54	3	0	0	3	100.0%	3	100.0%	3	100.0%	3	100.0%	3	100.0%
Agency Total	**12**	**9**	**485**	**20**	**32**	**18**	**19**	**95.0%**	**18**	**90.0%**	**17**	**85.0%**	**18**	**90.0%**	**13**	**65.0%**

Comments:

A.1.c: The total number of contractor operated facilities (32) was reported by DOT. However, during our review we found that Operating Administrations are reporting the number of contractor operations or facilities inconsistently. For example, three Operating Administrations (FAA, FHWA, and RSPA) did not include contractor provided web services in the reporting, while others did.

A.2.a: Our sample review of 20 systems, which were reported as having completed C&A reviews, identified deficiencies in the areas of assessing system certification levels, testing security controls, informing senior management of remaining security weaknesses, and approving systems for operations (accreditation). As a result of our review, we concluded the BTS system was not properly reviewed, and made a specific recommendation for the DOT CIO to examine the security certification review process employed by BTS for appropriateness.

A.2.b: We did not find any funding requests, and associated security costs, for two systems in the Department's Exhibit 53 submission.

A.2.c: As stated in our audit report, we did not find any documented evidence of security control testing for three of the five air traffic control systems we sampled.

A.2.d. & A.2.e: We made specific recommendations to improve system contingency planning in our audit report.

A.3

A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

Statement	Evaluation
a. Agency program officials and the agency CIO have used appropriate methods 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.	Mostly, or 81-95% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Mostly, or 81-95% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Almost Always, or 96-100% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Almost Always, or 96-100% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	Yes
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

Comments:
A.3.a,b&c: We reviewed 18 contractor operations and found that 2 did not receive any security reviews. The others received C&A reviews (13), self assessments (2), and a SAS-70 review (1). We have concluded that all reviews complied with NIST 800-26.

A.3.d&e: DOT reduced its system inventory from 630 to 485 systems (a reduction of 145). FAA reduced its inventory from 421 to 285 systems (a reduction of 136)--94 percent of the total reduction. FAA provided support and stated the reduction was due mainly to system consolidation. We were able to reconcile the inventory records between the 2 years.

A.3.f: We agree with the number of programs and systems, however, as we commented under A.1.c., Operating Administrations did not consistently include contractor operated web sites in their inventories. We estimate that at least 9 contractor-operated web sites were not included in the number of contractor operations or facilities report by the CIO Office.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.

	FY04 Significant Deficiencies			
Bureau Name	**Total Number**	**Number Repeated from FY03**	**Identify and Describe Each Significant Deficiency**	**POA&M developed? Yes or No**
			None reported	
Agency Total	0	0		

Comments:
For the last 3 years, DOT has reported its information security program as a material internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA). During FY 2004, DOT made a concerted effort to correct weaknesses identified in previous years. Based on the progress the Department made, we are of the opinion that the DOT's information security program should be reported as a reportable condition.

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.
To enter data in allowed fields, use password: fisma

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

C.1

Statement	**Evaluation**
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Almost Always, or 96-100% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Almost Always, or 96-100% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, or 96-100% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Mostly, or 81-95% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Frequently, or 71-80% of the time
g. 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).	Rarely, or 0-50% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Sometimes, or 51-70% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Mostly, or 81-95% of the time

Comments:

C.e&f: The Department has developed a database to centrally track, maintain, and review the POA&Ms. However, because Operating Administrations are not consistently updating the database, the centrally maintained POA&M information is not always reliable. OIG found inconsistent information between the database and the hard-copy POA&Ms prepared by Operating Administrations. The CIO office agreed to work with Operating Administrations to enhance the POA&M database.

C.g: Per OMB guidance, we reviewed the POA&Ms for 20 systems and found that project IDs, which enable OMB to tie POA&Ms directly to the system budget requests, were missing for 15 systems. According to the CIO office, this information will be added.

C.i: We sampled 4 systems which received audit coverage in FY 2004 and found critical findings were not incorporated into the system's POA&Ms in 2 cases.

C.1 OIG Assessment of the Certification and Accreditation Process

Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
As stated in our audit report, the Department has made good progress in completing security certification reviews during FY 2004. However, when we checked a sample of 20 systems, we identified deficiencies in 14 systems. The deficiencies were in the area of assessing systems risks; testing security controls; informing management of remaining weaknesses; and approving systems for operations. The CIO office agreed to continue its efforts to enhance the quality of OA security certification reviews. We also identified the need for continued departmental management support and monitoring to complete the remaining certification reviews at FAA. While FAA certified air traffic control systems security, the reviews were limited to developmental systems located at FAA's Technical Center computer laboratory. Operational systems deployed to air traffic control facilities also need to be reviewed. To comply with FISMA requirements, FAA needs to commit to reviewing all operational air traffic control systems—at en route, approach control, and airport terminal facilities—within 3 years. Six systems remaining to be certified by FAA involve local area network systems installed at hundreds of locations. Since there is no assurance that network systems at all these locations have the same configuration or operate the same way, FAA may have to perform certification reviews at all installation sites.	Satisfactory

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	**Evaluation**
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	**Yes**	
a. Windows XP Professional		
b. Windows NT		
c. Windows 2000 Professional		
d. Windows 2000		
e. Windows 2000 Server		
f. Windows 2003 Server		
g. Solaris		
h. HP-UX		
i. Linux		
j. Cisco Router IOS		
k. Oracle		
l. Other. Specify:		
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	

Comments:
D.1 a-l: During 2004, the CIO office issued security baseline standards for configuring computer systems using the following 5 software packages; server-based Windows, Linux, Solaris, Cisco (router), and wireless devices (PDA). As stated in our audit report, while DOT is moving at the right direction by implementing these configuration management controls, we identified two enhancement needs—issuing configuration standards for additional commonly used software and developing an enforcement process. Since DOT is in the an early stages of implementing these standards, we plan to perform a more detailed review in FY 2005.

Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	**Evaluation**
a. The agency follows documented policies and procedures for reporting incidents internally.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Almost Always, or 96-100% of the time

E.2.

E.2. Incident Detection Capabilities.

	Number of Systems	**Percentage of Total Systems**
a. How many systems underwent vulnerability scans and penetration tests in FY04?	369	

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

DOT uses Foundstone scanning software to regularly scan its 400 websites and about 14,000 computer systems on OAs internal networks.

Comments:

E.2.a: DOT reported that 369 IP-based systems underwent vulnerability scans as part of its C&A requirements. We generally concurred with this statement based on our sample review of system certification reviews.

E.2.b: DOT has effectively followed applicable policies and procedures for reporting incidents internally and externally to law enforcement and to the US-CERT. DOT also used Foundstone scanning software to regularly scan its 400 websites and about 14,000 computer systems on Operating Administrations' internal networks. However, as stated in our audit report, the vulnerability checks (scans) did not cover all computers on Operating Administrations' private networks, and vulnerabilities found were not always corrected in a timely manner.

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.						
	F.1. **Number of Incidents, by category:**			**F.2.** **Number of systems affected, by category, on:**		
	F.1.a **Reported internally**	**F.1.b.** **Reported to US-CERT**	**F.1.c.** **Reported to law enforcement**	**F.2.a.** **Systems with complete and up-to-date C&A**	**F.2.b.** **Systems without complete and up-to-date C&A**	**F.2.c.** **How many successful incidents occurred for known vulnerabilities for which a patch was available?**
	Number of Incidents	**Number of Incidents**	**Number of Incidents**	**Number of Systems Affected**	**Number of Systems Affected**	**Number of Systems Affected**
I. Root Compromise	2	0	0			
II. User Compromise	0	0	0			
III. Denial of Service Attack	0	0	0			
IV. Website Defacement	5	5	5			
V. Detection of Malicious Logic	5	5	0			
VI. Successful Virus/worm Introduction	379	338	0			
VII. Other	0	0	0			
Totals:	391	348	5	0	0	0

Comments:

The totals provided in F.a.b and F.1.c. were provided by the Office of the CIO. However, according to US-CERT, DOT reported a total of 3,125 incidents in FY 2004. According to the CIO office, the difference is a result of different methods of categorizing an "incident." For example, the CIO office reports a virus as one incident, while the US-CERT reports the number of machines affected by the virus.

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
59,867	58,413	98	445	445	100	See Comment Box Below	$463,616

G.2.

	Yes or No
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	Yes

Comments:

G.1.a,b,c,d: This information was provided by Office of the CIO. OIG generally concurs with the reported information based on our review of training records provided.

G.1.e: DOT sponsored training in the areas of computer forensics, wireless security, intrusion detection, user awareness, identity theft, privacy, contingency planning, certification & accreditation, designated approving authority, and risk management. On-site vendor training (CISSP), and computer-based training (system security administration, user awareness) were also provided.

EXHIBIT B. SCOPE AND METHODOLOGY

During fiscal year (FY) 2004, we fulfilled the requirements under FISMA by reviewing DOT major financial systems, FAA air traffic control systems, and the implementation of IT capital planning and investment control procedures and DOT's modernization plan (Enterprise Architecture). In addition, we sampled 20 OA systems that had undergone security certification reviews to determine whether the OAs have complied with Government and DOT standards in assessing system risks, identifying security requirements, testing security controls, and accrediting systems to support business operations.

We reviewed the reasonableness of DOT's continued reduction of computer systems in its inventory (from 630 to 485) during FY 2004 and assessed DOT's progress in correcting weaknesses identified in last year's FISMA review. We also provided input to DOT's FISMA report by answering questions specified by the Office of Management and Budget.

We used the audit methodologies recommended by the Government Accountability Office, and guidelines issued by other Government authorities such as the National Institute of Standards and Technology. We used commercial scanning software to assess contractor-operated web site vulnerabilities.

We performed our work throughout FY 2004 and focused on reviewing FISMA reporting between July 2004 and September 2004 at DOT and OAs' 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 and included such tests as we considered necessary to provide reasonable assurance of detecting abuse or illegal acts.

We previously issued three audit reports on DOT's information security program in response to the legislative mandate of the Federal Information Security Management Act (FISMA), formerly the Government Information Security Reform Act (GISRA). They are "DOT Information Security Program," Report Number FI-2003-086, September 25, 2003; "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 OPERATING ADMINISTRATIONS

Bureau of Transportation Statistics (BTS)

Federal Aviation Administration (FAA)

Federal Highway Administration (FHWA)

Federal Motor Carrier Safety Administration (FMCSA)

Federal Railroad Administration (FRA)

Federal Transit Administration (FTA)

Maritime Administration (MARAD)

National Highway Traffic Safety Administration (NHTSA)

Office of the Secretary (OST)

Research and Special Programs Administration (RSPA)

Surface Transportation Board (STB)

Saint Lawrence Seaway Development Corporation (SLSDC)

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

THE FOLLOWING INDIVIDUALS CONTRIBUTED TO THIS REPORT.

Name	**Title**
Rebecca Leng	Deputy Assistant Inspector General for Information Technology and Computer Security
Nathan Custer	Project Manager
Ping Sun	Project Manager
Philip deGonzague	Project Manager
Michael Marshlick	Computer Scientist Advisor
James Mallow	Senior Auditor
Henry Lee	Senior Computer Scientist
John Johnson	Senior Information Technology Specialist
Mitchell Balakit	Information Technology Specialist
Bradley Kistler	Information Technology Specialist
Jean Yoo	Information Technology Specialist
Aaron Nguyen	Computer Scientist
Pinaki Sandra	Information Technology Specialist