# INFORMATION SECURITY PROGRAM

***Department of Transportation***

***Report Number: FI–2006–002***
***Date Issued: October 7, 2005***

# Memorandum

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

Subject: ACTION: Audit of Information Security Program, Department of Transportation
Report Number: FI-2006-002

Date: October 7, 2005

From: Kenneth M. Mead
Inspector General

Reply to Attn. of: JA–20

To: Chief Information Officer

This report presents the results of our annual audit of the information security program at the Department of Transportation (DOT). In accordance with the Federal Information Security Management Act of 2002 (FISMA), our objective was to determine the effectiveness of DOT's information security program by measuring progress made in (1) implementing information security requirements since last year, (2) correcting air traffic control system security deficiencies, and (3) enhancing information technology (IT) investment management controls. We also 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.

Similar to last year, we tested a representative subset of DOT systems, including contractor-operated or -maintained systems that had undergone systems security certification reviews in order to determine whether DOT had complied with Government standards for (1) assessing system risks, (2) identifying security requirements, (3) testing security controls, and (4) accrediting systems as able to support business operations. We also performed more detailed reviews of the Department's process for managing remediation of known security weaknesses.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards prescribed by the Comptroller General of the United States and included such tests as we considered necessary to detect fraud. Details of 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 the agency. DOT maintains one of the largest portfolios of IT systems among Federal civilian agencies; it is therefore essential that the Department protect these systems, along with their sensitive data. In fiscal year (FY) 2005, DOT's IT budget totaled about $2.7 billion.

The Department has 12 Operating Administrations (OA). However, two OAs were reorganized during FY 2005: the Bureau of Transportation Statistics and the Research and Special Programs Administration have been replaced by the Pipeline and Hazardous Materials Safety Administration and Research and Innovative Technology Administration. This reorganization enables the Department to more efficiently coordinate and manage the Department's extensive research efforts and to expedite implementation of cross-cutting, innovative technologies.

Ownership of computer systems was also realigned between the two new component agencies. For FY 2005, the Department is reporting a total of 451 computer systems—about 7 percent fewer than last year—as a result of its continued effort to consolidate systems for FISMA reporting. Among the systems the Department maintains and operates is the air traffic control system, which the President has designated as part of the nation's critical infrastructure. Other systems owned by the Department include safety-sensitive surface transportation systems and financial systems that disburse over $50 billion in Federal funds each year. Systems inventory counts for FY 2004 and FY 2005 in each OA are detailed in Exhibit C.

## RESULTS IN BRIEF

Last year, we reported that DOT had made a concerted effort to correct security weaknesses identified in FY 2001, FY 2002, and FY 2003, years in which the Department reported its information security program as a material weakness under the Federal Managers' Financial Integrity Act (FMFIA).[1] Progress noted in last year's report included increased oversight of IT investment management and security controls, strengthened protection of DOT's network infrastructure against

[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 M-05-15, "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," June 13, 2005).

intrusion, and increased security certification reviews. In addition, FAA committed to taking aggressive action to enhance air traffic control security. Based on the progress made and management's commitment, DOT's information security program was downgraded to a reportable condition last year.[2]

In 2004, we also identified issues that required continued management attention, such as improving the quality of security certification reviews and making significant progress in enhancing air traffic control system security. DOT has worked to improve the quality of certification reviews and is now performing quality assurance reviews of systems already certified. Although the Department has continued to make progress in these areas, much remains to be done, and new challenges have also emerged. In addition, the Department did not implement a number of critical corrective actions[3] during FY 2005, partially due to turnover of key security personnel in the Office of the Chief Information Officer.

Meanwhile, FAA did not start in earnest to initiate aggressive actions to correct previously identified air traffic control security deficiencies until April 2005, after the Inspector General issued a letter to the Federal Aviation Administrator expressing concerns over the slow pace of FAA's corrective actions. FAA's progress improved, but since this effort only began in April, its overall progress in better securing air traffic control system operations for FY 2005 was insufficient.

In recent years, our office has issued several reports recommending that FAA act quickly to correct security deficiencies found in air traffic control systems.[4] Providing adequate security over these facilities is critical because the President has designated the air traffic control system part of the nation's critical infrastructure due to the important role commercial aviation plays in fostering and sustaining the national economy and ensuring the safety and mobility of citizens. In addition, our office is in the process of issuing two new reports identifying deficiencies in security over FAA's system for maintaining air traffic control surveillance, navigation, and communications equipment and deficiencies in physical security at air traffic control facilities. Despite all the advanced

---

[2] A reportable condition is a security or management control weakness that does not rise to the level of a significant deficiency, yet is still important enough to be reported to internal management (OMB M-05-15, "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," June 13, 2005).

[3] These include developing standards for secure configuration of Oracle databases used in many major Departmental systems, ensuring timely correction of computer vulnerabilities identified, and directing OAs to relocate their system recovery sites that are too close to DOT Headquarters.

[4] OIG Report Number FI-2004-078, "Audit of Security and Controls over En Route Center Computer Systems," August 9, 2004. OIG Report Number FI-2005-003, "Audit of Security and Controls over Technical Center Computer Systems," November 5, 2004. Most OIG reports can be accessed on our website: www.oig.dot.gov. The Department has determined that these reports contain Sensitive Security Information (SSI) as defined by 49 CFR Part 1520. Accordingly, they are 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.

technologies deployed in today's environment, adequate physical security is essential to ensuring safe and uninterrupted air traffic control services to the American public. In FY 2005, the Government Accountability Office also identified the need to enhance computer security protection in air traffic control systems and physical security protection at air traffic control facilities.[5]

The most significant challenges are summarized below.

## The Department Faces a Challenge in Recertifying Systems Security While Enhancing the Quality of Certifications

Last year, the Department increased the percentage of systems completing security certification reviews from 33 percent to over 90 percent. However, DOT has a significant challenge ahead in recertifying systems while improving the quality of system certifications. OMB requires Federal systems security to be recertified at least every 3 years because systems are constantly changed to support evolving business and technical needs.

Unlike last year, the Department did not have a planned schedule or designated resources to perform this task during FY 2005. In late August, we brought to management's attention that about 15 percent of Departmental systems were overdue for recertification. Since then, the Department engaged in a very ambitious plan to recertify the security of these systems by the end of the fiscal year. Committing resources to recertifying systems security will be a continuing challenge to the Department, with more than 300 systems due for recertification in the next 2 years.

The quality of the security certification reviews improved during FY 2005. Last year, we reported deficiencies such as inadequate risk assessments, a lack of evidence of security tests, and systems accredited by inappropriate officials. This year our sample review of 20 system security certification reviews identified fewer deficiencies in the 6 certification reviews completed in FY 2005. Nonetheless, improving the quality of the certification reviews will be a major challenge to the Department because of the large number of systems that will need to be recertified in 2006 and 2007.

[5] GAO-05-712, "Information Security: Progress Made, but Federal Aviation Administration Needs to Improve Controls over Air Traffic Control Systems," September 26, 2005.

## The Department Needs To Better Manage Correction of Systems Security Deficiencies

During FY 2005, the Department collected detailed data to track and prioritize efforts to correct identified security weaknesses, as required by OMB.[6] With this more complete view, it became clear that the Department needs to strengthen its system security correction activities to ensure that weaknesses are being fixed in a timely manner and that the most critical weaknesses are corrected first. Currently, the Department has about 3,000 weaknesses that need to be fixed. However, management could not effectively prioritize their correction because 1,620 of the weaknesses are missing information such as their severity and the cost needed to correct them. However, some of these weaknesses clearly require immediate action. For example, one of the pending actions is to enhance password security protection in a system that contains privacy information. This inexpensive fix would significantly reduce the risk of unauthorized access.

We understand that management cannot tackle every deficiency at once, especially in today's tight budget environment. Management has to make realistic decisions, balancing system importance, risk, and cost in prioritizing remediation efforts. Yet items requiring immediate attention should not be allowed to be delayed. We found that more than 300 identified deficiencies had passed their target completion dates by more than 6 months. Some of these overdue items were deemed to have a severe impact on the integrity of program operations, such as causing adverse effects on communications among air traffic control facilities.

## FAA Did Not Take Aggressive Actions To Enhance Air Traffic Control Systems Security

Last year FAA committed to completing security reviews of all operational air traffic control systems—at en route, approach control, and airport terminal facilities—within 3 years and to identifying a cost-effective alternative to restoring essential air service in the event of prolonged service disruption at an en route facility.

During FY 2005, FAA took limited steps in fulfilling its commitment to address prior air traffic control systems security recommendations. FAA fell short of fully addressing its commitments, as identified below:

- FAA collected system security information on only about half of the systems used to support en route (high-altitude) air traffic services. En route centers currently rely on approximately 30 systems to deliver safe and efficient air

[6] The process employed to track and prioritize security remediation efforts is referred to as a plan of action and milestones (POA&M) in DOT's FISMA reporting to OMB.

traffic control services. Since information was collected only on half of the systems, other critical systems, such as the system that routes critical weather and flight plan data to all en route centers, were not reviewed.

- FAA has not analyzed the information collected and therefore has not determined what remediation work is needed to better secure operational en route systems.

- FAA officials did not perform any independent testing on-site. As demonstrated by the Government Accountability Office and our reports, testing is the key to identifying potential security breaches. Performing independent testing on high-risk systems is also required by FISMA.[7]

Finally, while FAA has identified a cost-effective alternative to restoring essential en route air service in case of prolonged service disruption, it is years away from implementing the alternative. Implementing the selected alternative is a complicated endeavor but critical to supplementing FAA's current business continuity strategy, one that has worked well in the past in dealing with temporary, less severe service disruptions.

## Departmental Oversight of Major System Investments Needs To Be Enhanced

Last year, we reported that the Departmental Investment Review Board needed to perform more substantive and proactive reviews of IT investments managed by individual OAs. This remains a challenge, especially for air traffic control modernization projects, which account for over 80 percent of the Department's IT budget.

This year, the Board reviewed investment projects managed by various OAs, including FAA. While projects managed by most OAs have benefited from the Board's oversight, the Board has had little positive impact on complicated air traffic control projects, which are still experiencing significant cost increases and schedule delays. We reviewed 16 FAA major acquisitions and found that 9 projects had experienced schedule delays of 2 to 12 years and 11 projects had experienced cost growth of about $5.6 billion (from $8.9 billion to $14.5 billion). The bulk of the cost growth represented by the $5.6 billion occurred before the establishment of the new Air Traffic Organization and had been building for some time without being recognized. Some of the major investment projects have

[7] FISMA requires agencies to meet the minimum Government security standards developed by the National Institute of Standards and Technology (NIST). NIST Special Publication 800–37, "Guide for the Security Certification and Accreditation of Federal Information Systems," requires independent security testing when reviewing high-risk systems.

experienced persistent cost and schedule problems, such as the Wide Area Augmentation System and the Standard Terminal Automation Replacement System.

Nine years after Congress passed acquisition reform for FAA, exempting it from compliance with Federal acquisition regulations, air traffic control modernization projects are still experiencing performance problems, along with the cost increases and schedule delays. Further, FAA's acquisition process has stayed on the Government Accountability Office's high-risk list since 1995. Meanwhile, FAA continues to initiate new, costly, and complex IT modernization projects. This year, two new multibillion-dollar FAA investment projects—FAA Telecommunications Infrastructure and En Route Automation Modernization—went forward to OMB without reliable cost, schedule, and other project information. OMB rejected the budget submissions and asked the Board to reexamine business cases for these investment projects.

We are concerned that the Board's review of major FAA IT investment projects is not providing value-added services as intended and is facing the risk of becoming a paperwork exercise that provides little substantive value to the Secretary. There are two basic reasons for this.

- First, there is a lack of clarity about the Board's role in reviewing major FAA investment projects. The Clinger-Cohen Act of 1996 requires the Secretary to implement a process for "maximizing the value and assessing and managing the risks of the information technology acquisitions of the executive agency." The Board was created as part of this process and is tasked with advising the Secretary whether to continue, modify, or terminate major IT investments. However, FAA has frequently cited its independent acquisition authority, based on provisions in the Department's Appropriations Act for Fiscal Year 1996, to argue that the Board should play only a limited role in overseeing FAA investments. The provision in the Appropriations Act exempted FAA from compliance with the Federal acquisition regulations and key Federal procurement laws to help make the acquisition process more timely and cost-effective.

  The issue that needs to be resolved is whether FAA's exemption from compliance with the Federal procurement regulations also applies to management oversight required by the Clinger-Cohen Act. Until this issue is resolved, it is our opinion that the Board's continued "review" of FAA's multibillion-dollar investment projects will not result in "maximizing the value and assessing and managing the risks of the information technology acquisitions" and will impede the Secretary's ability to fulfill his Clinger-Cohen Act requirements.

- Second, to be effective, the Board needs to perform more substantive, in-depth, analytical reviews of progress, problems, and risks associated with these complicated investments. The current level of support available to the Board is not sufficient to allow the members to make responsible decisions about these investments. The Board relies on the "prep group" process, during which OA representatives perform a cursory review of each other's investment projects. This "prep group" is led by an Associate Chief Information Officer with the support of one mid-level staff person who came on board only 4 months ago. Obtaining adequate support to research potential project shortfalls in cost, schedule, and performance is essential if the Board is to perform oversight to maximize the value and to manage the risks of major IT investments in the Department.

We are making a series of recommendations on pages 21 through 23 of this report to help the Department strengthen its information security program and improve oversight of its multibillion-dollar annual IT investments. The office of the Departmental Chief Information Officer (CIO) agreed with our findings and recommendations. We have requested that DOT provide written comments describing the specific actions it will take to implement these recommendations.

## FINDINGS

### Systems Security

Last year, the Department made a concerted effort to increase the percentage of systems completing the security certification review from 33 percent to over 90 percent. However, the Department did not make the same commitment to this task during FY 2005. As a result, we found that about 15 percent of Departmental systems were overdue for recertification in late August. While the quality of the security certification review has improved during FY 2005, continued management attention is needed to ensure that quality is improved during system recertification reviews. Further, DOT needs to improve the process it uses in correcting identified security weaknesses to ensure that weaknesses are prioritized and corrected in a timely manner.

#### *Systems Security Reviews Need To Be Updated*

Conducting systems security certification reviews is not a one-time challenge but an ongoing business requirement. OMB requires Federal systems security be recertified at least every 3 years because systems are constantly changed to support evolving business and technical needs. Expired security certification and accreditation reviews present little value to management. About 90 percent of all

DOT systems will have to undergo security certification review between FY 2005 and FY 2007, as shown in Table 1.

***Table 1. DOT Systems Security Inventory Certification as of August 2005***

| OA* | Total Systems | Systems Left To Be Recertified in FY 2005 | Systems To Be Recertified in FY 2006 | Systems To Be Recertified in FY 2007 |
|---|---|---|---|---|
| FAA | 263 | 40 | 22 | 155 |
| FHWA | 25 | --- | 5 | 19 |
| FMCSA | 18 | --- | 6 | 11 |
| FRA | 21 | --- | 3 | 16 |
| FTA | 9 | 1 | 3 | 2 |
| MARAD | 12 | --- | 4 | 2 |
| NHTSA | 40 | 31 | 7 | --- |
| OST | 47 | 3 | 30 | 11 |
| PHMSA | 3 | --- | 33 | --- |
| RITA | 28 | --- | 3 | 8 |
| SLSDC | 1 | --- | 1 | --- |
| STB | 2 | --- | 2 | --- |
| **Total** | **469** | **75** | **119** | **224** |

* The full name of DOT Operating Administrations and system inventory counts for FY 2004 and FY 2005 is contained in Exhibit C.

However, in FY 2005, the Department did not assign a priority to completing security recertification reviews. In late August, we found that 75 (15 percent) of Departmental systems no longer had valid security certifications because the reviews were over 3 years old. We brought the issue to management's attention, and the Department engaged in an ambitious plan to recertify these systems by the end of the fiscal year. Our sample review of 20 systems also identified 3 systems with expired security certifications. The Department needs to assign a priority to completing security recertification reviews during FY 2006 and FY 2007, when over 300 systems will need to be recertified.

OMB also requires agencies to have systems security recertified sooner than every 3 years if the system has experienced major changes. In our sample review, we found four systems that had experienced major changes since they were certified and accredited, but none had been recertified. For example, one Maritime Administration system was moved from a contractor's site to the DOT Headquarters building in 2004, which completely changed its computing environment and thus could create new vulnerabilities. However, the Maritime

Administration does not plan to recertify the system until August 2006, when the current certification review expires.

### *Quality of Certification Reviews Needs To Be Enhanced*

Last year, we found deficiencies in the quality of systems security certification reviews, such as inadequate risk assessments, lack of evidence of security tests, and lack of proper senior management involvement in accrediting systems to support program operations. During FY 2005, the CIO Office increased its oversight of the quality of certification reviews, as we recommended. OMB also requires agencies to comply with standards established by the National Institute of Standards and Technology (NIST) in conducting security certification reviews after.[8] We sampled 20 systems security reviews—14 performed before May 2004 and 6 after. Our test results indicated that the quality of certification reviews has improved in the newer certification reviews (see Table 2).

### *Table 2. Quality of Systems Security Certification Reviews*

| Number of Systems Sampled (Number) | Risk Assessment Missing (1) | No Evidence of Security Testing (2) | Weakness Not Summarized (3) | Not Accredited by Proper Official (4) |
|---|---|---|---|---|
| Certified Before May 2004 (14) | 2 | 6 | 13 | 0 |
| Certified After May 2004 (6) | 0 | 1 | 4 | 1 |
| **Total** | **2** | **7** | **17** | **1** |

(1) *Risk Assessment.* Government security standards require agencies to perform security risk assessments based on potential impact to the confidentiality, integrity, and availability of respective system operations. The risk assessment performed for two systems before May 2004 lacked such specificity. A risk assessment is key because it determines the level of security protection and the degree of testing needed to certify a system as adequately secured commensurate with associated operational risks.

[8] Federal Information Processing Standards Number 199, "Standards for Security Categorization of Federal Information and Information Systems," and NIST Special Publication 800–37, "Guide for the Security Certification and Accreditation of Federal Information Systems." The special publication will become part of the minimum Government security standards in December 2005.

(2) *Security Testing*. While a systems security certification review is valid for 3 years as long as no major changes are made to the system, agencies are also required to perform limited annual security testing between certification reviews. Since security testing is a critical component of the certification review process, we independently tested a basic password security control in four systems—three certified before May 2004 and one after. All these systems were certified as having the ability to "lock out" users after they entered three incorrect passwords. However, two of the three systems certified before May 2004 failed our testing.

(3) *Summarizing Weaknesses*. Last year, we recommended that the CIO Office develop guidance for OAs to use in summarizing security test results that would assist accrediting officials when they decide whether to allow the system to operate. This area still requires more management attention. Security weaknesses were not summarized in both old and new certification reviews, inhibiting the ability of accrediting officials to easily evaluate remaining risks. 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. Authorizing officials need to know what remaining risks and corrective actions are planned before approving any system for operation.

(4) *Proper Certification and Accreditation.* Last year, we recommended that the CIO Office modify Departmental guidance to ensure that accreditation is done by appropriate senior officials. However, we continue finding problems in this area. One of the six certification reviews performed after May 2004 was accredited by a mid-level system manager, not the senior official responsible for the program office using the system. Obtaining system accreditation from the correct authorizing official is critical because this official has to accept the system risk (or impact) on business operations and also be able to allocate budget resources to secure the system.

### *More Attention Needed To Correct Known Security Weaknesses*

In reviewing DOT's plans of action and milestones to correct known security weaknesses, we identified several concerns with the process.

- There are about 3,000 known security weaknesses. However, management has not assessed the severity of more than half of them (1,600) or provided cost estimates for fixing the vast majority of these weaknesses. Without this information, management cannot effectively prioritize the use of limited resources so that the most significant weaknesses get fixed first. Some of these unprioritized weaknesses require immediate remediation. For example, one of

the pending corrections is to enhance password security protection in a system that contains privacy information to reduce the risk of unauthorized access.

Planned remediation of more than 300 security deficiencies has been delayed for more than 6 months past scheduled completion dates, including items deemed to have a severe impact on the integrity of program operations, such as causing adverse effects on communications among air traffic control facilities (see Table 3).

### *Table 3. Remediation of Security Weaknesses*

| **Status** | | **Remediation Items** |
|---|---|---|
| Prioritized | | |
| Overdue* | 309 | |
| Current | 896 | 1,205 |
| Not Prioritized | | 1,620 |
| **Total** | | 2,825 |

* Of the 309 overdue items, 7 were rated with high severity, 56 medium, and 246 low.

We understand that not everything can be tackled at once, especially in today's tight budget environment. Management has to make realistic decisions, balancing system importance, risk, and costs in order to prioritize remediation efforts. Yet management cannot effectively prioritize corrective actions if it lacks information on the associated risks and costs.

- The system used to track known security weaknesses lacks security protection itself. Currently, OA users not only can read but also can change the information entered by other users. This is a clear violation of the Department's policy for granting access to people on a need-to-know basis, especially for sensitive information such as air traffic control system weaknesses. Further, there is no management audit trail logging all changes made to the system to ensure accountability.

## Network Security

DOT maintains over 400 public web sites to provide Internet services to the public, and tens of thousands of computers on its private networks 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. The most noteworthy accomplishments include strengthening access security controls at the Internet connection points (the "front doors") and other network entry points (the "back doors"), establishing security incident-response centers, and regularly

checking for potential vulnerabilities in network computers. Last year, we also reported that DOT started developing security configuration policies for commonly used software.

This year, we found that the Department needs to enforce implementation of the security configuration policies, ensure that computer vulnerabilities are corrected in a timely manner, and complete deployment of the intrusion-detection system at one Internet connection point.

### *Security Configuration Policy Needs To Be Enhanced and Enforced*

Configuration management controls need enhancement and enforcement. Proper configuration is key to preventing computer vulnerabilities. FISMA requires each agency to develop specific IT security configuration requirements that meet its needs and to implement the requirements. Last year, we reported that the CIO Office issued baseline security standards for configuring computers using the following five software packages: server-based Windows, Linux, Solaris, Cisco (router), and wireless devices such as personal digital assistants. OAs were required to configure their computers in accordance with these standards.

However, there is little assurance that these security standards have been implemented due to the lack of enforcement. In June 2005, the CIO Office asked OAs to provide information on their implementation status. Only 4 of the 12 OAs provided statistics on their implementation efforts (see Table 4).

### *Table 4. Implementation of Security Configuration Policy*

| Operating Administration | Windows Servers | Cisco Router | Solaris | Linux |
|---|---|---|---|---|
| Federal Highway Administration | 95% | 46% | 93% | n/a* |
| Federal Motor Carrier Safety Administration | 100% | 85% | n/a | n/a |
| Research and Innovative Technology Administration | 92% | 75% | 94% | 100% |
| Federal Railroad Administration | 29% | 49% | n/a | 17% |

* n/a: not applicable because the technology is not used.

Also, two important configuration standards, the Oracle database and the web application, are still not final and are both widely used in DOT. The Oracle database is used in key application systems, such as the Departmental accounting system (Delphi), the Federal Highway Administration's grants 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 attack. In response to last year's 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. However, these standards are still not finalized, partially due to turnover of key security personnel in the CIO Office.

The Department needs to immediately finalize the configuration standards for the Oracle database and web applications and to develop enforcement mechanisms ensuring that DOT computers are configured in accordance with security standards.

### *Network Vulnerabilities Need To Be Checked and Corrected in a Timely Manner*

DOT still faces a challenge in patching of its computer systems in a timely manner. Our recent audit of the Federal Railroad Administration systems network found many vulnerabilities, some of which had been previously reported but remained uncorrected. These weaknesses enabled us to gain total control (root-level access) over a critical file server, desktop computers, and a network switch. From these computers, we accessed sensitive information that enabled us to gain unauthorized entry from the Internet and obtain sensitive information such as draft safety inspection reports and proposed penalties for safety violations. Given the interconnectivity among all DOT networks, this security lapse also puts other Departmental systems at risk. Federal Railroad Administration management is taking action to eliminate all critical vulnerabilities.

The recent Zotob worm attack also showed the need for more timely installation of software patches. More than 700 DOT computers were infected by this worm. The attack occurred 4 days after Microsoft Corporation released a patch to fix a security flaw in its Windows operating system. In DOT, 7 of 12 OAs were infected because they did not install the patch quickly, resulting in operational disruption.

The Zotob worm was first introduced into DOT's network by a contractor who connected his laptop computer to DOT's network, which was a violation of Departmental policy. Nonetheless, this incident highlighted an emerging challenge facing DOT and other Federal agencies concerning security checks on computers used by the telecommuting workforce. For example, about half of all Federal Railroad Administration computers are not subject to routine vulnerability checks because they are being used by employees who telecommute (or travel around the country) for the majority of the year. These unchecked computers, if

infected with hostile software, could become conduits for spreading problems to the rest of the networks. DOT needs to develop a mechanism to ensure that all computers used by telecommuting employees are periodically checked for vulnerabilities and patched with the latest security upgrades.

### *Intrusion-Detection Capability Needs To Be Improved*

Intrusion-detection systems are software or hardware systems used to help detect either the unauthorized use of or attack upon a computer or network. This security is particularly important to organizations with direct connections to the Internet because of relentless attacks by hackers worldwide. The Federal Railroad Administration is one of the OAs with direct connections to the Internet. However, it has not fully deployed an intrusion-detection system, despite years of effort. Until the intrusion-detection system is fully implemented, DOT cannot effectively protect its computers in today's volatile network environment.

## System Continuity and Contingency 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 serious concerns about losing both primary and recovery processing sites for critical systems because they were close to each other. During FY 2004, DOT emphasized this area and reported a significant increase in systems with contingency plans. However, this year we found insufficient testing of contingency plans and continued problems with recovery site locations. The recent events along the Gulf Coast underscore the importance of having adequate geographic distance between primary and recovery sites for continuity of operations.

### *Contingency Plans Need To Be Tested*

OA management is required to assess the consequences of the loss of availability of its computer system services. If deemed to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, management should rate the potential impact "high."[9] This year we reviewed a sample of 20 systems with different levels of impact—55 high, 8 medium, and 7 7 low. Overall, almost half had no contingency plan or recovery site identified,

[9] A loss of availability is the disruption of access to or use of information or an information system (FIPS Publication 199).

and 85 percent had not tested their contingency plans within the previous year (see Table 5).

### *Table 5. Contingency Planning and Testing*

| Availability Rating | High | Medium | Low | Total |
|---|---|---|---|---|
| Number of Systems Reviewed | 5 | 8 | 7 | **20** |
| No Contingency Plan | 1 | 4 | 4 | **9** |
| No Recovery Sites Identified | 1 | 4 | 5 | **10** |
| No Current Testing of Contingency Plan | 4 | 8 | 5 | **17** |

In these times of budgetary constraints, it is important to prioritize which programs and systems are most critical and therefore most in need of continuity of operations during an emergency. For the five high-impact systems, only one system has met all criteria (i.e., having a contingency plan, having a recovery site, and having the plan tested): the National Driver Registry, managed by the National Highway Traffic Safety Administration. The remaining four high-impact systems are all FAA systems. One system that is used to record airman medical examination information did not even have a contingency plan. No contingency plan testing had been performed for any of these systems, including the ones critical to time-sensitive air traffic control services.

#### *Recovery Sites Need To Be Further Separated From Primary Sites*

As we reported in both FY 2003 and FY 2004, some OA recovery sites are too close to the primary processing sites for their computer systems, thus risking loss of processing capability from both sites to the same disaster. The CIO Office agreed to develop Departmental policy establishing the minimum distance requirement between the two processing sites. However, after 2 years, the policy has yet to be developed. None of the OAs has relocated its recovery site to reduce the exposure. For example, the geographic distances between the two sites are still 10 miles for highway systems, 15 miles for transportation statistics systems, and 25 miles for transit systems. As we learned during the 2005 hurricane season, disasters can cover a very wide area.

DOT needs to develop and test contingency plans for the most critical systems, develop a policy on minimum geographical distance between primary and recovery sites, and enforce this policy.

## Protecting the Nation's Critical Infrastructure

The President has designated the air traffic control system part of the nation's critical 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 protected from disruption from man-made or natural events and are able to resume services in a timely manner if disrupted.

Last year, we reported that security certification reviews of en route[10] air traffic control computer systems needed to be enhanced. In particular, while officials had certified that en route systems were adequately secured, the reviews did not meet NIST requirements because they were limited to developmental systems at FAA's technical center computer laboratory. FAA committed to completing security reviews of all operational air traffic control systems—at en route, approach control, and airport terminal facilities—within 3 years. It also agreed to identify a cost-effective contingency plan to restore essential air service should a prolonged disruption affect service at an en route facility. Implementing the selected plan is a complicated endeavor but critical to supplementing FAA's current business continuity strategy, one that has worked well in the past in dealing with temporary, less severe service disruptions.

Yet FAA did not start aggressive actions to correct air traffic control security deficiencies previously identified until April of this year, after the DOT Inspector General issued a letter to the Federal Aviation Administrator expressing concerns over the slow pace of FAA's corrective actions. Progress improved, but since this effort only began in April, overall progress during FY 2005 to better secure air traffic control system operations was insufficient.

### *Security Certification Reviews Need To Be Expanded*

During FY 2005, FAA officials reported that they had conducted security reviews at all en route centers; however, these "reviews" were incomplete. First, FAA conducted site reviews to gather system information only—which has not yet been analyzed—and only on 16 of the 30 high-risk systems used to control air traffic at its en route centers. Since information was collected on only half of the systems, other critical systems, such as the system that routes critical weather and flight plan data to all en route centers, were not reviewed. It plans to analyze the data during FY 2006 to determine what remediation work will need to be done.

[10] En route centers control traffic over 18,000 feet (high-altitude), approach control centers control traffic between 4,000 and 18,000 feet (mid-level), and airport control towers control landings and takeoffs.

Second, no independent testing was performed at operational sites. Such on-site testing is required to meet minimum Government security standards and is critical for these systems. Our prior work identified different system configurations between the baseline (development) system and the operational systems. Independent testing may be the only way to detect such differences and assess the security implications.

FAA also needs to develop a schedule and commit resources to conducting security reviews of operational systems used at other air traffic control facilities. This includes systems used to monitor mid-level air traffic at approach control centers and those used to direct landings and takeoffs at airport control towers. It has previously committed to completing these reviews in 2006 and 2007, respectively.

### *The Selected Contingency Plan Needs To Be Implemented*

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 en route centers, could severely disrupt air traffic in cascading waves across the country, causing significant economic losses and subjecting travelers to widespread delays and inconvenience. FAA's current business continuity strategy has worked well in the past in dealing with temporary service disruptions, such as power outages. This year, FAA has selected a cost-effective alterative to restore essential air traffic service in case of prolonged disruption at an en route facility, but FAA is years away from implementing it.

Implementing this alternative will be a complicated endeavor. It will require restoring computer system operations at recovery centers, rerouting radar signals, and retraining or relocating air traffic controllers familiar with the affected airspace. We recognize that FAA faces critical decisions in balancing its priorities in today's tight budget environment with declining aviation trust fund revenues. Yet items requiring immediate attention should get that attention. FAA needs to start testing recovery of computer operations at back-up en route centers and aggressively pursue the plan to identify air traffic controllers to operate the reconfigured airspace.

## Management Controls

With an annual IT budget of about $2.7 billion, DOT is responsible for one of the largest IT investment portfolios among civilian agencies. As such, it needs to have processes in place that provide reasonable assurance that its major IT projects are adequately justified and monitored to ensure that they deliver promised benefits approximately on time and within budget. The Departmental Investment

Review Board is charged with exercising executive-level oversight to provide that assurance to the Secretary. Last year, we reported that the Board needed to perform more substantive and proactive reviews of IT investments managed by individual OAs. The Board has improved its reviews of investments by most OAs but has been unable so far to have a significant impact on FAA's air traffic control modernization projects, which are the most complex and challenging systems and account for over 80 percent of the Department's IT budget.

### *The Investment Review Board's Role Needs To Be Clarified*

This year, the Board reviewed investment projects managed by various OAs, including FAA. While projects managed by most OAs have benefited from the Board's oversight, the Board has had little positive impact on complicated air traffic control projects, which are still experiencing significant cost increases and schedule delays. We reviewed 16 major FAA acquisitions and found that 9 of them had experienced schedule delays of from 2 to 12 years, and 11 had experienced cost growth of about $5.6 billion (from $8.9 billion to $14.5 billion). The bulk of the cost growth represented by the $5.6 billion occurred before the establishment of the new Air Traffic Organization and had been building for some time without being recognized. Some of the major investment projects have experienced persistent cost and schedule problems, such as the Wide Area Augmentation System and the Standard Terminal Automation Replacement System.

Nine years after Congress passed acquisition reform for FAA, exempting it from compliance with Federal acquisition regulations, air traffic control modernization projects are still experiencing performance problems, along with the cost increases and schedule delays. Further, FAA's acquisition process has stayed on the Government Accountability Office's high-risk list since 1995. Meanwhile, FAA continues to initiate new, costly, and complex IT modernization projects. This year, two new multibillion-dollar FAA investment projects—FAA Telecommunications Infrastructure and En Route Automation Modernization—went forward to OMB without reliable cost, schedule, and other project information. OMB rejected the budget submissions and asked the Board to reexamine business cases for these investment projects.

We are concerned that the Board's review of major FAA IT investment projects is not providing value-added services as intended. Consequently, the Board's role risks becoming a paperwork exercise with little substantive value added to help the Secretary. There are two basic reasons for this.

- First, there is a lack of clarity about the Board's role in reviewing major FAA investment projects. The Clinger-Cohen Act of 1996 requires the Secretary to implement a process for "maximizing the value and assessing and managing

the risks of the information technology acquisitions of the executive agency." The Board was created as part of this process and is tasked with advising the Secretary regarding whether to continue, modify, or terminate major IT investments in the Department. However, FAA has frequently cited its independent acquisition authority, based on provisions in the Department's Appropriations Act for Fiscal Year 1996, to argue that the Board should play only a limited role in overseeing FAA investments. The provision in the Appropriations Act exempted FAA from compliance with the Federal acquisition regulations and key Federal procurement laws to help make the acquisition process more timely and cost-effective.

The issue that needs to be resolved is whether FAA's exemption from compliance with the Federal procurement regulations also applies to the investment management oversight requirements of the Clinger-Cohen Act. Until this issue is resolved, it is our opinion that the Board's continued "review" of FAA's multibillion-dollar investment projects will not provide reasonable assurance to the Secretary that FAA's major IT investments are adequately justified and monitored to ensure that they deliver promised benefits approximately on time and within budget. This will, in turn, impede the Secretary's ability to fulfill his responsibilities under the Clinger-Cohen Act.

- Second, to be effective, the Board needs to perform more substantive, in-depth, analytical reviews of progress, problems, and risks associated with these complicated investments. The current level of support available to the Board is not sufficient to allow its members to make responsible decisions about these investments. The Board relies on the "prep group" process, during which OA representatives perform a cursory review of each other's investment projects. This "prep group" is led by an Associate Chief Information Officer with the support of one mid-level staff person, who came on board only 4 months ago. Obtaining adequate support to research potential shortfalls in project cost, schedule, and performance is essential if the Board is to perform oversight that will maximize the value and to manage the risks of major IT investments in the Department.

### *More Focus Is Needed To Implement Management Tools To Track Progress of Major Systems*

Last year, we recommended that the CIO Office develop a better process to select investment projects for the Board's review. During FY 2005, the Department started using a sophisticated tool to identify at-risk projects for the Board's review: Earned Value Management (EVM). This approach measures progress against approved cost and schedule baselines. Through these measures, management can spot early projects that are falling behind schedule or are running over cost, before

they become “troubled” (experiencing a greater-than-10-percent variance from the baseline).

However, EVM usage at DOT is still in its infancy and is not yet being applied correctly across the Department. OMB recently issued a memorandum to all agencies, entitled “Improving IT Project Planning and Execution,” which outlines the need for further improvement Governmentwide in the use of EVM and listed 32 criteria developed by the American National Standards Institute. A recent study conducted by FAA on 19 major acquisition projects indicated that EVM reporting for over 60 percent of the projects did not meet OMB criteria.

It is also important that the OAs apply EVM measurements based on complete and accurate information. Otherwise, the tool will produce misleading results. For example, when evaluating whether a multibillion-dollar telecommunications project was proceeding according to schedule, FAA used “site acceptance”—how many sites had equipment installed and tested—to measure progress. However, site acceptance was only an interim step toward the ultimate goal of switching communications services to the new network. By using site acceptance as the measure, management was led to believe that the project was closer to completion than it actually was. DOT needs to ensure that OAs implement EVM management tools effectively by, for example, making sure that OAs provide accurate and complete information for EVM measurement. EVM training will also need to be a key focus in the coming year.

## RECOMMENDATIONS

In order to strengthen the Department’s information security posture and reduce its vulnerability to economic or operational harm, we recommend that the Department CIO:

**Enhance computer systems security reviews by:**

1. Requiring OAs to submit planned schedules for completing systems security (re)certification reviews throughout FY 2006 and conduct quarterly reviews of the progress made against the plans.

2. Increasing sample checks of OAs’ systems security reviews to ensure compliance with minimum Government standards, including performing recertification reviews of any systems that have experienced major changes.

3. Ensuring that OAs assess the severity of identified security weaknesses, estimate correction costs, and prioritize the remediation effort accordingly and ensuring that OAs correct deficiencies in a timely manner.

4. Enhancing security of the DOT system that tracks the plan of action and milestones by limiting access to those with a need to know and developing management audit trails to track changes made in the system.

**Enhance DOT network security by:**

5. Finalizing Departmental security standards for configuring the Oracle database and web application software on DOT systems and validating that DOT computers are configured in accordance with established security standards.

6. Verifying that OAs are correcting computer vulnerabilities and installing manufacturers' software patches in a timely manner.

7. Developing a mechanism to ensure that all computers used by telecommuting employees are periodically checked for vulnerabilities and patched with the latest security upgrades.

8. Working with the Federal Railroad Administration to fully implement an intrusion-detection system on its network.

**Enhance the DOT continuity of operations plan by:**

9. Requiring the OAs to prepare and test contingency plans and to provide evidence that the contingency plan for critical information systems has been successfully tested.

10. Developing Departmental policy establishing the minimum acceptable geographical distance between the primary and recovery processing sites for information systems, and setting a target completion date for the OAs to comply with the policy.

**Enhance critical infrastructure protection by:**

11. Directing FAA to complete, by the end of FY 2006, security certification reviews that meet NIST standards for operational air traffic control systems at en route centers and to complete security reviews at other operational sites (e.g., approach control centers and airport control towers) by the end of FY 2007, as FAA has committed to doing.

12. Ensuring that FAA continues to implement its en route continuity of operations plan by testing recovery of computer operations at back-up en route centers and identifying air traffic controllers to operate the reconfigured airspace during FY 2006.

13. Periodically reviewing the progress and quality of FAA's certification reviews and en route continuity of operations plan implementation.

**Enhance IT investment management controls by:**

14. Clarifying, in consultation with the Secretary, the Departmental Investment Review Board's role in performing investment management oversight of FAA's major investments.

15. Identifying resources and processes to better support the Board by performing more substantive, in-depth, analytical reviews of progress, problems, and risks associated with major FAA investments.

16. Ensuring that the OAs receive training in using the EVM management tool and that they use the tool effectively by including accurate and complete cost and schedule information.

## MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

The CIO Office reviewed a draft of this report and provided oral comments. CIO Office officials agreed with the report's findings and recommendations and stated that they will provide written comments describing the specific actions they will take to implement the recommendations.

## ACTIONS REQUIRED

In accordance with DOT Order 8000.1C, we would appreciate receiving your written comments on this report 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 CIO and the OAs' representatives during this audit. If you have any questions concerning this

report, please call me at (202) 366-1959 or Theodore Alves, Principal Assistant Inspector General for Auditing and Evaluation, at (202) 366-1992.

#

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

**Section C: Inspector General. Questions 1, 2, 3, 4, and 5.**

**Agency Name: Department of Transportation**

**Question 1 and 2**

**1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).**

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

**2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.**

| | | Question 1 | | | | | | Question 2 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | a. FY 05 Agency Systems | | b. FY 05 Contractor Systems | | c. FY 05 Total Number of Systems | | a. Number of systems certified and accredited | | b. Number of systems for which security controls have been tested and evaluated in the last year | | c. Number of systems for which contingency plans have been tested in accordance with policy and guidance | |
| Bureau Name | FIPS 199 Risk Impact Level | 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 |
| FAA | High | 81 | 5 | 11 | 2 | 92 | 7 | 5 | 71.4% | 5 | 71.4% | | 0.0% |
| | Moderate | 126 | 3 | 8 | | 134 | 3 | 2 | 66.7% | 3 | 100.0% | | 0.0% |
| | Low | 42 | | 3 | | 45 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | 0 | |
| | **Sub-total** | **249** | **8** | **22** | **2** | **271** | **10** | **7** | **70.0%** | **8** | **80.0%** | **0** | **0.0%** |
| FHWA | High | 7 | | | | 7 | 0 | | | | | | |
| | Moderate | 13 | | 1 | | 14 | 0 | | | | | | |
| | Low | 2 | | 1 | | 3 | 0 | | | | | | |
| | Not Categorized | | 1 | | | 0 | 1 | 1 | 100.0% | 0 | 0.0% | 1 | 100.0% |
| | **Sub-total** | **22** | **1** | **2** | **0** | **24** | **1** | **1** | **100.0%** | **0** | **0.0%** | **1** | **100.0%** |
| FMCSA | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 13 | | 3 | | 16 | 0 | | | | | | |
| | Low | 3 | | | | 3 | 0 | | | | | | |
| | Not Categorized | | 1 | | | 0 | 1 | 1 | 100.0% | 1 | 100.0% | 0 | 0.0% |
| | **Sub-total** | **16** | **1** | **3** | **0** | **19** | **1** | **1** | **100.0%** | **1** | **100.0%** | **0** | **0.0%** |
| FRA | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 18 | 1 | 3 | | 21 | 1 | 1 | 100.0% | | 0.0% | | 0.0% |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | 0 | | 0 | |
| | **Sub-total** | **18** | **1** | **3** | **0** | **21** | **1** | **1** | **100.0%** | **0** | **0.0%** | **0** | **0.0%** |
| FTA | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 8 | | 1 | | 9 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | 1 | 0 | 1 | 1 | 100.0% | 1 | 100.0% | 0 | 0.0% |
| | **Sub-total** | **8** | **0** | **1** | **1** | **9** | **1** | **1** | **100.0%** | **1** | **100.0%** | **0** | **0.0%** |
| MARAD | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 6 | | | | 6 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | 7 | 1 | | | 7 | 1 | 1 | 100.0% | 0 | 0.0% | 0 | 0.0% |
| | **Sub-total** | **13** | **1** | **0** | **0** | **13** | **1** | **1** | **100.0%** | **0** | **0.0%** | **0** | **0.0%** |
| NHSTA | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 6 | | 1 | | 7 | 0 | | | | | | |
| | Low | 10 | | 1 | | 11 | 0 | | | | | | |
| | Not Categorized | | | | 1 | 0 | 1 | 1 | 100.0% | 1 | 100.0% | 1 | 100.0% |
| | **Sub-total** | **16** | **0** | **2** | **1** | **18** | **1** | **1** | **100.0%** | **1** | **100.0%** | **1** | **100.0%** |
| OST | High | 6 | | | | 6 | 0 | | | | | | |
| | Moderate | 18 | | 3 | | 21 | 0 | | | | | | |
| | Low | 20 | | 3 | | 23 | 0 | | | | | | |
| | Not Categorized | 2 | 2 | | | 2 | 2 | 2 | 100.0% | 1 | 50.0% | 1 | 50.0% |
| | **Sub-total** | **46** | **2** | **6** | **0** | **52** | **2** | **2** | **100.0%** | **1** | **50.0%** | **1** | **50.0%** |
| PHMSA | High | 1 | | | | 1 | 0 | | | | | | |
| | Moderate | 1 | 1 | 1 | | 2 | 1 | 1 | 100.0% | | 0.0% | | 0.0% |
| | Low | 1 | | | | 1 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | 0 | | 0 | |
| | **Sub-total** | **3** | **1** | **1** | **0** | **4** | **1** | **1** | **100.0%** | **0** | **0.0%** | **0** | **0.0%** |
| RITA | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 16 | | | | 16 | 0 | | | | | | |
| | Low | 1 | | | | 1 | 0 | | | | | | |
| | Not Categorized | | 1 | | | 0 | 1 | 1 | 100.0% | 1 | 100.0% | 0 | 0.0% |
| | **Sub-total** | **17** | **1** | **0** | **0** | **17** | **1** | **1** | **100.0%** | **1** | **100.0%** | **0** | **0.0%** |
| SLSDC | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | 1 | | | | 1 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **1** | **0** | **0** | **0** | **1** | **0** | | | | | | |
| STB | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | | | | 2 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **2** | **0** | **0** | **0** | **2** | **0** | | | | | | |
| **Agency Totals** | **High** | **95** | **5** | **11** | **2** | **106** | **7** | **5** | 71.4% | **5** | 71.4% | **0** | 0.0% |
| | **Moderate** | **227** | **5** | **21** | **0** | **248** | **5** | **4** | 80.0% | **3** | 60.0% | **0** | 0.0% |
| | **Low** | **80** | **0** | **8** | **0** | **88** | **0** | **0** | | **0** | | **0** | |
| | **Not Categorized** | **9** | **6** | **0** | **2** | **9** | **8** | **8** | 100.0% | **5** | 62.5% | **3** | 37.5% |
| | **Total** | **411** | **16** | **40** | **4** | **451** | **20** | **17** | 85.0% | **13** | 65.0% | **3** | 15.0% |

| Question 3 | | |
|---|---|---|
| In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory. | | |
| **3.a.** | The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contracto or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.<br><br>Response Categories:<br>- Rarely, for example, approximately 0-50% of the time<br>- Sometimes, for example, approximately 51-70% of the time<br>- Frequently, for example, approximately 71-80% of the time<br>- Mostly, for example, approximately 81-95% of the time<br>- Almost Always, for example, approximately 96-100% of the time | - Almost Always, for example, approximately 96-100% of the time |
| **3.b.** | The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all othe systems or networks, including those not operated by or under the control of the agency.<br><br>Response Categories:<br>- Approximately 0-50% complete<br>- Approximately 51-70% complete<br>- Approximately 71-80% complete<br>- Approximately 81-95% complete<br>- Approximately 96-100% complete | - Approximately 96-100% complete |
| **3.c.** | The OIG **generally** agrees with the CIO on the number of agency owned systems. | Yes |
| **3.d.** | The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. | Yes |
| **3.e.** | The agency inventory is maintained and updated at least annually. | Yes |
| **3.f.** | The agency has completed system e-authentication risk assessments. | no |

| Question 4 | | |
|---|---|---|
| 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. 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 area provided below.<br><br>For items 4a.-4.f, the response categories are as follows:<br>- Rarely, for example, approximately 0-50% of the time<br>- Sometimes, for example, approximately 51-70% of the time<br>- Frequently, for example, approximately 71-80% of the time<br>- Mostly, for example, approximately 81-95% of the time<br>- Almost Always, for example, approximately 96-100% of the time | | |
| **4.a.** | The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. | - Mostly, for example, approximately 81-95% of the time |
| **4.b.** | When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s). | - Rarely, for example, approximately 0-50% of the time" |
| **4.c.** | Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress. | - Almost Always, for example, approximately 96-100% of the time |
| **4.d.** | CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis. | - Rarely, for example, approximately 0-50% of the time" |
| **4.e.** | OIG findings are incorporated into the POA&M process. | - Almost Always, for example, approximately 96-100% of the time |
| **4.f.** | POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources | - Rarely, for example, approximately 0-50% of the time" |
| **Comments: The Department needed to strengthen its security remediation activities to ensure that weaknesses are being corrected in a timely manner and that the most critical weaknesses are corrected first. Currently, the Department has about 3,000 weaknesses pending remediation. However, management could not effectively prioritize their correction because 1,620 weaknesses (more than half of the items in the database) are missing information such as the severity of, and costs to correct, the weakness. However, some of these weaknesses clearly require immediate remediation.** | | |

| Question 5 | | |
|---|---|---|
| OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. Thi includes use of the FIPS 199 (February, 2004), "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 . | | |
| | Assess the overall quality of the Department's certification and accreditation process<br><br>Response Categories:<br>- Excellent<br>- Good<br>- Satisfactory<br>- Poor<br>- Failing | - Satisfactory |
| **Comments: The quality of the security certification reviews has improved during FY 2005. This year our sample review of 20 systems security certification reviews, 6 of which were completed during FY 2005, identified fewer deficiencies in the newer certification reviews. Nonetheless, improving the quality of the certification reviews will be a major challenge to the Department when re-certifying more than 300 systems security in the next 2 years.** | | |

**Section B: Inspector General. Question 6, 7, 8, and 9.**

**Agency Name:**

**Question 6**

| | | |
|---|---|---|
| **6.a.** | Is there an agency wide security configuration policy?<br>Yes or No. | Yes |
| | Comments: | |

**6.b.** Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

| **Product** | **Addressed in agencywide policy?**<br><br>**Yes, No, or N/A.** | **Do any agency systems run this software?**<br><br>**Yes or No.** | **Approximate the extent of implementation of the security configuration policy on the systems running the software.**<br><br>**Response choices include:**<br>**- Rarely, or, on approximately 0-50% of the systems running this software**<br>**- Sometimes, or on approximately 51-70% of the systems running this software**<br>**- Frequently, or on approximately 71-80% of the systems running this software**<br>**- Mostly, or on approximately 81-95% of the systems running this software**<br>**- Almost Always, or on approximately 96-100% of the systems running this software** |
|---|---|---|---|
| Windows XP Professional | Yes | Yes | |
| Windows NT | Yes | Yes | |
| Windows 2000 Professional | Yes | Yes | - Frequently, or on approximately 71-80% of the systems running this software |
| Windows 2000 Server | Yes | Yes | - Frequently, or on approximately 71-80% of the systems running this software |
| Windows 2003 Server | No | Yes | |
| Solaris | Yes | Yes | - Frequently, or on approximately 71-80% of the systems running this software |
| HP-UX | No | Yes | |
| Linux | Yes | Yes | - Frequently, or on approximately 71-80% of the systems running this software |
| Cisco Router IOS | Yes | Yes | - Sometimes, or on approximately 51-70% of the systems running this software |
| Oracle | No | Yes | |
| Other. Specify: Wireless | Yes | Yes | |

Comments: DOT has issued 5 configuration standards (server-based Windows, Linux, Solaris, Cisco and Wireless PDA). However, there is little assurance for the implementation of these security standards. In June 2005, the CIO office asked OAs to provide implementation status on these standards. Only 4 of the 12 OAs provided statistics on their implementation effort. Based on our review, the statistics provided by 4 OAs appeared to be reasonable and were used to form our answers above.

**Question 7**

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

| | | |
|---|---|---|
| **7.a.** | The agency follows documented policies and procedures for identifying and reporting incidents internally.<br>Yes or No. | Yes |
| **7.b.** | The agency follows documented policies and procedures for external reporting to law enforcement authorities.<br>Yes or No. | Yes |
| **7.c.** | The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov<br>Yes or No. | Yes |
| Comments: | | |

| | | |
|---|---|---|
| | **Question 8** | |
| **8** | Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?<br><br>Response Choices include:<br>- Rarely, or, approximately 0-50% of employees have sufficient training<br>- Sometimes, or approximately 51-70% of employees have sufficient training<br>- Frequently, or approximately 71-80% of employees have sufficient training<br>- Mostly, or approximately 81-95% of employees have sufficient training<br>- Almost Always, or approximately 96-100% of employees have sufficient training | - Sometimes, or approximately 51-70% of employees have sufficient training |
| | **Question 9** | |
| **9** | Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?<br>Yes or No. | No |

## EXHIBIT B. SCOPE AND METHODOLOGY

During FY 2005, we fulfilled the requirements under FISMA by reviewing DOT's major financial systems, FAA air traffic control systems, the Federal Railroad Administration systems network, and the implementation of IT capital planning and investment control procedures. In addition, we sampled 20 systems that had undergone security certification reviews to determine whether the OAs had complied with Government and DOT standards in assessing system risks, identifying security requirements, testing security controls, and accrediting systems to support business operations.

We 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 NIST. We used commercial scanning software to assess network vulnerabilities.

We performed our work throughout FY 2005, and focused on reviewing FISMA reporting between July 2005 and September 2005 at DOT and OAs' Headquarters located in Washington, DC. This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards prescribed by the Comptroller General of the United States and included such tests as we considered necessary to detect fraud.

We previously issued four audit reports on DOT's information security program in response to the legislative mandate of the FISMA, formerly the Government Information Security Reform Act (GISRA). They are: "DOT Information Security Program," Report Number FI-2005-001, October 1, 2004; "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 AND SYSTEM INVENTORY COUNTS

| Operating Administration | Acronym | FY 2004 | FY 2005 |
|---|---|---|---|
| Federal Aviation Administration | FAA | 285 | 271 |
| Federal Highway Administration | FHWA | 24 | 24 |
| Federal Motor Carrier Safety Administration | FMCSA | 19 | 19 |
| Federal Railroad Administration | FRA | 22 | 21 |
| Federal Transit Administration | FTA | 9 | 9 |
| Maritime Administration | MARAD | 12 | 13 |
| National Highway Traffic Safety Administration | NHTSA | 38 | 18 |
| Office of the Secretary | OST | 54 | 52 |
| Pipeline and Hazardous Materials Safety Administration | PHMSA | 3 | 4 |
| Research and Innovative Technology Administration | RITA | 16 | 17 |
| Saint Lawrence Seaway Development Corporation | SLSDC | 1 | 1 |
| Surface Transportation Board | STB | 2 | 2 |
| **Total Systems** | | **485** | **451** |

# EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

| Name | Title |
|---|---|
| Rebecca C. Leng | Assistant Inspector General for Information Technology and Computer Security |
| Ed Densmore | Program Director |
| Phil DeGonzague | Project Manager |
| Nathan Custer | Project Manager |
| Dr. Ping Z. Sun | Project Manager |
| Lynn Dowds | Senior Auditor |
| Tim Roberts | Senior Auditor |
| John Johnson | Senior Information Technology Specialist |
| Mitchell Balakit | Information Technology Specialist |
| Christopher Cullerot | Information Technology Specialist |
| Atul Darooka | Information Technology Specialist |
| Narja Hylton | Auditor |
| Michael P. Fruitman | Communications Adviser |