

# **INFORMATION SECURITY PROGRAM**

*Department of Transportation*

*Report Number: FI-2007-002*

*Date Issued: October 23, 2006*

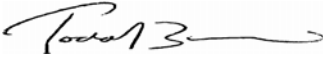


# Memorandum

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-2007-002

Date: October 23, 2006

  
From: Todd J. Zinser  
Acting 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) securing information systems and protecting sensitive agency data, (2) strengthening air traffic control system security as part of the nation's critical infrastructure, and (3) enhancing the departmental Investment Review Board's (IRB) ability to identify performance gaps in major information technology (IT) investments. We are also contributing to DOT's annual FISMA report by answering questions specified by the Office of Management and Budget (OMB). Our contribution to the annual DOT FISMA report is included as Exhibit A.

Similar to last year, in carrying out these objectives, 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 a detailed follow-up review of the Department's process for managing remediation of known security deficiencies.

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, waste, or abuse. Details of our scope and methodology are described in Exhibit B.

## **INTRODUCTION**

FISMA requires Federal agencies to identify and provide security protection commensurate with the risk and magnitude of harm resulting from the loss of, misuse of, unauthorized access to, or modification of information collected or maintained by or on behalf of an agency. 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) 2006, DOT's IT budget totaled about \$2.5 billion. During FY 2006, DOT experienced leadership changes at both departmental and Federal Aviation Administration (FAA) Chief Information Officer (CIO) offices.

The Department has 12 Operating Administrations (OA). All OAs except FAA and the Surface Transportation Board (STB) are scheduled to relocate to a new Headquarters building next year. To support this move, the Department consolidated individual OAs' IT infrastructures (e-mail, desktop computing, and local area networks) into a common IT operating environment. This consolidated IT infrastructure presents opportunities to enhance the Department's information security, along with challenges that include installing, testing, and accrediting the new common IT operating environment; installing more than 75 OA application systems on the new IT infrastructure; and recertifying the security of these systems to support business operations in the new Headquarters building—all on a very tight and still evolving schedule.

For FY 2006, the Department reported a total of 426 computer systems, about 6 percent fewer than last year as a result of its continuing effort to consolidate systems. Among the systems the Department maintains and operates is the air traffic control system, which the President has designated a national 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 2005 and FY 2006 for each OA are detailed in Exhibit C.

## **RESULTS IN BRIEF**

During FY 2006, the Department made noticeable improvement in tracking, prioritizing, and correcting security weaknesses—a major concern identified last year. The Department also took aggressive action to identify systems containing personally identifiable information (PII) for proper security protection, including procuring encryption software to secure all laptop computers. In addition, the departmental IRB provided oversight to a multibillion-dollar IT investment project managed by FAA.

FY 2007 will be a particularly challenging year for the Department in managing its IT security and investments. It has to recertify more than half of all its information systems, upgrade systems security to meet new Government standards, relocate its Headquarters (including more than 75 information systems), and take aggressive action to strengthen air traffic control systems security protection. In addition, the Department needs to develop a better methodology to validate the security configurations of commercial software products installed in DOT systems and continue enhancing oversight of IT investments. Specifically:

- **Air Traffic Control.** Securing the nation's critical air traffic control systems infrastructure should be a top priority of DOT's information security program. However, FAA has not made adequate progress in implementing planned corrective actions. In FY 2004, FAA committed to developing contingency planning for restoring essential air services in case of prolonged service disruption and completing reviews of operational air traffic control systems security over a period of 3 years. Last year, we reported that FAA's overall progress was insufficient because it did not start to initiate corrective action in earnest until April 2005. During FY 2006, FAA made limited progress in these areas due, according to FAA management, to funding constraints. We recognize that FAA faces critical decisions in balancing its priorities and using its funds at a time of increasingly tight budgets. Yet issues concerning the security of a critical national infrastructure should receive priority and immediate attention. The FAA Deputy Administrator, the head of the Air Traffic Organization, and the FAA CIO committed to developing detailed work plans, allocating required resources, and implementing corrective actions. During FY 2007, we plan to initiate an audit of FAA's progress in reviewing operational systems security and contingency planning in accordance with the approved plans.
- **Security Recertification.** About 230 systems—more than half of the Department's total inventory—are due for security recertification during FY 2007. On top of that, these systems must meet new minimum Government security standards before they can be recertified, which will require security upgrades in some cases. Meeting these new standards also requires policy guidance and awareness training. For example, system owners did not properly follow National Institute of Standards and Technology (NIST) guidance in assigning risk categories for 6 of 14 systems sampled this year. If not corrected, the erroneous (lower) risk rating could result in inadequate security protection for these systems. Further, critical infrastructure systems used to direct air traffic control and track shipments of hazardous materials were reported as having a moderate risk impact, which is inconsistent with OMB direction. The departmental CIO informed us that he plans to issue new policy guidance on risk categorization in FY 2007 to ensure more consistent

risk-impact analyses. Therefore, in our submission to OMB this year, we decided not to report how many high, moderate, or low risk-impact systems the Department had.

- **IT Infrastructure Consolidation.** In FY 2007, the Department has to implement a consolidated IT infrastructure to support all OAs relocated to the new Headquarters building. While this consolidated IT infrastructure presents a good opportunity to consolidate IT operations and eliminate fragmentation, it will require a higher level of security protection because the potential impact of disruption will be greater—i.e., on multiple OAs, not just one. However, the plan and schedule to implement and test this new infrastructure are still evolving, due to a variety of move-related problems. As part of this IT consolidation, the Department should also identify a systems backup/recovery site at a sufficient geographic distance from the new Headquarters and conduct systems contingency testing after completing the Headquarters move. Further, the CIO needs to direct OAs not to make additional investments to equip their individual system backup/recovery sites until decisions have been made for the consolidated recovery site. As we previously reported, some OA recovery sites are within a short distance from Headquarters—10, 15, or 25 miles. In case of an emergency, OAs would be likely to lose both the primary and backup computers used to support their missions. Such sites should be replaced by the consolidated backup/recovery site.
- **Network Security.** In the past several years, the Department has done a commendable job in enhancing its network security against both internal and external attacks based on known vulnerabilities in commercial off-the-shelf software, such as the Windows operating system and Oracle database system. To further reduce this risk, all agencies are now required to configure these commercial systems in accordance with NIST or agency standards. During FY 2006, 9 of 12 OAs submitted documentation to the CIO office to support their compliance with standards. However, the submissions were incomplete and inconclusive. As a result, the Department cannot determine whether commercial software is properly configured to help prevent attacks on DOT systems. The CIO needs to develop a better method of evaluating OAs' compliance with security configuration standards.
- **IT Investment Management.** In FY 2005, we recommended that the Department clarify the IRB's authority and increase the Board's capability to research potential project cost, schedule, and performance shortfalls on complicated IT investments. Subsequently, the Department confirmed that the Board, through advising the Secretary, can influence budget decisions on all IT investments. During FY 2006, using this authority, the Board enhanced project management of a multibillion-dollar investment project called the FAA

Telecommunications Infrastructure. In terms of identifying problems associated with major IT investments, the Department plans to delegate more responsibilities to individual OA review boards to oversee their specific IT investments. While we support the idea of holding each OA accountable for its own projects, this will not be possible until clear performance measures are established, such as Earned Value Management (EVM) measures. However, we found 70 percent of DOT's major IT investment projects met fewer than half of OMB's criteria for EVM implementation.

We are making a series of recommendations, starting on page 15, to help the Department strengthen its information security program, the security protection of the critical air traffic control systems infrastructure, and oversight of its multibillion-dollar annual IT investments. The departmental 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**

### **Protecting the Nation's Critical Infrastructure: FAA Needs To Make Greater Progress in Reviewing Operational Systems and in Contingency Planning**

The President has designated air traffic control systems a critical national infrastructure due to the important role commercial aviation plays in fostering and sustaining the national economy and ensuring citizens' safety and mobility. In FY 2004, based on audit findings, FAA made a strong commitment to enhancing the security protection of air traffic control systems. One of its promises was to complete security reviews of all operational air traffic control systems—at en route, approach control, and airport terminal facilities—between FY 2005 and FY 2007. This is critical to protecting air traffic control systems because security vulnerabilities could inadvertently be created when changes are made to the "baseline" systems to meet local operational needs.

FAA made little progress in reviewing operational air traffic control systems security until after April 2005, when the Inspector General sent a letter to the FAA Administrator expressing concern over the slow pace of the corrective action. By the end of FY 2005, FAA had conducted initial reviews at all en route facilities, representing a clear step in the right direction. However, FAA did not follow through with this effort during FY 2006 because of, according to FAA officials, a funding shortage.

In October of this year, the FAA CIO and the head of the Air Traffic Organization committed to developing a plan by the end of December 2006 detailing the approach FAA will take during FY 2007 to evaluate security differences between systems used to direct air traffic at terminal and tower facilities and the “baseline” systems previously tested in its computer laboratory. If this process is implemented effectively, it will significantly strengthen security protection of air traffic control systems.

Another FAA promise was to develop a contingency plan to restore essential air services in case of prolonged service disruptions at en route centers. FAA’s existing business continuity plan has worked well in the past to ensure flight safety when dealing with temporary, less severe disruptions. In FY 2005, we reported that FAA had identified a contingency strategy to deal with prolonged service disruptions but was years away from its implementation. In October 2006, the FAA Deputy Administrator informed us that FAA had identified an interim solution based on the results of an engineering study. The Deputy Administrator also made a strong commitment to fund this interim solution with existing FAA resources.

We recognize that FAA faces critical decisions in balancing its priorities and using its funds at a time of increasingly tight budgets. Yet issues concerning the security of a critical national infrastructure should receive attention and support from OMB and Congress. We plan to initiate an audit of FAA’s progress in reviewing operational systems security and implementing the interim solution for contingency planning in accordance with the approved plans.

### **Systems Security: The Department Faces a Unique Challenge in Recertifying More Than Half of Its Systems’ Security in Fiscal Year 2007, While Meeting a New Government Security Standard**

In FY 2004, the Department made significant strides in reviewing and testing information systems security and successfully increased the systems certification and accreditation rate from 33 percent to over 90 percent. The certification and accreditation process is a statutory requirement to ensure that information systems are adequately secured to support agency missions and must be conducted every 3 years or upon major system change. The reviews conducted in 2004 are due for recertification in 2007, as will be the systems moving to the new Headquarters building—as moving constitutes a significant change. Prior to the move, the CIO decided to delay recertifying systems that were moving to the new building and were due to be recertified within 180 days of their scheduled move date. The CIO also extended the system certification statements for an additional 120 days after the systems move. Given the move, DOT will be faced with the need to recertify

some 230 systems during FY 2007—almost double the number that DOT would like to review on a yearly basis (see Table 1).

**Table 1. Number of DOT Systems Due For Security Recertification as of September 28, 2006**

OA*	Systems to be recertified in:			Total systems
	FY 2007	FY 2008	FY 2009	
FAA	106	79	78	263
FHWA	23	0	0	23
FMCSA	11	4	7	22
FRA	9	0	13	22
FTA	5	0	1	6
MARAD	12	0	0	12
NHTSA	14	2	2	18
OST	38	1	4	43
PHMSA	3	1	1	5
RITA	8	0	1	9
SLSDC	0	0	1	1
STB	1	0	1	2
<b>Total</b>	<b>230</b>	<b>87</b>	<b>109</b>	<b>426</b>

\*See Exhibit C for a list of OA acronyms.

### **Systems Security Needs To Be Upgraded To Meet Minimum Standards**

In addition to the number of systems that require recertification, another complication is that the recertifications will have to be conducted to a higher standard. FISMA required NIST to develop minimum security standards for Federal agencies' systems. These new standards become effective in March 2007 and will most likely require security upgrades in the Department's systems. In an attempt to estimate the gap between existing security controls and the minimum security requirements, we performed a preliminary assessment on a safety-sensitive system that had undergone the security certification review in previous years. It met only about two-thirds of the minimum security standards in one critical area. Although this gap is not a reflection of improper certification reviews in the past, it needs to be addressed before the system is recertified in the future.

Another area that can have a significant impact on the quality of the review is determining the correct risk categorization of a system. This categorization is the first step in determining what minimum security controls will be required for a system. Six of 14 systems sampled this year were incorrectly categorized with a lower-than-warranted risk-impact level. In addition, critical infrastructure systems



used to direct air traffic control and track shipments of hazardous materials are reported as having a moderate risk-impact, which is inconsistent with OMB direction.

We also reviewed systems containing PII. These systems contain individuals' names and unique identifiers, such as social security numbers. DOT has made progress by identifying PII systems, but has no assurance that they are adequately secured, because the correct impact level was not identified. Our review of the risk impact levels of the 100 DOT PII systems uncovered varying levels of confidentiality: 9 high, 63 moderate, 18 low, and 10 lacking a rating. Further evaluation of the 18 PII systems with a low confidentiality risk rating identified 11 with a low overall risk rating.<sup>1</sup> This is contrary to DOT policy, which states that any system containing PII must by definition have an overall risk level rating of at least moderate.

To meet all of these challenges, the OAs will need to submit system recertification work schedules for approval, identify security upgrade needs and funding sources, and report progress against approved schedules throughout the year. Continual oversight by the departmental CIO will be needed to ensure that the schedules address the funding sources and upgrades needed for the recertifications, to measure OAs' progress against their plans, and to provide policy guidance where necessary throughout the year.

### ***Responsibility for Securing Safety Systems Used Nationwide Needs To Be Clarified***

We also found that the Commercial Driver's License Information System (CDLIS) is not included in the departmental systems inventory—and therefore did not receive a system security review. CDLIS is used by the Federal Motor Carrier Safety Administration (FMCSA) and state agencies to manage information on drivers holding commercial driver's licenses. Contained in the system are an individual's name, address, social security number, date of birth, and race. The system works as a pointer system,<sup>2</sup> similar to the National Driver Register (NDR)—another safety-critical system, which we reviewed last year. The Department has a legal responsibility to protect the information in both of these systems, yet is inconsistent in its approach to them. For example, NDR has had a system security review in the past few years, while CDLIS has not. The

---

<sup>1</sup> Systems are rated for confidentiality, integrity, and availability and are also given an overall rating, which is equal to the highest rating given for any of those three components.

<sup>2</sup> A pointer system is one that provides abbreviated information while identifying the location of a more complete record. In the case of NDR, limited information is available on individuals whose privilege to drive has been revoked, suspended, canceled, or denied or who have been convicted of a serious traffic-related offense. The system also identifies the state in which a more complete record can be accessed.

Department thus lacks assurance that CDLIS is operating at a level of security commensurate with its risks.

When we attempted to determine the cause for its exclusion from the Department's inventory, the reason provided by FMCSA was that CDLIS is only a grants program, meaning that the organization receiving the grant would be responsible for the system. In our opinion, however, CDLIS remains a DOT system. FMCSA officials have asked their counsel for an opinion on the matter and will not commit to conducting a security review until the legal opinion is received. In the interim, however, FMCSA has initiated action to meet with the contractor, review the security in place, and determine if it is effective and adequate. Following this meeting and security review, FMCSA will plan a course of action to remediate any gaps found in CDLIS security.

### **Headquarters Move: The Department Needs To Thoroughly Test Its Consolidated IT Infrastructure for Adequate Security Before Moving Critical Systems to Its New Headquarters**

Traditionally, each OA has managed its own IT infrastructure (desktop computers, local area networks, and e-mail) in the departmental Headquarters. These duplicative IT operations were expensive to maintain and had inconsistent security protections—both physical and logical.<sup>3</sup> Since they were interconnected, security weaknesses in one OA's infrastructure could endanger others: in other words, they are only as strong as the weakest link.

As part of the move to the new Headquarters, the Department seized the opportunity to consolidate these IT infrastructure operations into one. Because the consolidated IT infrastructure will support all OAs' operations, it will require a higher level of security protection than is presently the case and will therefore also need thorough testing. While this consolidated infrastructure can help strengthen departmentwide security protection and make IT operations more efficient, the current schedule and plan for implementation and testing are still evolving, due to a variety of move-related problems. If not properly secured, this consolidated infrastructure could result in much greater harm to the integrity of departmental system operations than would be the case if only one OA were affected. The Department must thoroughly test this new IT infrastructure before installing OA mission-critical systems in this new infrastructure.

---

<sup>3</sup> Logical security consists of software safeguards for an organization's systems, including user identification and password access, authentication, access rights, and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.

### ***Fragmented Systems Backup and Recovery Sites Need To Be Eliminated***

As part of this IT consolidation, the Department should also identify a systems backup/recovery site at a sufficient geographic distance from the new Headquarters and conduct systems contingency testing after completing the Headquarters move. Further, the CIO needs to direct OAs not to make additional investments to equip their individual system backup/recovery sites until decisions have been made for the consolidated recovery site.

OAs have been responsible for establishing their individual backup/recovery sites because they had separate IT infrastructures. In FY 2003, we reported inadequate contingency planning and testing at OA recovery sites. In addition, we stated that to reduce the probability of losing both primary and backup sites to the same disaster, the Department needed to develop guidance on the minimum allowable geographic distance between a system's primary and recovery processing sites. Some OAs' recovery sites are within 10, 15, or 25 miles of primary sites. In case of an emergency, those OAs would likely lose both the primary and backup computers for their mission-critical systems, such as safety inspection and grants management systems, since natural disasters often cover areas as large as 25 miles or more. Such sites should be replaced by the consolidated backup/recovery site.

In FY 2005 we reported that over 50 percent of the systems in the sample lacked contingency plans and over 80 percent of the plans were not tested and continued to have recovery site locations that were too close. This year, 9 of the 14 systems did not have contingency plans; in addition, 11 of the 14 systems did not provide documented evidence that a contingency plan had been tested, and the problem with recovery site proximity continues. Overall, about 60 percent lacked contingency plans and about 75 percent lacked plan testing within the previous year, as required by OMB. The Department needs to enhance systems contingency planning through this IT consolidation effort.

### **Network Security: The Department Needs To Ensure That Operating Administrations' Systems Are Configured According to Security Standards**

To meet FISMA requirements for a minimally acceptable system configuration, DOT published additional baseline configuration standards for various commercial off-the-self software products in FY 2006. The issuance of these additional guidelines has provided DOT with greater capability to configure all of its software products based on standardized security benchmarks. Yet obtaining the data with which to ensure compliance with these standards has proved elusive.

During FY 2006, as an initial effort, DOT identified 117 systems from its inventory of 426 to be tested for compliance with its baseline configuration standards. Accordingly, in April 2006, the Department issued a policy requiring these systems to be completely checked and validated by OAs. In August 2006, the departmental CIO reminded all OAs' CIOs to complete their compliance checks and report the testing results by early September 2006. Only 9 of the 12 OAs responded to the Department's request for information regarding their implementation of DOT configuration standards, and they were responsible for only 36 of the 117 systems (see Table 2).

**Table 2. Operating Administrations' Responses to CIO Request for Information on Implementation of DOT Security Configuration Standards**

Operating Administration (OA)*		Number of systems OAs are responsible for (compliance review)	Subtotal
OA Did Not Respond	FAA	77	
	MARAD	3	
	SLSDC	1	
			<b>81</b>
OA Responded	FHWA	6	
	FMCSA	2	
	FRA	3	
	FTA	3	
	NHTSA	12	
	OST	3	
	PHMSA	3	
	RITA	2	
	STB	2	
		<b>36</b>	
<b>Total for all OAs</b>			<b>117</b>

\*See Exhibit C for a list of OA acronyms.

In addition, the OAs' responses presented a big challenge for the CIO to effectively validate the actual implementation of DOT's configuration standards. Specifically, the OAs' responses

- came in a variety of formats, including spreadsheets, vulnerability scanning results, automatically generated scoring reports, and manual checklists;
- did not include the evidence requested, such as computer screen shots showing actual settings on a tested system; and

- contained data on systems that were not selected for the compliance review.

As a result, the CIO was not able to effectively determine how many of the 117 systems selected for compliance review were actually tested and to what extent they were in compliance with DOT baseline configuration standards. This happened because DOT has not established a consistent method or set of criteria to be used when validating the actual configuration implementation of its systems. We closely worked with the CIO's office to determine the percentage of DOT systems meeting security configuration standards based on these submissions for this year's OMB reporting.

Our contractors also identified deficiencies in the commercial software products used in DOT financial systems, such as vulnerabilities on the computer servers. Those servers were running Windows operating systems and did not meet DOT's Windows security baseline configuration standards.

The Department needs to enforce its configuration standards. Specifically, DOT needs to establish a consistent method to be used when validating the actual configuration implementation of its systems.

### **Management Controls: The Department Needs To Work With Operating Administrations To Strengthen Oversight of IT Investments and Streamline Duplicative IT Systems**

Last year, we expressed concern over the departmental IRB's ability to provide value-added services when reviewing FAA's major IT investment projects. As a result, we recommended that the Department clarify the Board's authority and increase the Board's capability to research potential project cost, schedule, and performance shortfalls on complex IT investments. Subsequently, the Department confirmed that the Board, through advising the Secretary, can influence budget decisions on all IT investments. During FY 2006, using this authority, the Board enhanced project management of a multibillion-dollar investment project called FAA Telecommunications Infrastructure.

In terms of identifying problems associated with major IT investments, the Department plans to delegate more responsibilities to individual OA review boards to oversee their specific IT investments. While we support the idea of holding OAs more accountable for their own projects, this will not be possible until the departmental IRB establishes clear performance measures, such as earned value management measures for IT investments (see following section). Currently, 13 departmental IT investment projects are included in OMB's high-risk list, which account for about \$24 billion in life-cycle costs. Twelve of these high-risk projects are related to air traffic control modernization, which has been on the

Government Accountability Office's high-risk list for more than 10 years. The departmental IRB needs to work with OA review boards to continue exercising knowledgeable oversight of these major IT investments.

### ***Earned Value Management System Needs To Be Utilized To Better Monitor IT Investments***

As a fundamental requirement of acquisition or modification of major systems, the earned value management system offers management important insights into progress. Full implementation of the EVM system on IT programs would ensure that management receives information providing accurate cost and schedule performance data essential for planning and making effective IT business decisions. In addition, recognizing the importance of EVMS, OMB issued a memorandum last year, which listed 32 criteria that agencies should meet when implementing EVMS to monitor their major IT investments.<sup>4</sup>

However, an effective EVMS practice has not yet been implemented at DOT. For example:

- Seventy-one percent (15 out of 21) of major FAA IT investments met fewer than half of the OMB criteria.
- Seventy percent (7 out of 10) of other major DOT IT investments met fewer than half of the OMB criteria.

According to the CIO, during FY 2006 his office was not able to develop a plan for improvement, given the loss of key personnel and the fact that they have not been able to identify qualified staff with extensive EVM knowledge. As a result, the EVM data generated and reported to the CIO by the OAs do not go through an assessment of integrity or accuracy. However, these EVM data are still provided to DOT management, which uses this information to better understand the progress on approved IT investments and to make investment decisions. In addition, the CIO continues to use these EVM data for mandatory reporting to OMB. OMB placed seven major DOT investments—FAA (6) and Departmentwide (1)—on the high-risk list because of the questionable EVM data reported. These projects account for about \$720 million in DOT's FY 2006 IT budget, and \$16 billion in life-cycle cost estimates. Enhancing the use of EVMS to monitor major IT investment projects requires committed management attention.

---

<sup>4</sup> *Improving Information Technology (IT) Project Planning and Execution*, M-05-23, August 4, 2005.

### ***Efforts To Streamline Duplicative Systems for Cost Savings Need To Continue***

Another area requiring senior management attention is continuing to streamline duplicative common systems for cost savings. In FY 2003, the Department identified opportunities to consolidate duplicative systems used in 11 common business areas across OAs, such as office IT infrastructure, financial management, grants management, and training. During FY 2006, the Department completed its consolidation of recruitment systems and will complete consolidation of IT infrastructures at the new Headquarters in FY 2007. Progress has also been made in eliminating duplicative financial systems and teaming with the Department of Housing and Urban Development to streamline grants management systems. The Department needs to continue to actively pursue streamlining these duplicative systems to realize the cost savings that consolidation can offer (see Table 3).

***Table 3. Status of Enterprise Initiatives  
as of September 15, 2006***

<b>Initiative</b>	<b>Number of current systems</b>	<b>Amount of life-cycle budget (in millions of dollars)</b>
Financial Management/Travel Systems	26	\$725
Grants Management	5	8
Recruitment	2	26
Internal Rulemaking Tracking	3	1
Procurement Management	9	26
Enterprise Document Management	N/A	45
Training	16	50
ACE/ITDS (Automated Commercial Environment/International Trade Data System)	N/A	2
Intermodal Hazmat Data Sharing	N/A	14
Enterprise Architecture	11	39
IT Consolidation	61	1,309
<b>Total</b>		<b>\$2,245</b>

N/A: information not available.

## **RECOMMENDATIONS**

In order to strengthen the Department's information security program, we recommend that the Department's Chief Information Officer:

### **Enhance critical infrastructure protection by:**

1. Evaluating the adequacy of the corrective action plans submitted by FAA for reviewing operational air traffic control system security and developing contingency plans for prolonged service disruptions, to ensure accountability.
2. Conducting quarterly assessment review meetings with FAA to measure progress made against the approved plans.

### **Enhance computer systems security reviews by:**

3. Ensuring that recertifications of DOT information systems are prioritized and needed security upgrades identified. OAs must report progress measured against a pre-approved schedule throughout the year, including but not limited to budget and staffing levels for FY 2007.
4. Developing, implementing, and enforcing a policy clarifying to OAs how to correctly determine overall systems risk-impact levels.
5. Issuing a memorandum of understanding delineating systems security roles and responsibilities for national databases such as CDLIS and NDR, to ensure that they are correctly assessed for risk and appropriately secured.

### **Enhance the security protection associated with the Headquarters move by:**

6. Testing the new building's infrastructure before installing OAs' mission-critical systems on the infrastructure.
7. Establishing system backup and recovery sites for the consolidated IT infrastructure and all applications systems operating on it, committing to a specific date for conducting systems recovery testing after completing the Headquarters move, and directing OAs to eliminate their individual system backup/recovery sites.

### **Enhance systems contingency planning and testing by:**

8. Developing and testing contingency plans for information systems that lack such plans.



**Enhance DOT network security by:**

9. Developing a standard methodology to collect information from OAs to validate that commercial software products used in their information systems are configured in accordance with security standards.
10. Conducting a validation review and following up with OAs on a quarterly basis throughout the year.

**Enhance IT investment management controls by:**

11. (a) Working with OAs to develop performance measures on their IT investment projects to ensure effective oversight by OAs' investment review boards.  
  
(b) Requiring OAs to report the review results to the departmental IRB.
12. (a) Working with FAA to ensure proper implementation of earned value management to oversee all high-risk projects.  
  
(b) Working with other OAs to measure their implementation of earned value management based on OMB criteria.
13. Developing a plan to continue streamlining duplicative common systems in identified areas after completing the Headquarters move.

**MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR  
GENERAL RESPONSE**

The CIO Office reviewed a draft of this report and provided oral comments. CIO officials concurred 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) 366-6767; Theodore P. Alves, Acting Deputy Inspector General, at (202) 366-1992; or Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1496.

#

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

# EXHIBIT A. OIG INPUT TO FISMA REPORT

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

Agency Name:

### 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 over the past fiscal year 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					
Bureau Name	FIPS 199 Risk Impact Level	a. Agency Systems		b. Contractor Systems		c. 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	
		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	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>252</b>	<b>6</b>	<b>11</b>	<b>1</b>	<b>263</b>	<b>7</b>	<b>7</b>	<b>100.0%</b>	<b>3</b>	<b>42.9%</b>	<b>2</b>	<b>28.6%</b>
FHWA	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>22</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>23</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
FMCSA	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>22</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>22</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
FRA	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>22</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>22</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
FTA	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>5</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>6</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
MARAD	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>12</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>12</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
NHTSA	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>15</b>	<b>0</b>	<b>3</b>	<b>0</b>	<b>18</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
OST	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>43</b>	<b>3</b>	<b>0</b>	<b>0</b>	<b>43</b>	<b>3</b>	<b>3</b>	<b>100.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
PHMSA	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>5</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>5</b>	<b>1</b>	<b>1</b>	<b>100.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
RITA	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>9</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>9</b>	<b>2</b>	<b>2</b>	<b>100.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
SLSDC	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
STB	High	0	0	0	0	0	0						
	Moderate	0	0	0	0	0	0						
	Low	0	0	0	0	0	0						
	<b>Sub-total</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>0</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>	<b>0</b>	<b>0.0%</b>
Agency	High	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
Totals	Moderate	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Low	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
	<b>Total</b>	<b>410</b>	<b>12</b>	<b>16</b>	<b>1</b>	<b>426</b>	<b>13</b>	<b>13</b>	<b>100.0%</b>	<b>3</b>	<b>23.1%</b>	<b>2</b>	<b>15.4%</b>

### Question 3

In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

<b>3.a.</b>	<p>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 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Rarely, for example, approximately 0-50% of the time</li> <li>- Sometimes, for example, approximately 51-70% of the time</li> <li>- Frequently, for example, approximately 71-80% of the time</li> <li>- Mostly, for example, approximately 81-95% of the time</li> <li>- Almost Always, for example, approximately 96-100% of the time</li> </ul>	<p>- Almost Always, for example, approximately 96-100% of the time</p>
<b>3.b.1.</b>	<p>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 other systems or networks, including those not operated by or under the control of the agency.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> <li>- Approximately 0-50% complete</li> <li>- Approximately 51-70% complete</li> <li>- Approximately 71-80% complete</li> <li>- Approximately 81-95% complete</li> <li>- Approximately 96-100% complete</li> </ul>	<p>- Approximately 96-100% complete</p>
<b>3.b.2.</b>	<p>If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.</p>	<p>N/A</p>
<b>3.c.</b>	<p>The OIG <b>generally</b> agrees with the CIO on the number of agency owned systems.</p>	<p>Yes</p>
<b>3.d.</b>	<p>The OIG <b>generally</b> 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.</p>	<p>Yes</p>
<b>3.e.</b>	<p>The agency inventory is maintained and updated at least annually.</p>	<p>Yes</p>
<b>3.f.</b>	<p>The agency has completed system e-authentication risk assessments.</p>	<p>Yes</p>

## 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.

For items 4a.-4.f, the response categories are as follows:

- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

<b>4.a.</b>	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
<b>4.b.</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).	- Mostly, for example, approximately 81-95% of the time
<b>4.c.</b>	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
<b>4.d.</b>	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
<b>4.e.</b>	OIG findings are incorporated into the POA&M process.	- Almost Always, for example, approximately 96-100% of the time
<b>4.f.</b>	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Mostly, for example, approximately 81-95% of the time

## 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. This 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.

Response Categories:

- Excellent
- Good
- Satisfactory
- Poor
- Failing

- Good

**Comments:** We found that critical infrastructure systems used to direct air traffic control and track shipments of hazardous materials were reported as having a moderate risk impact which is inconsistent with OMB's suggestions and the upcoming departmental policy on security categorization. Due to this concern, we decided not to report how many high, moderate, and low risk-impact systems the Department has in question 1.

## Question 6

<b>6.a.</b>	Is there an agency wide security configuration policy?	Yes	
Comments:			
<b>6.b.</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.		
<b>Product</b>	<b>Addressed in agency-wide policy?</b>  Yes, No, or N/A	<b>Do any agency systems run this software?</b>  Yes or No.	<p><b>Approximate the extent of implementation of the security configuration policy on the systems running the software.</b></p> <p><b>Response choices include:</b></p> <ul style="list-style-type: none"> <li>- Rarely, or, on approximately 0-50% of the systems running this software</li> <li>- Sometimes, or on approximately 51-70% of the systems running this software</li> <li>- Frequently, or on approximately 71-80% of the systems running this software</li> <li>- Mostly, or on approximately 81-95% of the systems running this software</li> <li>- Almost Always, or on approximately 96-100% of the systems running this software</li> </ul>
Windows XP Professional	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows NT	Yes	No	
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	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Solaris	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
HP-UX	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Linux	Yes	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Cisco Router IOS	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Oracle	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Other: Wireless/PDA and SQL	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
<p>Comments: During FY 2006, DOT published additional baseline configuration standards for software products. In addition, DOT's Office of Chief Information Officer (OCIO) identified 117 DOT systems to be tested for compliance with its baseline configuration standards, and required OAs to complete the compliance checks and report the testing results by early September 2006. Nine OAs that were responsible for 36 of 117 systems submitted their test results. Our review was based on this submission. However, we found deficiencies in this submission that are detailed in our audit report.</p>			

### 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.

<b>7.a.</b>	The agency follows documented policies and procedures for identifying and reporting incidents internally.	Yes
<b>7.b.</b>	The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Yes
<b>7.c.</b>	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). <a href="http://www.us-cert.gov">http://www.us-cert.gov</a>	Yes

Comments: In FY 2006, DOT TCIRC has reported over 500 security incidents to US-CERT and was praised as a diligent and responsive federal agency in reporting incidents.

### Question 8

<b>8</b>	<p>Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?</p> <p>Response Choices include:</p> <ul style="list-style-type: none"> <li>- Rarely, or, approximately 0-50% of employees have sufficient training</li> <li>- Sometimes, or approximately 51-70% of employees have sufficient training</li> <li>- Frequently, or approximately 71-80% of employees have sufficient training</li> <li>- Mostly, or approximately 81-95% of employees have sufficient training</li> <li>- Almost Always, or approximately 96-100% of employees have sufficient training</li> </ul>	<ul style="list-style-type: none"> <li>- Mostly, or approximately 81-95% of employees have sufficient training</li> </ul>
----------	--	---

### Question 9

<b>9</b>	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	Yes
----------	---	-----



## **EXHIBIT B. SCOPE AND METHODOLOGY**

During FY 2006, we fulfilled the requirements of FISMA by reviewing the progress made in securing FAA's air traffic control systems, the unique challenge in recertifying 50 percent of the DOT systems' security, the security of the consolidated IT infrastructure, the validation that OAs systems are configured according to security standards, and the implementation of IT capital planning and investment control procedures. In addition, we sampled 14 systems that had undergone system security 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 and contributed to DOT's FISMA report by rating DOT progress in areas specified by OMB.

We used the audit methodologies recommended by the Government Accountability Office and guidelines issued by other Government authorities such as NIST. We also used commercial scanning software to assess network vulnerabilities.

We performed our information security review work throughout FY 2006, focusing on FISMA evaluation between July and September 2006 at DOT and OA Headquarters offices in the Washington, DC, metropolitan area. 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, waste, and abuse.

Previous audit reports on DOT's information security program issued in response to the FISMA legislative mandate (formerly the Government Information Security Reform Act [GISRA]) include:

*DOT Information Security Program*, FI-2006-002, October 7, 2005;  
*DOT Information Security Program*, FI-2005-001, October 1, 2004;  
*DOT Information Security Program*, FI-2003-086, September 25, 2003;  
*DOT Information Security Program*, FI-2002-115, September 27, 2002; and  
*DOT Information Security Program*, FI-2001-090, September 7, 2001.

## EXHIBIT C. DOT OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

Operating Administration	Acronym	FY 2005	FY 2006
Federal Aviation Administration	FAA	271	263
Federal Highway Administration	FHWA	24	23
Federal Motor Carrier Safety Administration	FMCSA	19	22
Federal Railroad Administration	FRA	21	22
Federal Transit Administration	FTA	9	6
Maritime Administration	MARAD	13	12
National Highway Traffic Safety Administration	NHTSA	18	18
Office of the Secretary	OST	52	43
Pipeline and Hazardous Materials Safety Administration	PHMSA	4	5
Research and Innovative Technology Administration	RITA	17	9
Saint Lawrence Seaway Development Corporation	SLSDC	1	1
Surface Transportation Board	STB	2	2
<b>Total Systems</b>		<b>451</b>	<b>426</b>

## EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

<b>Name</b>	<b>Title</b>
Ed Densmore	Program Director
Nathan Custer	Project Manager
Dr. Ping Z. Sun	Project Manager
Michael Marshlick	Computer Science Adviser
Michael P. Fruitman	Communications Adviser
Victoria La Rock	Senior Auditor
Jim Mallow	Senior Auditor
Lynn Dowds	Senior Auditor
Tim Roberts	Senior Auditor
Mitchell Balakit	Information Technology Specialist
Aaron Nguyen	Computer Scientist
Narja Hylton	Auditor
Christopher Cullerot	Information Technology Specialist
Vasily Gerasimov	Information Technology Specialist
Martha Morrobel	Information Technology Specialist
Ann Moles	Information Technology Specialist