Memorandum

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

Subject: ACTION: Report on Information Security Program, DOT FI-2002-115

Date: September 27, 2002

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply to Attn. of: Meche: x61496

To: Acting Chief Information Officer

This report presents the results of our audit of the information security program at the Department of Transportation (DOT). Our audit objective was to respond to the legislative mandate of the Government Information Security Reform Act (GISRA), which requires an annual independent evaluation of agencies' information security programs. In addition to this report, we provided input (Exhibit A) to DOT's GISRA Executive Summary by answering 12 questions specified by the Office of Management and Budget (OMB). Our scope and methodology are discussed in Exhibit B.

INTRODUCTION

GISRA requires Federal agencies to identify and provide security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, information collected or maintained by or on behalf of an agency. DOT, with $3.6 billion in planned expenditures in Fiscal Year (FY) 2003, has one of the largest information technology investments of all Federal civilian agencies. About 70 percent of FY 2003 expenditures are for the Federal Aviation Administration (FAA), 18 percent are for the Transportation Security Administration (TSA), and 8 percent are for the U.S. Coast Guard (Coast Guard). The Administration has identified TSA and the Coast Guard as component agencies to be transferred to the Department of Homeland Security.

DOT has 15 Operating Administrations (Exhibit C). Last year, DOT reported it had about 1,200 computer systems, including safety-sensitive air traffic control systems, Coast Guard search and rescue systems, and financial systems supporting the accounting for and distribution of billions of dollars in Federal funds. DOT identified the systems and facilities used to support air traffic control, Coast Guard search and

rescue and marine safety operations, as well as the Saint Lawrence Seaway, as its infrastructure-critical systems and assets.

To provide Electronic-government (E-government) services, DOT has more than 200 web sites with about 1 million web pages accessible through the Internet. DOT uses these web sites to conduct business, such as accepting payments, or to disseminate information, such as motor carrier safety records.

During FY 2002, the Office of Inspector General (OIG) continued its focus on network security, systems security, infrastructure-critical systems and asset protection, E-government (web) security, and personnel security. For this year's GISRA reporting, we included the additional category of management controls to emphasize the importance of management commitment to information security.

RESULTS IN BRIEF

Last year, DOT reported its information security program as a material internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA). During FY 2002, DOT made a strong management commitment to improve information security by developing performance measurements in the E-government scorecard, issuing additional security guidance, and enhancing its network defense against intrusions from the Internet. However, more progress is needed to secure individual systems to reduce unauthorized access to DOT's private networks (insider threats).[1] DOT agreed to focus on individual systems security during FY 2003.

The Secretary is committed to having all DOT mission-critical systems[2] reviewed and certified for adequate security by December 2005. However, DOT needs to complete its work to update the systems inventory, finish identification of all mission-critical systems, and develop detailed schedules for certification reviews. DOT progress and remaining challenges are summarized below.

- ***Management Controls***: The Clinger-Cohen Act requires establishment of an agency Chief Information Officer (CIO) responsible for acquiring and managing information technology resources. GISRA further directs the agency CIO to develop and maintain an agencywide information security program, including effective implementation of information security policies, procedures, and control techniques. DOT has not had an agency CIO since January 2001. Because of this,

[1] For security reasons, specifics concerning the weaknesses and vulnerabilities we identified and our audit procedures are not discussed in this report, but were provided to DOT managers during the audits.

[2] DOT identified about 500 systems (mission-critical) that requires special security attention due to the risk and magnitude of the harm from unauthorized access. About 100 of these mission-critical systems are identified as essential to the nation's defense, economic security, or public confidence (infrastructure-critical) and need to be secured on a priority basis.

the Secretary delegated the authority to administer information security requirements to the Acting CIO.

DOT needs to continue enhancing its information security program. During FY 2002, DOT incorporated information security as a performance metric in the E-government scorecard for implementing the President's Management Agenda. The CIO office also issued security guidance on network security, cyber incident reporting, and the capital planning process. However, Operating Administrations have not effectively implemented the guidance.

The lack of effective implementation of the CIO office guidance has been a long-standing problem in DOT since passage of the Clinger-Cohen Act in 1996. Unlike some of its counterparts in other Federal agencies, the DOT CIO office does not have budget or performance evaluation authority over the Operating Administrations to oversee implementation.[3] Until it is clear that there are management and budget consequences, the Operating Administrations are likely to continue the current practice of not effectively implementing guidance. To this end, we are recommending that the Deputy Secretary establish the CIO's authority and clarify the consequences for not implementing the CIO office's security guidance.

- ***Network Security***: DOT employees, contractors, grantees, industry associations, and the public can access DOT computers through various network entry points, such as through the Internet (front doors). Business associates also can access DOT computers through other means such as direct network connections (back doors). During FY 2002, DOT enhanced security over its front doors; however, controls over back door entry points and the cyber incident reporting process need to be strengthened. For example, at one FAA facility, we found three unsecured network connections to contractor sites and about 300 unauthorized telephone line (dial-up) computer connections.

  During FY 2002, DOT reported more than 25,000 cyber incidents to the Federal Computer Incident Response Center without sufficient analyses to determine whether these incidents were caused by intrusion activity or by innocent acts such as making an error when entering passwords. Meanwhile, we found significant incidents were not reported as required. For example, 3 of 10 web defacements were reported. We recommend that the CIO office develop action plans to oversee Operating Administrations' implementation of network security and cyber incident reporting guidance.

[3] For example, in the Department of Agriculture, no appropriated funds may be used to acquire new information technology systems or upgrades without the approval of its CIO. In the Department of Commerce, the CIO participates in the performance appraisal of bureau CIOs.

- ***System Security***: More than 100,000 insiders are authorized to access computer systems on DOT's private networks. DOT systems are vulnerable to these insiders because most of these systems have not undergone security certification reviews to ensure the integrity, availability, and confidentiality of systems operations. According to the Federal Bureau of Investigation (FBI), about 50 percent of unauthorized access activities in FY 2001 were by insiders.

.

  The Secretary established a goal to have all 561 mission-critical systems certified and accredited for adequate security by December 2005. This is a major challenge for DOT because only 123 mission-critical systems, or 22 percent, have been certified and accredited as of September 2002.

  We also found that DOT needs to develop a reliable systems inventory. This year, DOT reported 677 systems, a drop of 519 systems from last year, because Operating Administrations used inconsistent methodologies to inventory systems. A reliable systems inventory is essential for developing certification schedules and resource estimation.

  Proper development and reporting of budget estimates are needed to ensure information security is adequately funded. This year, DOT reported $103 million in security cost estimates. However, Operating Administrations did not use DOT guidance in estimating systems security costs and could not support the cost estimates submitted to OMB. We recommend that the CIO office develop action plans to update systems inventory, schedule mission-critical systems to undergo certifications reviews, and oversee Operating Administrations' development of cost estimates.

- ***Infrastructure-Critical Systems and Asset Protection***: DOT identified about 100 systems and facilities supporting FAA air traffic control operations, the Coast Guard search and rescue and marine safety missions, and the Saint Lawrence Seaway as essential to the Nation's defense, economic security, or public confidence (infrastructure-critical). Last year, we reported that DOT did not adequately consider system interdependencies when identifying infrastructure-critical systems, Coast Guard did not have an adequate disaster recovery capability for its search and rescue systems, and FAA needed to accelerate its plan to eliminate physical security vulnerabilities.

  During FY 2002, Coast Guard enhanced its disaster recovery capability and DOT assigned a higher priority to enhance network security than to protect infrastructure-critical systems because of pending presidential direction on

securing critical infrastructure.[4] This year, we identified additional concerns with FAA's efforts to secure air traffic control systems.

FAA certified 36 infrastructure-critical air traffic control systems for adequate security, which represented only about half of its planned accomplishments. FAA stated that it focused systems certification reviews on new systems instead of legacy systems. Rather than accelerate its timetable, FAA delayed the planned certification of physical security at air traffic control facilities from FY 2006 to FY 2009 due to funding constraints. We also discovered that FAA needs a better contingency plan to ensure continued air traffic control operations if systems were shutdown for extended periods.

Specific recommendations to enhance security within FAA will be included in a separate report. For this report, we recommend that the CIO office include FAA's corrective action plans in the FY 2002 FMFIA submission to OMB and Congress.

- ***E-government (Web) Security***: Web security and privacy protection are essential for E-government services. Attacks on Government web sites could result in embarrassment to agencies (web sites defaced), inconvenience to the public (web servers out of service), or disruptions to business (reports to meet regulatory requirements deleted). During FY 2002, DOT made good progress to better protect the public's privacy. DOT also initiated proactive actions to identify and correct vulnerabilities on web systems. Notwithstanding, we identified 453 vulnerabilities on 175 DOT web servers, 66 percent of which were on FAA and Federal Highway Administration (FHWA) web sites. As of September 10, 2002, the Operating Administrations already had corrected 435 of these vulnerabilities.

  DOT also has at least 35 web sites that operate on third-party computers. However, service providers were not required to provide assurance that DOT web sites are adequately protected. During FY 2002, one of these sites was defaced. We also found information labeled "For Official Use Only" and sensitive security information on DOT's public web sites. The Operating Administrations promptly removed these documents. Specific recommendations for improving web security will be included in a separate report.

- ***Personnel Security:*** Our review focused on background checks because about 18,000 contractor employees are working on DOT systems. Since we first reported concerns on background checks, DOT issued multiple memoranda for corrective actions. This year, we sampled 178 contractor employees and found 43 (24 percent) individuals who did not receive background checks, including people

[4] The President's cyber strategy is expected to be finalized later this year.

occupying sensitive positions. We also sampled 13 contracts from 5 Operating Administrations and found 3 Coast Guard contracts did not contain contractual requirements for background checks. We recommend that the CIO office work with the procurement and security officials to develop a plan to ensure that background checks on contractor employees are performed timely.

In view of the existing security weaknesses, we concluded that the DOT information security program remains a material weakness and requires continued senior management attention. In last year's GISRA report,[5] we recommended that DOT develop policies and guidance for correcting material weaknesses. While DOT developed specific guidance, effective implementation by the Operating Administrations has not occurred. To ensure proper followup and implementation, we are recommending that the Deputy Secretary provide the CIO office with more authority to oversee the information security program and that the CIO office develop new corrective action plans in the FY 2002 FMFIA submission to OMB and Congress. The DOT Acting CIO agreed with our findings and recommendations.

RESULTS

Management Controls

DOT has not had an agency CIO since January 2001. Because of this, the Secretary delegated the authority to administer information security requirements to the Acting CIO. The Acting CIO chairs the CIO Council, which is comprised of CIOs from each Operating Administration. However, the DOT CIO office does not have budget or performance evaluation authority over Council members who report to the Administrators of each Operating Administration.

The Acting CIO is assisted by an Associate CIO for Information Security who is responsible for maintaining an agency-wide security program and issuing security guidance. We found that DOT made a strong commitment to improve information security by developing performance measurements in the E-government scorecard, issuing additional security guidance, and enhancing its network defense against intrusions from the Internet. However, effective implementation of security guidance needs management attention throughout DOT.

- **DOT increased its management commitment to information security.** The CIO office provided televised training sessions to all DOT employees and developed a security performance measurement program as part of the Secretary's E-government scorecard. A key element in the scorecard is to complete

[5] DOT Information Security Program, Report Number: FI-2001-090, September 7, 2001.

certification and accreditation reviews of 50 percent of mission-critical systems by September 2003. Accomplishing this goal will reduce unauthorized insider access.

- **DOT needs to establish the CIO's authority to enable effective implementation of the information security program.** DOT reported the information security program as a material weakness in its FY 2001 FMFIA submission to OMB and Congress. In its submission, the CIO office specified four corrective actions to develop (1) a security performance measurement program, (2) network security guidance, (3) the cyber incident reporting program, and (4) the capital planning process for information security. While the CIO office issued security guidance as planned, Operating Administrations have not effectively implemented the guidance. We continue to find unsecured network connections, inaccurate reporting of significant cyber incidents, and unsupported security cost estimates.

  The lack of effective implementation of the CIO office guidance has been a long-standing problem in DOT since passage of the Clinger-Cohen Act. Unlike some of its counterparts in other Federal agencies, the DOT CIO office does not have budget or performance evaluation authority over the Operating Administrations to oversee implementation of security policy. For example, in the Department of Agriculture, no appropriated funds may be used to acquire new information technology systems or upgrades without the approval of its CIO. In the Department of Commerce, the CIO participates in the performance appraisal of bureau CIOs. Until it is clear that there are management and budget consequences, the Operating Administrations are likely to continue the current practice.

Network Security

DOT employees, contractors, grantees, industry associations, and the public can access DOT computers through various network entry points, such as through Internet entry points (front doors). Business associates also can access DOT computers through direct network connections (back doors). Last year, we expressed concerns over FAA's plan to place its air traffic control systems and its administrative systems on one integrated network. Since then, FAA decided to keep its air traffic control systems on a dedicated network without direct connections to the Internet. During FY 2002, DOT enhanced security over its front doors; however, controls over cyber incident reporting and back door entry points need to be strengthened.

- **DOT enhanced network security but needs to better analyze data for cyber incident reporting.** DOT has 17 authorized Internet entry points and relies on

network security software (firewalls and intrusion detection systems) to ensure that only authorized users are allowed to enter DOT's private networks. During FY 2002, DOT continued enhancing security at its front doors. For example, FAA issued guidance on configuring Internet connection points, deployed more intrusion detection mechanisms at Internet connection points and major network control points, and established a cyber incident response center with continuous operations capability. The CIO office also issued interim reporting guidelines and reported some significant cyber incidents, such as web defacement, to the Federal Computer Incident Response Center and law enforcement agencies, as required.

However, DOT reported more than 25,000 cyber incidents to the Federal Computer Incident Response Center without sufficient analyses to determine whether these incidents were caused by intrusion activity or by innocent acts, such as making an error when entering passwords. Meanwhile, we found significant cyber incidents were not reported as required. For example, DOT identified 10 web defacements, but only 3 were reported. DOT needs to perform in-depth analyses before reporting cyber incidents to outside organizations.

- **DOT needs to strengthen security over back door connections.** Employees, contractors, and industry associations can access DOT systems through direct network connections or can gain access from anywhere by telephone (dial-up access). DOT policy requires Operating Administrations to obtain written assurance from non-Federal entities certifying that their computer systems are in compliance with DOT security requirements for network connections. DOT policy also requires controls over dial-up access to computer systems by validating the calling source.

  We first reported the lack of compliance with DOT's network connection policy in August 1998.[6] The CIO office issued a memorandum requiring Operating Administrations to obtain written assurance from all external entities for compliance with DOT security requirements before establishing network connections. In April 2002, the CIO office issued additional guidance on securing network entry points. However, the CIO office did not require Operating Administrations to assess whether existing connections to DOT systems are in compliance with the new guidance. As a result, we found 3 unsecured network connections to contractor sites and over 300 unauthorized dial-up computer connections at one FAA facility.

[6] Report on the Year 2000 Computer Program and Computer Security Challenges, Report Number: FE-1998-187, August 25, 1998.

System Security

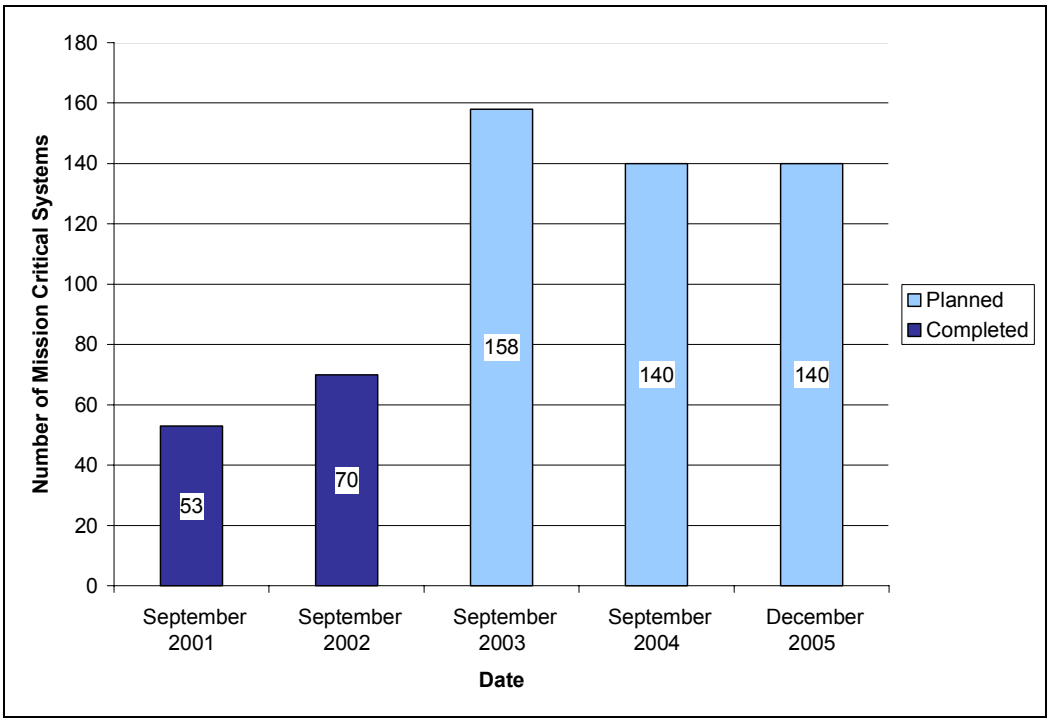
More than 100,000 insiders, including DOT employees, contractor personnel, grantees, industry associations, and other Government agency personnel, are authorized to access computer systems on DOT's private networks. DOT systems are vulnerable to these insiders because most systems have not undergone security certification reviews. According to the Computer Crime and Security Survey published by the FBI, about 50 percent of reported unauthorized access activities in FY 2001 were by insiders.

In the FY 2002 DOT Performance Plan, the Secretary established a goal to have all 561 mission-critical systems certified for adequate security by December 2005. This will be a major challenge for DOT considering that only 123 mission-critical systems, or 22 percent, have been certified and accredited as of September 2002.

- **DOT needs to accelerate its systems certification reviews.** To achieve the Secretary's goal, DOT plans to have 50, 75, and 100 percent of its mission-critical systems certified by the end of FYs 2003, 2004, and 2005, respectively. DOT reported 53 and 70 mission-critical systems were reviewed, tested, and certified during FY 2001 and FY 2002. Based on its recent performance rate, DOT can expect to certify about 62 additional systems by FY 2003, totaling 33 percent of its mission-critical systems rather than the 50 percent as planned.

To meet the Secretary's goals, DOT needs to make a dedicated effort to certify another 158, 140, and 140 systems during the next 3 years (see Table 1).

Table 1
Certification and Accreditation of Mission Critical Systems



To meet the December 2005 goal, DOT has to practically double the number of annual system certification reviews in the next 3 years. To ensure proper planning for resource allocation, DOT needs to develop a schedule detailing the systems to undergo certification reviews during FYs 2003, 2004, and 2005.

- **DOT needs an accurate systems inventory.** This year, DOT reported a total of 677 information systems, a drop of 519 systems from the 1,196 systems reported last year. FAA and Coast Guard account for about 95 percent of the reductions in systems inventory. We found that Operating Administrations used inconsistent methodologies in reporting systems inventory. For example, instead of reporting total systems, Coast Guard reported only major systems. Conversely, the Maritime Administration increased its systems inventory from 26 to 56 by including small systems, such as a Microsoft Access database. Meanwhile, TSA does not consider its more than 1,000 explosive detection systems as information systems, although these machines are equipped with software, hardware, and communication capabilities.

Table 2 lists the number of total systems reported by each Operating Administration in FYs 2001 and 2002.

Table 2
Total Systems Inventory Reported

Operating Administration	FY 2001	FY 2002
Bureau of Transportation Statistics	3	7
Federal Aviation Administration	628	350
Federal Highway Administration	14	36
Federal Motor Carrier Safety Administration	9	30
Federal Railroad Administration	10	14
Federal Transit Administration	4	5
Maritime Administration	26	56
National Highway Traffic Safety Adm.	42	45
Office of the Secretary	16	23
Research and Special Programs Administration	128	29
Surface Transportation Board	4	1
Saint Lawrence Seaway Development Corp.	2	2
Transportation Administration Service Center	60	41
Transportation Security Administration	0	1
U.S. Coast Guard	250	37
	---	---
Totals	**1196**	**677**

Establishing a reliable total systems inventory is an essential step to fulfilling the OMB requirement that all information systems be certified and accredited. With an accurate systems inventory, DOT can budget for and schedule systems that should receive priority for certification and accreditation in accordance with the Secretary's Performance Plan.

- **DOT needs to support security cost estimates.** Proper development and reporting of budget estimates are needed to ensure information security is adequately funded. Last year, DOT reported $51 million in security cost estimates representing about 2 percent of total systems expenditures. The average reported by Federal agencies was 6 percent.[7] This year, DOT reported $103 million in security cost estimates representing about 4 percent of total systems expenditures.

  The FY 2003 security cost percentage still was not supported. As part of the newly developed capital planning and investment control process, the CIO office developed specific guidance for estimating systems security costs. We examined security cost estimates reported for seven projects, totaling $5.4 million, by FAA,

[7] OMB's FY 2001 Report to Congress on Federal Government Information Security Reform.

Coast Guard, FHWA, and TSA. We found that these Operating Administrations did not use DOT guidance in estimating systems security costs and could not support the cost estimates submitted to OMB.

Infrastructure-Critical Systems and Asset Protection

DOT identified about 100 systems and facilities supporting FAA air traffic control operations, Coast Guard search and rescue and marine safety missions, and the Saint Lawrence Seaway as critical infrastructure essential to the Nation's defense, economic security, or public confidence. These assets are considered as meeting the requirements of the Presidential Decision Directive 63 (PDD-63), which requires infrastructure-critical assets be secured by May 2003. Last year, we identified a lack of methodology in identifying infrastructure-critical assets, the need to accelerate FAA's plan to eliminate physical security vulnerabilities by FY 2006, and a lack of disaster recovery capabilities for Coast Guard search and rescue and marine safety systems.

During FY 2002, Coast Guard enhanced its disaster recovery capability and DOT assigned a higher priority to enhance network security than to protect infrastructure-critical systems because of pending presidential direction on securing critical infrastructure. While the current Administration has chosen not to be held to the PDD-63 milestone date (May 2003), officials at both OMB and the Office of Homeland Security agreed that the basic principles of PDD-63 remain in effect. Therefore, securing systems and assets critical to the Nation's infrastructure should still be a high priority.

- **DOT needs to reevaluate identification of infrastructure-critical systems.** Last year, DOT did not use any specific methodology, such as the Project Matrix,[8] to ensure comprehensive reviews of system dependencies when identifying infrastructure-critical assets. As a result, some systems were inappropriately excluded. For example, the Coast Guard's primary network system and an FAA voice switching system were not included. This year, we identified two additional infrastructure-critical systems missing from DOT's list, including a system used to receive radar signals and a network used to route data among air traffic control facilities.

  During FY 2002, DOT initiated use of Project Matrix to reevaluate its identification of infrastructure-critical assets. To successfully implement Project

[8] Project Matrix is a program developed by the Department of Commerce's Critical Infrastructure Assurance Office to accurately identify and characterize the assets and associated infrastructure dependencies and interdependencies that the U.S. Government requires to fulfill its most critical responsibilities. OMB directed most large agencies to undergo a Project Matrix review.

Matrix, DOT needs to develop a work plan detailing the tasks to be completed and determine the necessary funding commitments.

- **Securing air traffic control systems and assets need more attention.** Our focus this year on the air traffic control systems identified additional security concerns that need to be addressed.

  - Testing and fixing system vulnerabilities. FAA identified 92 systems supporting air traffic control operations as infrastructure-critical systems. Last year, FAA developed plans to certify systems security by May 2003. According to the plan, FAA should have had 76 of these systems reviewed, tested, and certified by September 2002. This year, FAA reported that it had certified 12 additional air traffic control systems during FY 2002, bringing the total systems certified to 36. FAA accomplished only about half of its plan. FAA stated that it focused systems certification reviews on new systems instead of legacy systems.

  - Accelerating elimination of physical security vulnerabilities. FAA determined that facilities housing infrastructure-critical air traffic control systems such as en-route centers need to be protected to ensure continued systems operations. Last year, we reported that FAA did not plan to have these facilities certified for adequate physical security until FY 2006. FAA initially agreed to accelerate the schedule. However, the current schedule shows the target completion date has been delayed to FY 2009 due to resource and funding constraints.

  - Assessing security at air traffic control computer centers. OMB Circular A-130 requires agencies to review systems security in both application and general support systems, such as computer centers and networks, because of their interdependencies.[9] This presents a unique challenge to FAA because air traffic control systems operate in 20 independent computer centers. None of these computer center operations has gone through certification reviews as required by OMB. During FY 2002, we audited two centers and found weaknesses in management, operational, and technical controls.

    FAA needs to have these centers reviewed, tested, and certified because the same air traffic control system can operate differently from one center to another. As a result, FAA cannot solely rely on systems certification for assurance. For example, while FAA has the Host Computer System certified as one system, there are 20 individual Host systems operating at en-route

[9] The certification review of general support systems should include rules of using and securing systems, training, personnel controls, incident response capability, continuity of support, technical security, and controls over system interconnection.

computer centers. Until these center operations are reviewed, FAA has little assurance about the integrity, confidentiality, and continuity of these operational systems.

- Developing a contingency plan for prolonged service disruptions. FAA relies on built-in redundancy in air traffic control systems to ensure continued operations in case of systems failures. In case of a major failure, en-route centers could provide backup coverage to each other. However, this is not feasible over an extended period. FAA needs to develop a comprehensive contingency plan that accounts for extended periods of system shutdown.

Recommendations for improving security over air traffic control systems are included in a separate report. Therefore, no recommendations are included in this report. However, we are recommending that the CIO office include FAA's corrective action plans in the FY 2002 FMFIA submission to OMB and Congress.

E-government (Web) Security

Web security and privacy protection are essential for E-government services. Attacks on Government web sites could result in embarrassment to agencies (web sites defaced), inconvenience to the public (web servers out of service), or disruptions to business (reports to meet regulatory requirements deleted). During FY 2002, DOT made good progress to better protect the public's privacy. However, more needs to be done to adequately secure DOT public web sites.

- **Web site vulnerabilities**. Using a commercial scanning software on 175 of DOT's public web servers, we identified 453 vulnerabilities, 66 percent of which were on FAA and FHWA web sites. We rated these vulnerabilities as 79 high, 283 medium and 91 low.[10] Of the high vulnerabilities, 21 are among "The 20 Most Critical Internet Security Vulnerabilities" identified by the FBI. These vulnerabilities could be exploited. For example, we were able to gain access to payroll and personnel information on a private DOT web site. As of September 10, 2002, DOT corrected 435 of the 453 vulnerabilities, including all high vulnerabilities on the FBI Top 20 listing.

- **Security over web sites contracted to third parties.** DOT has at least 35 web sites that operate on third-party computers.[11] However, these service providers

[10] High vulnerabilities may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium and low vulnerabilities may provide an attacker with useful information, such as password files, to compromise DOT computers.

[11] For example, web sites disclosing motor carrier safety records or ordering transportation statistics are operated by contractors.

were not required to provide assurance that DOT web sites are adequately protected. We found that one of the web systems contracted to a third party was defaced during FY 2002. DOT has no policy requiring written assurance from third-party providers.

- **Sensitive information on public web sites.** Protecting sensitive information from inappropriate disclosure is a new challenge for agencies. We found sensitive information labeled "For Official Use Only" on DOT public web sites. For example, one document discussed how FAA selects aviation repair facilities for safety inspections. This type of information should be protected against uncontrolled release. We also found sensitive security information such as procedures for screening passengers carrying classified materials. DOT promptly removed these documents from its web sites.

Recommendations for improving web security and cyber incident reporting will be included in a separate report. Therefore, no recommendations are included in this report.

Personnel Security

Personnel security includes segregating key duties among staff, holding individuals accountable, restricting individuals' access, and conducting background checks on individuals in positions of trust. Our review focused on background checks because DOT had about 18,000 contractor personnel working on DOT systems. DOT policy requires background checks be completed in a timely manner.[12] The responsibility for enforcing this policy is shared among the offices of the CIO, Senior Procurement Executive, and Security and Administrative Management.

- **DOT still needs to conduct background checks on contractor employees.** Last year, FAA reported that it completed background checks on 85 percent of its contractor employees while the other Operating Administrations reported about 25 percent completion. During FY 2002, we sampled 178 contractor employees working for FAA, TSA, and the Office of the Secretary. We found 43 (24 percent) individuals who did not receive background checks, including 2 individuals requiring top secret clearances.

- **DOT needs to include requirements for conducting background checks in contracts.** Requirements for background checks still are not consistently included in DOT contracts. We reviewed 13 contracts administered by FAA, Coast Guard, TSA, the Federal Transit Administration, and the National Highway Traffic Safety

[12] DOT Order 1630.2B, entitled "Personnel Security Management," May 30, 2001.

Administration and found 3 Coast Guard contracts contained no requirement for performing background checks.

.

In view of the existing security weaknesses identified in this report, we concluded that the DOT information security remains a material weakness and requires continued senior management attention.

RECOMMENDATIONS

1. We recommend that the Deputy Secretary establish the Chief Information Officer's authority by requiring the CIO office to review and approve Operating Administrations' budget submissions for acquiring and operating information systems, and to provide input into performance evaluations for the Operating Administrations' Chief Information Officers.

2. We also recommend that the Acting DOT Chief Information Officer incorporate corrective action plans and target completion dates for the following items in the FY 2002 Federal Managers' Financial Integrity Act report:

   a. Oversee the Operating Administrations implementation of DOT guidance on securing network entry points and estimating systems security costs, which was developed in response to the FY 2001 FMFIA submission.

   b. Improve the systems inventory methodology, complete an updated systems inventory, and reevaluate identification of infrastructure-critical systems and assets using Project Matrix.

   c. Develop a schedule detailing the systems to undergo certification reviews during FYs 2003, 2004, and 2005 to help resource planning.

   d. Work with the Office of the Senior Procurement Executive and the Office of Security and Administrative Management to establish a plan to ensure background checks on contractor employees are performed timely, as required by DOT's personnel security policy.

   e. Incorporate FAA's corrective action plans to (i) have infrastructure-critical air traffic control systems, computer centers, and facilities certified for adequate security and (ii) establish a comprehensive contingency plan to ensure continued air traffic control operations during extended periods of system shutdown.

MANAGEMENT RESPONSE

A draft of this report was provided to the DOT Deputy Chief of Staff, the Acting DOT Chief Information Officer, and the FAA Chief Information Officer on September 19, 2002. They agreed with the report. The Acting DOT Chief Information Officer agreed to provide specific action plans and estimated completion dates in DOT's GISRA and FMFIA submissions to OMB.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, we would appreciate receiving DOT's GISRA corrective action plan upon its submission to OMB. If you concur with our findings and recommendations, please state specific actions taken or planned for each recommendation and provide target dates for completion. If you do not concur, please provide your rationale. 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 DOT and the Operating Administrations' representatives. If you have questions concerning this report, please call me at (202) 366-1992 or John Meche at (202) 366-1496.

#

EXHIBIT A. OIG INPUT TO GISRA EXECUTIVE SUMMARY

This section presents the Office of Inspector General (OIG) input to meet the legislative mandate of the Government Information Security Reform Act (GISRA). The Office of Management and Budget (OMB) guidance requires that OIG (1) provide comments to DOT's Executive Summary for program reviews and independent evaluations and (2) prepare a detailed independent evaluation report. The OIG independent evaluation report is provided separately. As required by OMB, OIG is commenting on 12 of the 13 items specified in the reporting guideline.

The Department has not had a Chief Information Officer (CIO) since January 2001. Because of this, the Secretary delegated the authority to administer GISRA requirements to the Acting CIO. While the CIO office is responsible for the information security program, it does not have budget or performance evaluation authority to oversee implementation of security guidance by DOT operating divisions.

During Fiscal Year (FY) 2002, DOT made a strong management commitment to improve information security by developing performance measurements in the E-government scorecard, issuing additional security guidance, and enhancing its network defense against intrusions from the Internet. However, more progress is needed to secure individual systems to reduce unauthorized access to computer systems on DOT's private networks (insider threats). DOT agreed to focus on individual systems security during FY 2003.

STUDY A. 1. – SECURITY FUNDING

OIG was not required to respond to this item.

STUDY A. 2. – PROGRAMS AND SYSTEMS

Describe the total number of programs and systems in the agency.

DOT has 15 major operating divisions, which includes the Transportation Security Administration (TSA). This year, DOT is reporting a total of 677 systems, a drop of 519 from the 1,196 systems it reported last year. The Federal Aviation Administration (FAA) and Coast Guard account for about 95 percent of the reductions in systems inventory. We found that operating divisions used inconsistent methodologies to inventory systems. For example, TSA does not consider its more than 1,000 explosive detection systems as information systems, although these machines are equipped with software, hardware, and communication capabilities.

Conversely, the Maritime Administration included small systems, such as a Microsoft Access database, when reporting systems inventory.

DOT needs an accurate systems inventory to finalize the identification of mission-critical systems for resource allocations, to estimate security funding requirements, and to develop performance measures for assessing, testing, and securing its systems. The CIO office agreed to improve the systems inventory methodology and complete an updated systems inventory in FY 2003.

How many systems were reviewed by OIG?

DOT reported one classified system in FAA, and one in the Coast Guard for national security programs. During FY 2002, the Coast Guard system was reviewed by the Defense Information Systems Agency. The FAA system, which is being transitioned to TSA, was accredited by the Central Intelligence Agency. OIG did not audit the independent evaluations performed by these two external agencies.

During FY 2002, OIG reviewed the following DOT systems and incorporated the review results in its independent evaluation report.

- We reviewed management oversight of air traffic control systems security, and performed detailed reviews of 11 systems supporting en-route center operations. These systems support high altitude air traffic control operations and also provide essential information to systems supporting other air traffic control components. We identified the need to increase management oversight, improve access security, and enhance contingency planning. FAA initiated corrective actions to enhance air traffic control systems security.

- We reviewed security and privacy protection over DOT public web systems, including operating division-specific web systems. DOT has more than 200 web sites supporting about 1 million web pages that are accessible to the public through the Internet. DOT is increasing its services to citizens and businesses through these web sites as part of the President's E-government Management Agenda.[13] During FY 2002, DOT made good progress in protecting the public's privacy. However, some operating divisions' web sites contained vulnerabilities and sensitive information. Operating divisions took immediate actions to eliminate vulnerabilities and remove sensitive information from public web sites. DOT needs to develop a process to have all web sites periodically reviewed to identify and correct vulnerabilities.

[13] The Government Paperwork Elimination Act requires agencies to provide the option of electronic maintenance, submission, or disclosure of information as a substitute for paper by October 2003.

- We reviewed the newly implemented capital planning and investment control process for information technology investment. Having a process in place to better select, implement, and evaluate information technology investment is part of the President's E-government agenda. During FY 2002, DOT made a concerted effort to develop this process, including guidance on estimating systems security costs. However, the process was not implemented. We examined the security cost estimates for seven projects submitted by FAA, Coast Guard, TSA, and the Federal Highway Administration. These operating divisions did not use DOT's guidance and could not support cost estimates. The CIO office agreed to provide training during FY 2003 on estimating security costs and to develop a metric in the E-government scorecard to measure operating divisions' compliance.

- Using a contractor, we evaluated controls and security over six major financial systems used to compile DOT financial statements. We identified weaknesses in access controls, documentation for program changes, and segregation of duties. DOT is reviewing these concerns for corrective actions.

Did the agency use the self-assessment guide or agency developed methodology in assessing system security?

OMB requires agencies to use the National Institute of Standards and Technology self-assessment guide in assessing all agency systems. While the total systems inventory is in flux, DOT completed an initial inventory of 561 mission-critical systems. DOT reported that operating divisions used the self-assessment guide to review 106 mission-critical systems during FY 2002. OIG reviewed 15 systems and found they were evaluated based on the self-assessment guide.

STUDY A. 3. – MATERIAL WEAKNESSES

Describe the material weaknesses reported for FY 2001 and FY 2002 and any recurring weaknesses.

DOT reported the information security program as a material weakness in its FY 2001 Federal Managers' Financial Integrity Act (FMFIA) submission to OMB and Congress. DOT specified four corrective actions—developing a security performance measurement program, network security guidance, cyber incident reporting program, and capital planning process for information security. While DOT has implemented a performance measurement program (scorecard) and issued guidance as planned, it faces other major challenges. We recommend that DOT incorporate planned corrective actions for the following items in its FY 2002 FMFIA submission.

- Overseeing implementation of security guidance by operating divisions. While the CIO office issued guidance on improving network security, reporting cyber incidents, and estimating security costs, operating divisions have not effectively implemented the guidance. For example, we identified unsecured network connections, inaccurate reporting of significant cyber incidents, and unsupported security cost estimates.

- Securing infrastructure-critical air traffic control systems and assets. Last year, we reported that DOT might not be able to secure its infrastructure-critical assets by May 2003, as required by Presidential Decision Directive 63 (PDD-63).[14] We also identified a lack of methodology in identifying infrastructure-critical assets, the need to accelerate FAA's plan to eliminate physical security vulnerabilities by FY 2006, and a lack of disaster recovery capabilities for Coast Guard search and rescue and marine safety systems. While Coast Guard has enhanced its disaster recovery capability, FAA made little progress during FY 2002. We identified additional concerns with air traffic control systems, which are discussed in our independent evaluation report.

- Completing mission-critical systems security reviews. In the FY 2002 DOT Performance Plan, DOT established a goal to have all of its 561 mission-critical systems certified for adequate security by December 2005. To achieve this goal, DOT plans to have about 280 (50 percent) of the 561 mission-critical systems certified by September 2003, as specified in its E-government scorecard. During FYs 2001 and 2002, DOT reported 53 and 70 mission-critical systems, respectively, were reviewed, tested, and certified. At this rate, DOT will have certified only about 185 of the 280 systems by September 2003. DOT needs to develop a detailed schedule, including target dates for completing specific systems certifications, to achieve this goal.

STUDY B. 1. – IMPLEMENTATION BY AGENCY HEAD

Describe what steps were taken by the agency head to implement and enforce the Security Act responsibilities.

The Department has not had a CIO since January 2001. Because of this, the Secretary delegated the authority to administer GISRA requirements to the Acting CIO. DOT also hired an Associate CIO for Information Security. This individual is responsible

[14] While the current Administration has chosen not to be held to the PDD-63 milestone date, officials at both OMB and the Office of Homeland Security agreed that the basic principles of PDD-63 remain in effect.

for developing, maintaining, and implementing agencywide security policies and reports directly to the Acting CIO as required by the GISRA legislation.

The Acting CIO chairs the DOT CIO Council, which is comprised of operating division CIOs. The Council established an Information Technology (IT) Security Committee to coordinate information security issues. The Secretary, with the assistance of the CIO Council, made information systems security a priority for DOT. In addition to reporting its information security program as a material weakness in the FY 2001 FMFIA report, the Secretary established specific performance measures in the FY 2002 DOT Performance Plan that all mission-critical systems be reviewed and certified for adequate security by December 2005. Improving computer security also is one of the metrics specified in DOT's E-government scorecard, which is being closely monitored by the Secretary's office.

Can a major operating component of the agency make IT investment decisions without review by and concurrence of the agency CIO?

The CIO Council is mainly a coordination committee with its members reporting to individual operating divisions. The CIO office does not have budget authority over IT investments. Operating divisions can, and do, make IT investment decisions without the CIO office review and concurrence. In June 2002, DOT issued new IT capital planning guidance that established a DOT Investment Review Board to review major IT investment decisions. The Deputy Secretary chairs the Investment Board with members of the DOT CIO, the Chief Financial Officer, the General Counsel, and the Assistant Secretary for Administration. The following guidance was issued to categorize major IT investment projects to be reviewed by the Investment Board:

- "Cross-cutting" IT projects common to two or more operating divisions, such as e-mail, payroll, or personnel projects.

- Operating division-specific IT projects with sufficient dollar value, mission criticality, or public visibility to "merit consideration" by the Investment Board.

Establishing the Investment Board is a step in the right direction. However, the guidance to identify projects for review by the Investment Board needs to be more specific. For example, the guidance does not establish dollar thresholds for projects to be reviewed. More specific guidance is needed to ensure that operating divisions provide timely information on projects that should be reviewed by the Investment Board.

STUDY B. 2. –LIFE-CYCLE SECURITY PRACTICE

What specific and direct actions were taken by the agency head to ensure that information security plans were updated and practiced throughout the life cycle of each system?

Updating and practicing the security plan throughout the systems life cycle are the underlying requirements in systems security certification reviews. Last year, DOT reported that 53 (10 percent) mission-critical systems had been certified for adequate security. In the FY 2002 DOT Performance Plan, the Secretary established specific performance measures that all mission-critical systems be reviewed and certified for adequate security by December 2005. Operating divisions are working toward this goal and reported having 123 (22 percent) mission-critical systems certified and accredited as of September 2002, including 12 additional infrastructure-critical air traffic control systems. In addition, FAA is transitioning its systems certification and accreditation process to the National Information Assurance Certification and Accreditation Process to be more in line with national security systems.

However, the Secretary's performance measures apply only to mission-critical systems, not all DOT systems as required by OMB. The Department's decision to focus on mission-critical systems is appropriate for prioritizing resource usage. Getting all mission-critical systems reviewed and certified will be a major challenge for DOT considering that only 22 percent of mission-critical systems have been certified and accredited as of September 2002.

STUDY B. 3. – INTEGRATION OF SECURITY RESPONSIBILITIES

How has the agency integrated IT security with critical infrastructure protection responsibilities?

FAA has not fully integrated the information technology security program with its critical infrastructure protection responsibility concerning physical security at air traffic control facilities. Last year, we reported that FAA did not plan to eliminate physical vulnerabilities until FY 2006 at facilities where infrastructure-critical air traffic control systems operate. Rather than accelerating its timetable to eliminate physical security vulnerabilities, FAA's target completion date for securing both en-route centers and long-range radar facilities, where infrastructure-critical systems operate, has been delayed from FY 2006 to FY 2009. We are again recommending that FAA reconsider its schedule to eliminate these vulnerabilities and that DOT should include a corrective action plan in its FY 2002 FMFIA submission.

STUDY B. 4. – IDENTIFICATION OF CRITICAL ASSETS

Has the agency undergone a Project Matrix review to identify its critical operations and assets? If not, describe the method used by the agency.

OIG reported last year that DOT did not use any specific methodology in identifying its critical assets. Instead, DOT identified its infrastructure-critical assets as those DOT-owned, controlled, or operated facilities and information based systems that are essential to the nation's defense, economic security, or public confidence in such facilities or systems.

DOT identified about 100 systems and facilities as its infrastructure-critical assets to include those supporting air traffic control operations, Coast Guard search and rescue and marine safety missions, and the Saint Lawrence Seaway. Because DOT did not fully evaluate system interdependencies in the informal evaluation process, it overlooked some infrastructure-critical systems. This year, we identified two additional air traffic control systems missing from DOT's list.

Project Matrix is a program developed by the Department of Commerce Critical Infrastructure Assurance Office to accurately identify and characterize the assets and associated infrastructure dependencies and interdependencies that the U.S. Government requires to fulfill its most critical responsibilities. OMB directed that most large agencies undergo a Project Matrix review. During FY 2002, DOT initiated the use of Project Matrix to reevaluate the identification of its infrastructure-critical systems and assets. DOT is in the early data collection phase and has not developed a work plan detailing the tasks, milestones, or funding commitments.

STUDY B. 5. – REPORTING OF SECURITY INCIDENTS

Does the agency have documented procedures for reporting security incidents and sharing information on common vulnerabilities?

OMB requires agencies to develop a cyber incident response capability to adequately detect intrusion activities and to timely share the information with law enforcement authorities and the Federal Computer Incident Response Center (FedCIRC). The CIO office issued its Interim Incident Handling and Reporting Guidelines in December 2001. The guidelines require Information Systems Security Officers to collect and report information regarding computer security incidents to the CIO

office, which then will share the information with FedCIRC or the FBI's National Infrastructure Protection Center.
We found that the interim reporting guidelines were not effectively implemented and need to be improved. While DOT reported more than 25,000 cyber incidents to FedCIRC during FY 2002, which represented a significant increase from last year, DOT did not sufficiently analyze whether these cyber incidents were caused by intrusion activities or by innocent acts such as typing a wrong password.

While DOT was reporting innocent acts to agencies outside DOT, significant cyber incidents were not reported as required. For example, DOT identified 10 web defacements, but only 3 were reported. OIG recommended that DOT perform in-depth analyses before reporting cyber incidents to outside agencies.

STUDY C. 1. –SECURITY EVALUATION BY PROGRAM OFFICIALS

Have agency program officials assessed the risk, determined the appropriate security level, updated the security plan, and tested the security controls for each system under their control?

DOT decided to focus first on getting mission-critical systems assessed and tested. Consequently, operating divisions have not assessed the risk, determined the appropriate security level, updated the security plan, and tested the security controls for each system under their control. During FY 2002, operating divisions reviewed 106 of 561 mission-critical systems using the National Institute of Standards and Technology self-assessment guide. However, DOT has not developed a schedule to have the remaining mission-critical systems assessed. OIG also found that DOT needs to establish a complete and accurate systems inventory to develop an adequate plan to assess the non-mission critical systems.

STUDY C. 2. –SECURITY OVER CONTRACTOR PROVIDED SERVICES

Have agency program officials used proper methods to ensure that contractor provided services (e.g., network or web site operations) are adequately secured?

DOT does not have a policy requiring assurance from contractors that the services provided to DOT are adequately secure. Operating divisions are to include such requirements for contracted services. We reviewed DOT contracts for 4 data center operations and 35 web system operations and found that independent reviews were required for only one of the contracted data centers. During FY 2002, one web system contracted to a third party was defaced.

In contrast, DOT has a network connection policy requiring non-Federal entities, such as third-party contractors, to provide written assurance that their computer systems are in compliance with DOT security requirements. Last year, we reported unsecured network connections to contractor sites as a weakness. To address this, the CIO office issued additional guidance; however, it has not been implemented. During FY 2002, we found three unsecured contractor connections at one FAA site.

DOT policy also requires that contractor employees receive the same background checks as DOT employees performing similar work. DOT has about 18,000 contractor employees working on its systems. This year, we found that DOT needs to continue improving background checks. We sampled 156 contractor employees working on air traffic control systems and found no background checks on 24 (15 percent) individuals. Of the 10 contractor employees working for TSA that we reviewed, none had background checks. Of the 13 contracts administered by 5 operating divisions that we reviewed, 3 Coast Guard contracts contained no requirement for conducting background checks.

STUDY D. 1. – IMPLEMENTATION BY AGENCY CIO

Has the agency CIO adequately maintained an agency-wide security program, ensured effective implementation, and evaluated performance of major agency components?

The CIO office developed a departmentwide information security program, which provides direction to operating divisions to protect DOT systems. It also issued specific guidance addressing network security, cyber incident reporting, and capital planning. The CIO office does not directly supervise implementation of the security program or guidance because it does not have budget or performance evaluation authority over operating divisions. Meanwhile, the guidance issued by the CIO office was not effectively implemented by operating divisions. For example, operating divisions continue to have unsecured network connections with third parties although DOT issued specific guidance in FY 1999.

Has the agency CIO ensured the training of agency employees with significant security responsibilities?

There are two important security positions established in the DOT information security program—Information Systems Security Officers and System Administrators. While DOT developed and provided specialized training programs to employees in these key positions, it does not have a complete listing of designated

employees. As a result, DOT does not yet have an accurate count of employees requiring specialized training.

STUDY D. 2. – SECURITY OVER CONTRACTOR PROVIDED SERVICES

Has the agency CIO used proper methods to ensure that contractor provided services (e.g., network or web site operations) under his/her control are adequately secured?

OIG reviewed one contract awarded by the CIO office during FY 2002, which tasked the service provider to perform network maintenance for the Office of the Secretary, which includes the CIO and the intelligence offices. The contract included a requirement for background checks on all 12 individuals working on the contract. However, nine contractor employees had not received the background checks, including two individuals requiring top secret clearances. The CIO office is working with DOT security officials to complete these checks.

STUDY D. 3. – CAPITAL PLANNING FOR SECURITY COSTS

Has the agency CIO fully integrated security into the agency's capital planning and investment control process?

OIG reviewed the newly implemented capital planning and investment control process for information technology investment. During FY 2002, DOT made a concerted effort to develop this process, including guidance on estimating systems security costs. However, operating divisions did not use this guidance. For example, in preparing the FY 2004 budget submission, FAA initially estimated its security costs to be one percent of total systems cost, which was later increased to two percent. TSA estimated that 10 percent of its systems costs to be for security. Neither FAA nor TSA could provide support for using these percentages. The CIO office agreed to provide training on estimating security costs and to develop a metric in the E-government scorecard to measure operating divisions' compliance during FY 2003.

Were security costs reported on every capital asset plan (as well as Exhibit 53) submitted to OMB for FYs 2003 and 2004? Any discrepancies in the submissions? Any independent validation prior to submission?

In addition to Exhibit 53 (agency IT portfolio), DOT submitted 25 and 86 Form-300's (capital asset plans) for FYs 2003 and 2004, respectively. Information security costs were reported on every capital asset plan and Exhibit 53. DOT also included

information security costs in the current year's GISRA submission. However, discrepancies existed as indicated in the following table.

Information Security Costs Reported to OMB

Information Source	FY 2003 (millions)	FY 2004 (millions)
Agency IT Portfolio (Exhibit 53)	$65	$170
Capital Asset Plan (Form 300)	$15	$140
GISRA Report	$103	N/A

OIG reviewed seven projects listed on Exhibit 53. Operating divisions could not provide support for $5.4 million in security costs reported for these projects. The CIO office's review was limited to ensuring that operating divisions included security costs in the submissions. The CIO office agreed to expand its review to ensure the integrity of security cost estimates.

OIG CONCLUSION

In view of the security weaknesses identified in this GISRA report, we concluded that the DOT information security program remains a material weakness and requires continued senior management attention. OIG recommends that DOT provide the CIO office with more authority to oversee the information security program and include specific action plans in its FY 2002 FMFIA submission to OMB and Congress for implementing security guidance, protecting infrastructure-critical air traffic control systems and facilities, and completing mission-critical systems reviews and certifications.

EXHIBIT B. SCOPE AND METHODOLOGY

Our FY 2002 GISRA audit focused on FAA air traffic control systems, DOT major financial systems, and DOT E-government (web) security. We reviewed progress made since last year's GISRA submission, including the adequacy of corrective actions specified in the FMFIA submission. We provided input (Exhibit A) to DOT's GISRA Executive Summary by answering 12 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. Information developed by DOT program officials and their contractors also was considered.

Our work was performed between June and September 2002 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.

EXHIBIT C. DOT OPERATING ADMINISTRATIONS

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
Transportation Administration Service Center
Transportation Security Administration
U.S. Coast Guard

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

THE FOLLOWING INDIVIDUALS CONTRIBUTED TO THIS REPORT.

Name	Title
Rebecca Leng	Program Director
Philip deGonzague	Project Manager
Michael Marshlick	Senior Computer Scientist
Ping Sun	Senior Computer Scientist
James Mallow	Senior Auditor
Nathan Custer	Senior Auditor
William Coker	Senior Auditor
Henry Lee	Computer Scientist
Gary Klauber	Computer Scientist
Mitchell Balakit	Computer Scientist
Cynthia Tims	Information Technology Specialist
Bradley Kistler	Information Technology Specialist
Jean Ablutz	Information Technology Specialist
Jean Yoo	Information Technology Specialist