INFORMATION SECURITY PROGRAM

Department of Transportation

Report Number: FI–2008–001
Date Issued: October 10, 2007

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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-2008-001

Date: October 10, 2007

From: Calvin L. Scovel III
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. In accordance with the Federal Information Security Management Act of 2002 (FISMA), our objective was to determine the effectiveness of the Department's information security program, especially in the areas of (1) meeting the minimum Government security standards to protect sensitive information systems and data, (2) establishing a secure network operating environment at the Department's new Headquarters building and other key locations, (3) correcting security weaknesses identified previously in the air traffic control system, and (4) implementing earned value management to better monitor major information technology (IT) investment projects.

We are also contributing to the annual departmental FISMA report by answering questions specified by the Office of Management and Budget (OMB). This is included as Exhibit A. Similar to last year, we tested a representative subset of departmental systems, including contractor-operated and/or -maintained systems that had undergone systems security certification reviews, in order to determine whether the Department 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. 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, disclosure of, disruption to, or modification of information collected or maintained by or on behalf of an agency. The Department 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) 2007, the departmental IT budget totaled about $2.6 billion.

The Department has 13 Operating Administrations. During FY 2007, all Operating Administrations except the Federal Aviation Administration (FAA), the Federal Railroad Administration (FRA),[1] and the Surface Transportation Board were relocated to the new Headquarters. As part of the Headquarters relocation, the Department consolidated individual Operating Administrations' network infrastructures (e-mail, desktop computing, and local area networks) into a common IT infrastructure—one of the IT consolidation target projects identified by the Department in FY 2003.[2]

For FY 2007, the Department is reporting a total of 429 computer systems—3 more than last year, of which 60 percent are FAA systems. Among the systems the Department maintains and operates is the air traffic control system, which the President has designated part of the critical national infrastructure. Other systems owned by the Department include safety-sensitive surface transportation systems and financial systems that are used to manage and disburse over $50 billion in Federal funds each year. Systems inventory counts for FY 2006 and FY 2007 for each Operating Administration are detailed in Exhibit C.

RESULTS IN BRIEF

FY 2007 was a particularly challenging year for the Department in managing its IT resources. In addition to establishing a common IT infrastructure for the new Headquarters, it had to review, test, and certify security protection in more than half of its information systems to meet the recertification requirement.

While the Department has completed most of the scheduled security recertification reviews, the overall effectiveness of its information security program declined this year because management had to divert resources and attention to resolving

---

[1] FRA will be relocated in early FY 2008.

[2] The initial network consolidation was limited to Headquarters operations. Operating Administrations are still responsible for supporting network operations to their field offices. The Federal Highway Administration is leading a task force to evaluate consolidation of field network infrastructure.

Headquarters move-related issues.[3] Specifically, management did not meet Government security standards to protect information systems and did not take sufficient action to correct identified security deficiencies. We also found that commercial software products used in departmental systems were not configured in accordance with security standards and security incidents were incompletely and/or inaccurately reported.

In terms of correcting the two security weaknesses identified previously in the air traffic control system—contingency planning and review of operational air traffic control systems security—FAA demonstrated renewed initiative in undertaking multiyear correction efforts starting in FY 2007. FAA also made modest progress in enhancing the implementation of earned value management for major IT investment projects. Nonetheless, challenges remain in both areas.

These issues are summarized below and detailed in the Findings section, beginning on page 8.

Failure to Meet Government Security Standards to Protect Information Systems. According to the National Institute of Standards and Technology (NIST), risk categorization is key in determining the level of security protection needed for individual systems. Systems categorized as having a high-risk impact on the agency's mission are required to meet a more stringent security standard than moderate- or low-risk-impact systems. These security standards (referred to as minimum security requirements) became mandatory for Federal agencies in March 2007.

Last year we reported a concern in the Department's risk categorization. Specifically, FAA categorized all air traffic control systems as having a moderate-risk impact. We also reported that departmental systems would likely require security upgrades to meet the minimum security standards in FY 2007. We continue to find deficiencies in risk categorization and insufficient implementation of minimum security protection.

- *Risk Categorization*. NIST guidance emphasizes the importance of performing risk categorization on an entitywide basis versus at the individual bureau level. During FY 2007, the departmental Chief Information Officer (CIO) issued a draft policy requiring high-risk-impact categorization of systems used to support the Nation's critical infrastructure. However, the policy has resulted in little change at FAA. Among about 100 systems used to direct air traffic control operations—surveillance, navigation, landing, communications, weather, and flight plan processing—none were reported as having a high-risk impact. Instead, the 19 systems reported by FAA as high-risk impact are primarily for administrative functions, such as the procurement system and

[3] During FY 2007, no significant service disruptions to departmental systems were reported.

local-area-network systems. Although FAA claims that air traffic control systems are properly protected, it has no assurance that minimum security standards are being met in protecting these systems in accordance with NIST standards and departmental directives for system categorization and testing of the appropriate security controls. After this issue was brought to management's attention, the departmental CIO, the FAA Acting Deputy Administrator, and the FAA CIO all agreed to collaborate with Air Traffic Organization business owners to ensure that air traffic control systems are individually reviewed and categorized in accordance with NIST standards and DOT policy, as a key priority for FY 2008.

- *Minimum Security Protection*. Agencies are required to implement different levels of security protection for individual systems based on risk categorization. Our review of 21 sample systems from the departmental inventory revealed that 11 systems from 7 Operating Administrations did not meet the minimum security requirements for the risk category assigned to them. For example, there were instances in which records containing sensitive personally identifiable information are transmitted on the network in clear text. The minimum security standards require such information to be encrypted during transmission.

- *Certification Review of the New IT Infrastructure*. Another challenge facing the Department is that it has not completed the security certification review of the common IT infrastructure at the new Headquarters, which is used to support more than 80 application systems, such as grants management systems, safety inspection systems, and various administrative systems. This happened because the Department experienced complications with the electrical power supply in the new Headquarters and had to move the application systems to a commercial vendor site before it could complete reviewing, testing, and accrediting the expanded common IT environment. Until the planned review of the common infrastructure is completed, management cannot provide security assurance for the 80-plus application systems because the common IT infrastructure, if not properly secured, could cause security risks to all systems operating on the infrastructure.[4] The Department needs to retest systems security in these application systems after certifying the expanded IT infrastructure as adequately secure.

Insufficient Action to Correct Identified Security Deficiencies. Security deficiencies identified during security certification reviews are tracked and prioritized for correction through a process called Plan of Action and Milestones (POA&M). Last year we reported that management had improved this process significantly to ensure that correction items were prioritized and completed in a

[4] The Department plans to complete testing of the expanded common IT environment for security accreditation in the near future.

timely manner. This year, we found that management did not exercise the same amount of attention to correct identified security deficiencies. Most Operating Administrations still do not have a formalized process to guide this effort. In addition, the CIO has not yet finalized the departmental POA&M Handbook to manage the identified weaknesses during the life cycle.

We found that 30 percent of planned corrections (901 out of a total of about 3,000 identified security deficiencies) are overdue for more than 6 months past their scheduled completion dates. We also found cost estimates to fix 60 percent of the approximately 3,000 identified security deficiencies missing. Details of Operating Administrations responsible for delayed corrections and missing cost estimates are on page 12. This is a clear reversal of the improvement we witnessed last year.

Without reliable cost estimates, management cannot make informed decisions to prioritize use of limited resources. This may have resulted in delays in and cancellation of planned correction efforts. For example:

- Cost estimates were missing from 91 percent of overdue correction items, including 3 critical deficiencies, such as ineffective password protection to limit user access.

- Cost estimates were also missing from 98 percent of canceled correction items, including 2 critical deficiencies. Cancelled items are security deficiencies for which management accepted the risk of not making corrections. For example, management decided to accept the risk of not having proper password controls for system administrators for a system used by FAA to manage air traffic control flow.

Continuous Deficiencies in Network Computers' Configuration. To reduce the risk of hostile attack based on known vulnerabilities in commercial off-the-shelf software, such as the Windows operating systems and Oracle database systems, agencies are required to configure such commercial software in accordance with NIST or agency security standards. Last year we reported that Operating Administrations' submissions to the CIO office to support their compliance with configuration standards were incomplete and inconclusive. As a result, the Department had no assurance that the commercial software was properly configured to reduce the risk of being attacked. We found little progress made in this area during FY 2007, and departmental network computers remain vulnerable to possible attacks due to improper configuration.

In addition, with the new common IT infrastructure, the Department faces a new security challenge. The new infrastructure has significantly expanded its ability to have secure connections on the Internet by using virtual private network (VPN) access. This has positioned the Department well to support the telecommuting

initiative and continuity of business operations. However, when employees connect their home computers to departmental networks, they create security exposure because their home computers may not be properly secured.[5] Management should explore more secured alternatives to support telecommuting.

Incomplete and Inaccurate Reporting of Security Incidents. During FY 2007, FAA did not report 40[6] cyber security incidents to the Department and, in turn, to the central Government authority, the United States Computer Emergency Readiness Team (US–CERT). Most of these incidents involved viruses in FAA computers. This happened partially because of inconsistent reporting practices within FAA. Employing a consistent reporting practice in line with established departmental policies and procedures should be a prerequisite for FAA to provide incident monitoring and reporting services to other Operating Administrations—a new initiative starting in FY 2008. This initiative was recently approved by the Department in preparation for FAA to become a shared service provider to other Government agencies for cyber incidence monitoring and reporting.

To better prepare it to become a shared service provider, FAA also needs to enhance its performance measurement reporting to senior management on security incidents. We noticed inaccurate reporting in last year's FAA Performance and Accountability Report. During FY 2006, FAA had to shut down a portion of air traffic control systems because of security events. While FAA did a commendable job in cleaning up the infected computers and enhancing the underlying configuration management controls, it nonetheless reported to the Secretary, OMB, and the Congress in its annual Performance and Accountability Report that "no successful cyber events that significantly disabled or degraded our service" had taken place.

Renewed Initiatives in Correcting Air Traffic Control System Security Weaknesses. The President has designated air traffic control systems as part of the Nation's critical 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, we reported deficiencies in protecting this critical infrastructure in two areas: (1) continuity planning to restore essential air service in case of prolonged service disruptions at en route centers and (2) review of operational air traffic control systems security outside of the computer laboratory. Last year, we reported inadequate progress in both areas. FAA senior management pledged aggressive action.

---

[5] Security concerns on telework have been raised recently among other Federal agencies. For example, the Department of Justice has decided to ban the use of home computers for telework.

[6] FAA claimed that 31 of these 40 incidents were either repeated or duplicated incidents that should have been previously reported to the Department. However, FAA was not able to provide any evidence that the original incidents had been reported. In addition, FAA indicated that two incidents were false-positives and therefore did not need to be reported, even though they were not recorded as false-positives in FAA's official log.

During FY 2007, under the Deputy Administrator's (now Acting Administrator) direction, FAA undertook renewed initiatives and made modest progress in both areas, such as developing a concept of operations for business continuity planning and a methodology to select high-risk operational air traffic control systems for security review. However, these are multiyear efforts, for which FAA still faces many uncertainties. Due to the sensitivity of air traffic control systems, we will issue a separate report detailing the progress and potential challenges associated with these corrective actions along with recommendations.

Modest Progress in Implementation of Earned Value Management. During FY 2007, the Department revised its Investment Review Board's charter by delegating more responsibilities to individual OA review boards to oversee their specific IT investments. Regardless of the change in governance responsibility, establishing clear measurement benchmarks to evaluate major investment projects such as earned value management (EVM) is key to success. Last year we found that only 23 percent of major departmental IT investment projects met at least half of OMB's criteria for EVM implementation. During FY 2007, 35 percent of all major departmental IT investment projects met at least half of OMB's criteria for EVM implementation, a modest increase from last year. Continued enhancements in EVM implementation to ensure fiscal discipline with major investment projects is especially critical in today's tight economic environment.

We are making a series of recommendations, beginning on page 23, to help the Department continue to strengthen its information security program and better oversee major IT investments. In summary, we are recommending that the Chief Information Officer:

- Enhance the protection of information systems by ensuring that Operating Administrations comply with new Government security standards when completing their certification and accreditation reviews,
- Enhance correction of identified security deficiencies by working with Operating Administrations to develop measures of accountability that would hold Operating Administration officials responsible for timely correction of security weaknesses,
- Enhance network security by establishing a methodology, including use of automated tools, to verify that commercial software products are configured in accordance with security standards, and evaluating alternatives to using home computers to support telework,
- Ensure accurate reporting of security incidents, and
- Enhance the Department's implementation of EVM by establishing goals for improvement.

A draft of this report was provided to the Department's Chief Information Officer on September 28, 2007. On October 4, we received the Department's Chief

Information Officer's response, which can be found in the appendix. The Chief Information Officer generally concurred with the report's findings and recommendations and will provide details in 30 days, describing the specific actions and milestones that will be taken to implement the recommendations.

FINDINGS

Government Security Standards to Protect Information Systems Were Not Met

In our FY 2006 FISMA report, we stated that the Department faced several challenges in implementing and monitoring security controls to meet Government standards. This year, we found continued deficiencies in risk categorization of sensitive systems and implementation of security upgrades required to meet Government standards. In addition, security recertification review of the expanded IT infrastructure at the new Headquarters has not been completed. As a result, management has no security assurance for the 80-plus application systems operating on this infrastructure.

Risk Categorization for Department's Sensitive Systems Has Not Been Accurately Assessed

Last year we reported that air traffic control systems, which are designated part of the national critical infrastructure, were found to be rated low and moderate in terms of risk categorization. This appeared to conflict with NIST standards, which used air traffic control systems as an example of high-risk impact systems in the Federal Government.

During FY 2007, the CIO office issued a draft policy requiring high-risk-impact categorization of systems used to support the Nation's critical infrastructure. However, the policy has resulted in little change at FAA. In our review this year, of the nearly 100 FAA air traffic control systems, none had an overall security categorization of high. FAA did have 19 systems rated high, most of which were for administrative purposes, such as the procurement system and several local area networks. Although FAA claims that air traffic control systems are properly protected, it has no assurance that minimum security standards are being met in protecting these systems in accordance with NIST standards and departmental directives for system categorization and testing of the appropriate security controls.

FAA management stated that if the whole air traffic control system were to be rated, it should be high, but each system is rated individually. Because of the redundancy in functionality among the systems, losing one system would not have a severe impact. However, security controls in NIST 800-53 require that

assessments be completed considering national impact, not just system-level or organization-level impact. If any air traffic control system that operates on a national level were to go down for any reason and have a negative impact, that system should be rated high. After this issue was brought to management's attention, the departmental CIO, the FAA Acting Deputy Administrator, and the FAA CIO all agreed to collaborate with Air Traffic Organization business owners to ensure that air traffic control systems are individually reviewed and categorized in accordance with NIST standards and DOT policy, as a key priority for FY 2008.

We also reviewed the categorization of systems that contain personally identifiable information. In FY 2006, we reported that 28 systems containing personally identifiable information were improperly rated for confidentiality, 18 were rated "low" and 10 were not rated. The departmental guidance states that all systems containing personally identifiable information must have a confidentially rating of at least "moderate."[7]

Operating Administrations have made progress during FY 2007 in upgrading their confidentiality system ratings; however, three Operating Administrations are still deficient in the rating of systems containing personally identifiable information. Of the 110 systems containing personally identifiable information that were reported to the CIO Privacy Office, 11 systems' confidentiality levels are improperly rated "low" (see Table 1).

Table 1. Confidentiality Rating of Systems Containing Personally Identifiable Information

Operating Administration[a]	Number of Systems with Personally Identifiable Information	Number of Systems with a Confidentiality Rating of Low
FAA	47	1
FHWA	8	3
FMCSA	9	0
OST	23	7
RITA	4	0
Other Operating Administrations	19	0
Total	**110**	**11**

Data source: CIO Privacy Office Inventory of systems containing personally identifiable information as of 9/7/2007.
[a] See Exhibit C for full Operating Administration names.

Until the systems are rated properly according to departmental policy, the Department has limited assurance that the Operating Administrations are implementing and testing appropriate security controls to effectively protect personally identifiable information.

[7] DOT Information Technology and Information Assurance Policy Number 039: Information Technology: Mapping Information Systems to Risk Level Categories.

Minimum Security Standards Have Not Been Incorporated Departmentwide

Last year we reported that the Department needed to address stronger security requirements that would come into play in March 2007, when Federal Information Processing Standards (FIPS) 200[8] became effective. This standard specifies minimum security requirements for Federal information systems in 17 security-related areas. Federal agencies must meet the minimum security requirements through the use of security controls in accordance with NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.* The applicable security controls must be documented in the system security plan, based on the results of the security assessment or modification of security controls in the information systems.

This year, in our review of the 21 sample systems, 11 from 7 Operating Administrations did not provide support in their system security plans that their systems were compliant with the new minimum security standards (see Table 2).

Table 2. FIPS 200 Noncompliant Systems

Operating Administration[a]	Number of Systems Sampled	Number of Systems Not Compliant with New Minimum Security Standards
FAA	9	2
FHWA	2	2
FMCSA	1	1
MARAD	3	3
NHTSA	1	1
OST	4	1
PHMSA	1	1
Total	**21**	**11**

Data source: Sample Systems' Certification & Accreditation documents provided by system owners through 9/5/2007.
[a] See Exhibit C for full Operating Administration names.

These systems are not compliant with the new security standards and could pose serious security risks. For example, one Operating Administration system with millions of records containing personally identifiable information that are transmitted across the network in clear text has not had its security plan updated since before March 2006. Had this system's security plan been updated to comply with the new minimum security standards, these records would have to be encrypted before they were sent across the network. Operating Administration management stated that they were not aware of the requirements to upgrade system security to meet the Government standards prior to their scheduled system recertification reviews—some of which are not due until 2009. The CIO Office

[8] Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 9, 2006.

needs to provide clear direction to Operating Administrations to ensure timely compliance with Government security standards.

Certification Review of the New IT Infrastructure Is Not Complete

The Department has not completed the security certification review of the expanded common IT infrastructure at the new Headquarters. As one of the critical components of the common IT infrastructure, the campus area network (CAN) is a backbone network infrastructure that provides connectivity among departmental Headquarters computers, the Internet, data centers, and remote offices. Due to electric power complications at the new Headquarters, the CAN was extended to include a commercial vendor site in Maryland in FY 2007. Currently, this expanded common IT infrastructure hosts more than 80 Operating Administration application systems.

Last year we recommended that the Department test security in the new IT infrastructure before installing Operating Administration application systems.[9] As part of such testing, the Department conducted a security certification review for the CAN. However, the security certification review did not cover the segment of the network located at the commercial vendor site. This happened because the initial CAN security certification review was conducted in April 2007, prior to its extension to the commercial vendor site. Without completing security certification reviews for the CAN, the most critical component of the Department's IT infrastructure, the Department cannot be assured that it is providing an adequate level of security protection to its more than 80 systems operating on the infrastructure.[10]

According to the CIO office, it plans to complete a certification review of CAN, including its extension at the commercial vendor site, in the near future. If not properly secured, the common IT infrastructure could create security risks for all systems operating on the infrastructure. The Department needs to retest security in these application systems after certifying the expanded IT infrastructure as adequately secure. Because the Operating Administrations' system security certifications rely on security controls of the CAN, any delay in completing the common IT infrastructure's certification would impede Operating Administration systems' timely certification.

---

[9] OIG report "Audit of Information Security Program," Report Number FI-2007-002, October 23, 2006.

[10] This consolidated IT infrastructure is also included on OMB's Watch List due to security concerns not related to the CAN.

Insufficient Action Has Been Taken To Correct Identified Security Deficiencies

Remediation of system security weaknesses is a complex process involving analysis, corrective action planning, budgeting, assignment of resources, and post-closure verification. This process begins when security weaknesses identified during certification reviews of departmental systems are documented in the POA&M database by the Operating Administration that owns the system. The information that is included in the POA&M database is used by management to ensure effective oversight of the remediation process and to report the status of correcting security weaknesses.

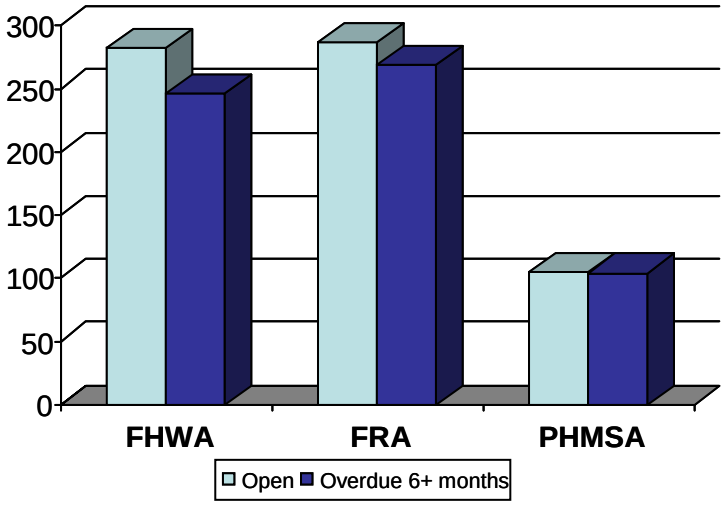
Last year we reported that the Department made noticeable improvement from the previous year in tracking, prioritizing, and correcting system security weaknesses. A review of the POA&M information this year found that 30 percent of corrections (901 out of about 3,000 identified security deficiencies) were overdue for more than 6 months past their scheduled completion dates. We also found cost estimates to fix 60 percent of the approximately 3,000 identified security deficiencies missing (see Table 3).

Table 3. POA&Ms & Cost Estimates

Operating Administration[a]	Number of Open POA&Ms	Number of POA&Ms with Cost Estimates Not Identified	Number of Overdue POA&Ms	Number of POA&Ms Overdue 6+ months past planned correction date
FAA	2102	942	365	266
FHWA[b]	282	282	250	246
FMCSA	36	27	0	0
FRA[b]	287	287	287	269
FTA	1	1	0	0
MARAD	4	4	0	0
NHTSA	5	5	0	0
OIG	7	2	3	1
OST	135	126	105	5
PHMSA[b]	105	105	105	104
RITA	27	27	27	10
SLSDC	0	0	0	0
STB	0	0	0	0
Total	**2991**	**1808**	**1142**	**901[c]**
Percent of Total	**100%**	**60%**	**38%**	**30%**

Data Source: Enterprise Security Portal data as of 9/5/2007.
[a] See Exhibit C for full Operating Administration names.
[b] These Operating Administrations have a high number of POA&Ms overdue 6+ months past their planned correction dates in relation to the total number of open POA&Ms.
[c] Of the corrections overdue for 6+ months, only 3 were categorized as high risk.

Figure 1. Operating Administrations With Highest Ratios of Overdue Corrections



FHWA, FRA, and PHMSA all had at least 90 percent of their corrections overdue for at least 6 months (see Figure 1). This is a clear reversal of the improvement we witnessed last year, when only 9 percent of corrections Departmentwide were overdue for more than 6 months.

Without reliable cost estimates, it is difficult for management to make an informed decision to prioritize use of limited resources. This may have resulted in delays in and cancellation of planned correction efforts. For the 1142 POA&Ms recorded as past due, 91 percent (1040 of 1142) lack cost estimates (see Table 4).

Table 4. Overdue POA&Ms

Risk Rating	Quantity	Number with Cost Not Identified	% Correction Cost Not Identified
High	3	3	100%
Medium	308	275	89%
Low	831	762	92%
Total	**1142**	**1040**	**91%**

Data Source: Enterprise Security Portal data as of 9/11/2007.

In addition, for the 380 items in which the risk of not correcting security deficiencies was accepted by management, as indicated in the POA&M database, 98 percent (374 of 380) lacked cost estimates (see Table 5). Management normally decides to cancel items in which identified security deficiencies are deemed not cost-beneficial to correct. Without adequate cost data, however, management lacks essential information needed to make informed cancellation decisions. Therefore, management may not have made proper decision in cancelling the 374 identified security deficiencies, including the 2 rated as high risk. For example, management decided to accept the risk of not having proper password controls for system administrators for a system used by FAA to manage air traffic control flow.

Table 5. Accepted Risk POA&Ms

Risk Rating	Quantity	Number with Cost Not Identified	% Correction Cost Not Identified
High	4	2	50%
Medium	26	26	100%
Low	350	346	99%
Total	**380**	**374**	**98%**

Data Source: Enterprise Security Portal data as of 9/11/2007.

Operating Administration management reported they do not have a formalized process to guide this effort such as data that should be required as input for each identified security weakness recorded in the database. In addition, the CIO has not yet finalized the departmental POA&M Handbook to manage the identified weaknesses during the life cycle, including required information needed as part of the record in the database. Without information such as cost data, management lacks data needed to make an informed decision for allocating resources needed to prioritize or accept risk for identified security weaknesses. As a result, the Department faces delays in scheduled correction, leaving departmental systems exposed to vulnerabilities that could be exploited.

Continuous Deficiencies Are Evident in Network Computers' Configuration

Both OMB and the Department require that the commercial off-the-shelf software incorporated in departmental computers, such as Windows operating systems and Oracle database systems, be configured in accordance with security configuration standards. Last year we reported that the Department had no assurance that the commercial software was properly configured to reduce the risk of being attacked. In FY 2007, little progress was made in this area, and departmental network computers remain vulnerable to attack due to improper configuration. Further, using employees' home computers to access departmental networks could present another security challenge because home computers may not be properly secured.

Departmental Systems Are Not Properly Configured in Compliance With Security Baseline Standards

Responding to our recommendations last year, the Department made some improvement in baseline security configuration implementation. For example, it started to use its management tracking system—Enterprise Security Portal (ESP)—to collect data from Operation Administrations about their implementation of departmental baseline configuration standards, explored an opportunity to deploy an automated tool that could enable the Department to verify its systems' compliance, and drafted new departmental Information Systems Security Baseline policy. However, deficiencies in this area remain. Based on the CIO Office's FISMA Weekly Scorecard from September 7, 2007, only 126 out of 429 systems have been reported by Operating Administrations to have met baseline configuration standards (see Table 6 and Figure 2).

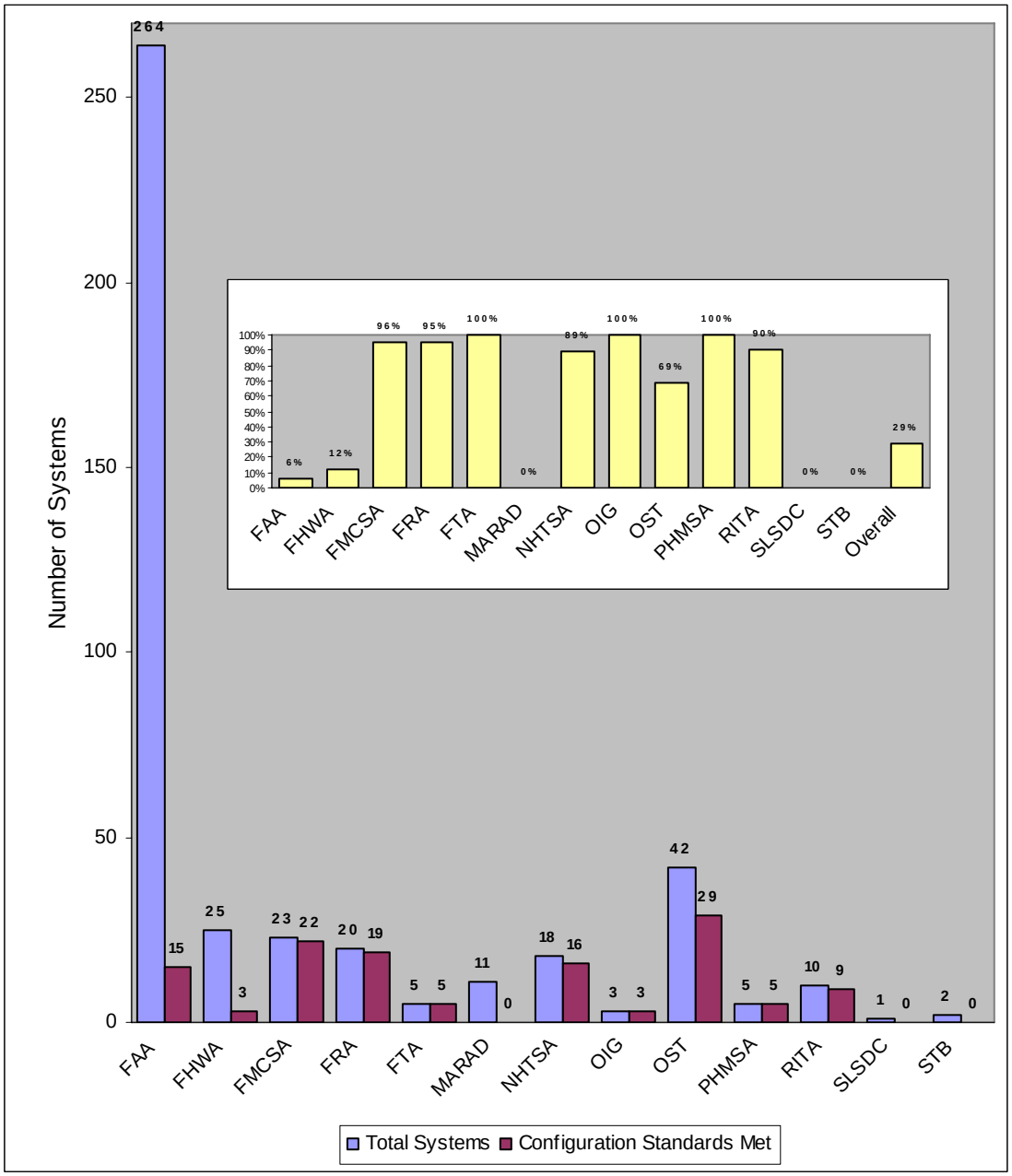
Table 6. Status of Departmental Systems Meeting Security Baseline Configuration Standards as Reported by Operating Administrations

Operating Administrations[a]	Total Number of Systems	Number of Systems Reported to Have Met Security Baseline Configuration
FAA	264	15
FHWA	25	3
FMCSA	23	22
FRA	20	19
FTA	5	5
MARAD	11	0
NHTSA	18	16
OIG	3	3
OST	42	29
PHMSA	5	5
RITA	10	9
SLSDC	1	0
STB	2	0
Total	**429**	**126**

Data Source: Department's CIO Office FISMA Weekly Scorecard, 9/7/2007.

[a] See Exhibit C for full Operating Administration names.

Figure 2. Operating Administrations' Total Systems and Percentages of Systems Reported as Having Met Baseline Security Configuration Standards



We also found that the CIO Office did not verify the accuracy of Operating Administrations' reporting. The CIO Office conducted two quarterly compliance reviews on 93 randomly selected departmental systems during FY 2007. The reviews required Operating Administrations to test the selected systems for baseline configuration compliance. Operating Administrations reported that only 52 systems have been through such a test and provided evidence of this testing. However, the CIO Office did not review the evidence provided by Operating Administrations for adequacy of compliance.

As a result, the Department has no assurance that Operating Administration computer systems have been adequately configured to ensure that effective security controls are in place. The inadequately configured systems increase security vulnerabilities, which could have an adverse impact on departmental operations.

Use of Employee Home Computers for Teleworking Could Create Security Exposure

The new IT infrastructure enables the Department to rapidly expand remote access such as VPN to support the Department's telework initiative and continuity of business operations. VPN allows departmental employees and contractors to access information hosted on departmental networks from home or remote locations. Currently, all Department user accounts are configured to have VPN access. However, when employees connect their home computers to departmental networks, it creates security exposure because their computers may not be properly secured. Meanwhile, the Department has no authority to regulate home computers, as indicated in the CIO's July 2007 testimony before the House Committee on Oversight and Government Reform.

While the Department has developed a policy for implementing secure remote access, including scanning the user's computer security profile prior to allowing access to the Department's network,[11] it has not been finalized. Currently, the Department has to rely on users to faithfully follow the user agreement such as employing appropriate virus-prevention tools that they agreed to when VPN privileges were granted. This procedural control, however, provides limited assurance because employees may not be fully aware how their home computers are configured or used by other family members. The Department of Justice recently banned the use of home computers for telework because of security concerns. If home computers that are not adequately secured are used to connect to the VPN, rather than departmental laptops, they could introduce viruses or malicious code to the Department's networks and even become entry points of unauthorized access to departmental systems. Management should finalize policy and continue to explore more secure alternatives to support telecommuting.

[11] DOT IT Assurance Policy 2006-23 (draft): Secure Remote Access Implementation and Management Policy.

Reporting of Security Incidents Has Been Incomplete and Inaccurate

The Department relies on two entities—the Transportation Cyber Incident Response Center (TCIRC) and FAA Computer Security Incident Response Center (CSIRC)—to promote information assurance by performing activities such as network monitoring, intrusion detection, incident handling, and reporting.

The Department requires that all cyber security incidents[12] be reported to TCIRC. It is then TCIRC's responsibility to report the security incidents to US–CERT. We found that CSIRC did not report all incidents to TCIRC. Based on FAA's internal incidents log, 616 security events were detected between October 2006 and June 2007. CSIRC categorized these events as 212 incidents and 404 findings. According to CSIRC, an incident is a *confirmed* cyber event, which should be reported, while a finding is a cyber event that is under investigation and should not be reported. However, we found that CSIRC did not report 40 incidents (about 20 percent) and, conversely, incorrectly reported 30 findings to TCIRC. FAA claimed that 31 of these 40 incidents were either repeated or duplicated incidents. However, FAA was not able to provide any evidence that the original incidents had been reported. In addition, FAA indicated that two incidents were false-positives and did not need to be reported, even though they were not recorded as false-positives in FAA's official log.

This inconsistent reporting happened partly because CSIRC did not have documented procedures for escalating findings to incidents once they were confirmed and then reporting these to TCIRC. In addition, communication breakdowns appear to be another contributing factor for incidents going unreported. For example, some incidents were detected during its weekend shift but were not relayed to the weekday shift for TCIRC reporting.

The majority of the unreported incidents involved virus infections of FAA computers. Because these incidents did not get reported to TCIRC, they were, in turn, left unreported to US–CERT. In order for proper coordination for defense against and response to cyber attacks Governmentwide, all incidents must be reported to the Department and US–CERT.

Recently, TCIRC's operation has been merged into FAA CSIRC as a consolidated unit known as the Cyber Security Management Center (CSMC). This merge initiative was approved by the Department in positioning FAA to become an

[12] An incident is defined as the act of violating an explicit or implied security policy. It includes but is not limited to attempts to gain unauthorized access to a system or its data, unwanted disruption or denial of service, or the unauthorized use of a system for the processing or storage of data.

information systems security shared service provider to offer cyber security services to other Government agencies. Starting in FY 2008, CSMC will provide incident monitoring and reporting services to other Operating Administrations. Employing a consistent reporting practice in line with established departmental policies and procedures should be a prerequisite for FAA to provide services to the Department, and eventually to other Government agencies, as a shared service provider for information system security.

To better prepare it to become a shared service provider, FAA also needs to enhance its performance measurement reporting to senior management on security incidents. During FY 2006, a cyber incident caused severe service degradation and forced FAA to shut down a portion of air traffic control systems because of a security incident. FAA thoroughly investigated the incident, identified the cause of the problem, and implemented countermeasures to prevent it from occurring again. Nonetheless, it inaccurately reported to the Secretary, OMB, and the Congress, in its Performance and Accountability Report, that "no successful cyber events that significantly disabled or degraded our service" had taken place.

FAA Took Renewed Initiatives in Correcting Air Traffic Control System Security Weaknesses

The President has designated FAA's air traffic control systems as part of the Nation's critical 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, we reported deficiencies in protecting this critical infrastructure in two areas: (1) continuity planning to restore essential air service in case of prolonged service disruptions at en route centers and (2) review of operational air traffic control systems security outside of the computer laboratory. Last year, we reported inadequate progress in both areas. FAA senior management pledged aggressive action.

FAA's renewed initiatives during 2007 were directly related to the leadership provided by the Deputy Administrator (now Acting Administrator) and demonstrated modest progress in developing a back-up continuity capability for restoring essential en route air traffic control services. However, FAA has encountered several challenges.

- *Measuring the loss of each en route center's impact on the National Airspace System.*[13] FAA's plan estimates restoration of 80 percent of any affected en route center's capabilities within 3 weeks at a designated recovery site; however, the impact that a disabled center will have on the National Airspace System as a whole has not been assessed. Since en route centers rely on

[13]The National Airspace System is an interconnected system of airports, air traffic facilities and equipment, navigational aids, and airways.

adjacent centers to efficiently manage air traffic, the loss of each center could cause a different ripple effect throughout the entire system. In order for FAA to better understand the overall impact, it will need to conduct an impact analysis on the effect that the loss of 20 percent of operational capability at each en route center would have on the entire system. Because the plan would shift functionality of the disabled center to the FAA recovery site located at its Technical Center in Atlantic City, NJ, the analysis should also determine the impact that an activated recovery plan will have on the Technical Center's core mission—developing and testing systems used to support air traffic control operations and aircraft safety.

- *Resolving continuity plan technical and resource concerns.* The success of the continuity plan hinges on FAA's ability to overcome logistical challenges. These challenges include rerouting voice communications and surveillance signals from the affected en route center to the recovery center, ensuring that the spare en route center at the Technical Center is properly staffed in the event it is activated, and coordinating with the appropriate labor unions for human resource management. Another resource concern involves its funding. FAA has budgeted $12 million for developing and implementing the continuity plan. However, this funding level was not based on sufficient analysis or cost estimates; rather, it was obtained by reallocating excess funds from current and ongoing FAA projects. FAA should complete a cost and schedule analysis to better determine the estimated costs and use these figures to secure additional funding commitments, if needed.

Regarding reviews of operational air traffic control systems security, FAA developed a methodology to select high-risk systems located in the field for testing. In fact, FAA went beyond our recommendation and applied this methodology to systems other than those used for air traffic control. However, FAA did not meet its commitment to us to complete its reviews of all TRACON and tower systems by the end of FY 2007.[14] Further, despite the improved site-selection methodology, FAA did not enhance its methodology to help identify software differences between the baseline systems at the Tech Center and the operational air traffic control systems in the field. This deficiency could weaken overall security protection because vulnerabilities could inadvertently be created when software changes are made to meet local (field site) operational needs, as evidenced in our previous audit reports. Due to the sensitivity of air traffic control systems, we will issue a separate report detailing progress, potential challenges, and recommendations.

[14] A Terminal Radar Approach Control facility (TRACON) is an Air Traffic Control Center usually located within the vicinity of a large airport that controls aircraft within 30-50 nautical miles of the airport between the surface and 10,000 feet. Towers are located on the airport and control landing and departing aircraft.

Modest Progress Was Made in Implementing Earned Value Management

Since FY 2002, OMB has required the use of EVM as a project management tool for major IT investments. This process is intended to ensure that data produced through EVM are reliable enough to allow objective reporting of project status, produce early warning signs of impending schedule delays and cost overruns, and provide estimates of anticipated costs at completion based on actual progress made against the planned work.

As stated in last year's report, EVM can have a significant impact on the success of an IT acquisition because it heightens departmental Investment Review Board (IRB) visibility into whether the major IT investment is on target with respect to cost, schedule, and technical performance.[15] We have made recommendations in the past that would require Operating Administration management to improve EVM practices to ensure that the IRB and OMB have reliable and quantifiable data available with which to make effective IT investment decisions.

This year, Operating Administrations reported that 35 percent of major departmental IT investments met at least half of OMB's criteria for EVM implementation, OMB's memorandum M-05-23,[16] which lists 32 criteria for EVM compliance. This represents a modest improvement from the 23 percent reported last year (see Table 7).

Table 7. Departmental Major IT Investment EVM Status

Operating Administration[a]	Major IT Investments (Requiring EVM)	OMB's EVM (Meeting 50 percent or greater criteria)			
		FY 2006		FY 2007	
		Investments	Percent	Investments	Percent
FAA	21	6	29%	10	48%
Other	10	1	10%	1	10%
Total	**31**	**7**	**23%**	**11**	**35%**

Data Source: Department's EVM Quarterly Report, 5/2007, and FAA EVM Self Assessment, 6/2007.
[a] See Exhibit C for full Operating Administration names.

While FAA made more progress than other Operating Administrations in enhancing EVM implementation, it still faces a significant challenge and requires continued management attention. In FY 2007 OMB identified 22 departmental major investments as high-risk and required the Department to promote more effective oversight by establishing and validating performance measurement baselines, specifically through the use of EVM, for 12 investments. FAA is responsible for managing all of these 12 high-risk investment projects, 5 of which have not met half of the OMB EVM implementation requirements. One of these

[15] OIG Report "Audit of Information Security Program," Report Number FI-2007-002, October 23, 2006.
[16] Improving Information Technology (IT) Project Planning and Execution, OMB M-05 23, August 4, 2005.

systems is the Automatic Dependent Surveillance-Broadcast (ADS-B) system. Congress specifically requires FAA to use EVM to manage development cost and schedule because of its importance to future air traffic control operations. These five investments account for about $10 billion in life-cycle cost estimates; half of the total high-risk investment life-cycle estimated cost (see Table 8).

Table 8. FAA Major High-Risk IT Investments

	High-Risk IT Investments	Life-Cycle Dollars (in Millions)	Project Met 50% of OMB's EVM Implementation Criteria in FY 2006	Project Met 50% of OMB's EVM Implementation Criteria in FY 2007
1	Automated Surface Observing System/Automated Weather Observing System (ASOS/AWOS)	$1,075	NO	NO
2	Wide Area Augmentation System (WAAS)	$4,225	NO	NO
3	FAA Telecommunications Infrastructure (FTI)	$2,289	NO	NO
4	System-Wide Information Management (SWIM)	$431	new development	NO
5	Automatic Dependent Surveillance-Broadcast (ADS-B)	$2,341	new development	NO
	Sub-total	**$10,361**		
6	Standard Terminal Automation Replacement System (STARS)	$3,580	NO	YES
7	Terminal Radar Digitizing, Replacement, and Establishment (TRDRE) (ASR-11)	$1,148	NO	YES
8	Oceanic Automation System: Advanced Technologies and Oceanic Procedures (ATOP)	$1,605	NO	YES
9	Next Generation VHF Air/Ground Communications (NEXCOM)	$440	YES	YES
10	En Route Automation Modernization (ERAM)	$2,843	YES	YES
11	Terminal Automation Modernization and Replacement (TAMR)	$178	YES	YES
12	Traffic Flow Management (TFM)	$968	YES	YES
	Sub-total	**$10,762**		
	Total	**$21,123**		

Data Source: FAA EVM Self-Assessment, 6/2007, and OMB High Risk IT Projects, 6/30/2007.

Another area requiring management attention is that the CIO Office has not developed procedures to verify Operating Administrations' EVM progress reporting. During FY 2007, the CIO Office devoted resources to other higher priority initiatives, such as the move to the new Headquarters and revising IRB charters for IT governance issues. However, the CIO Office continues to use these EVM data submitted by the Operating Administrations to report the status of investments to OMB and senior departmental officials. Until the Department

adequately implements EVM processes, it has limited assurance that the information used for tracking the cost, schedule, and performance of its investments is reliable. As reported last year, the CIO Office needs to develop a work plan to guide and measure EVM implementation in the Department.

RECOMMENDATIONS

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

Enhance the protection of information systems by:

1. Working with the Acting FAA Administrator to establish target dates for correcting air traffic control systems' risk categorization in accordance with departmental policy;
2. Working with the affected Operating Administrations to ensure proper risk categorization and security protection of systems containing personally identifiable information;
3. Requiring Operating Administration CIOs and system owners to identify and implement security upgrades needed to meet minimum security standards by March 31, 2008; and
4. Establishing a security test and evaluation process for all departmental systems operating on the common IT infrastructure after the security controls review is complete for the expanded infrastructure.

Enhance correction of identified security deficiencies by:

5. Working with Operating Administrators to develop measures of accountability that would hold Operating Administration CIOs and system owners responsible for timely correction, and decisions to support cancellations, of identified security weaknesses, such as incorporating these measures as part of their performance standards.

Enhance network security configuration by:

6. Working with Operating Administrations to establish an effective methodology to ensure that commercial software products used in departmental systems are configured in accordance with security standards; and deploying an automated tool to systematically verify compliance with departmental baseline configuration standards; and
7. Finalizing the secure remote access implementation and management policy; and continuing to explore alternatives to using employee home computers for telework, such as having a pool of Government-issued laptop computers that are properly configured and in compliance with departmental security standards to support telework.

Ensure the consistency and timeliness of security incident reporting by:

8. Directing the FAA CSIRC to establish consistent procedures to ensure that all security incidents are reported to the Department and US–CERT in a timely manner;
9. Conducting periodic reviews of the effectiveness of FAA's security incident reporting practice; and
10. Working with the FAA CIO to ensure accurate security performance measurement reporting in the Performance and Accountability Report to OMB and the Congress.

Enhance the Department's implementation of earned value management by:

11. Working with Operating Administration CIOs to establish goals for improving EVM implementation in all major investment projects; and
12. Performing an EVM system compliance assessment based on Operating Administration progress reporting.

MANAGEMENT COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

A draft of this report was provided to the Department's Chief Information Officer on September 28, 2007. On October 4, we received the Department's Chief Information Officer's response, which can be found in the appendix. The Chief Information Officer generally concurred with the report's findings and recommendations and will provide details in 30 days, describing the specific actions and milestones that will be taken to implement the recommendations.

ACTIONS REQUIRED

We will review the Chief Information Officer's detailed action plans to determine whether they satisfy the intent of our recommendations. All corrections are subject to follow-up provisions in DOT Order 8000.1.C. We appreciate the courtesies and cooperation of the CIO Office and the Operating Administrations' representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1959; David Dobbs, Principal Assistant Inspector General for Auditing and Evaluation, at (202) 366-0500; or Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1496.

#

cc: Deputy Secretary
Assistant Secretary for Budget and Programs/Chief Financial Officer
Acting Federal Aviation Administrator
CIO Council Members
Martin Gertel, M-1

EXHIBIT A. OIG INPUT TO FISMA REPORT

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	% of Total	Total Number	% of Total	Total Number	% of Total
FAA	High	19	0	0	0	19	0	0		0		0	
	Moderate	159	2	7	0	166	2	2	100%	1	50%	1	50%
	Low	75	6	4	1	79	7	7	100%	6	86%	0	0%
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**253**	**8**	**11**	**1**	**264**	**9**	**9**	100%	**7**	78%	**1**	11%
FHWA	High	6	0	0	0	6	0	0		0		0	
	Moderate	13	2	1	0	14	2	0	0%	0	0%	0	0%
	Low	5	0	0	0	5	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**24**	**2**	**1**	**0**	**25**	**2**	**0**	0%	**0**	0%	**0**	0%
FMCSA	High	1	0	0	0	1	0	0		0		0	
	Moderate	21	1	0	0	21	1	1	100%	0	0%	1	100%
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**23**	**1**	**0**	**0**	**23**	**1**	**1**	100%	**0**	0%	**1**	100%
FRA	High	0	0	0	0	0	0	0		0		0	
	Moderate	19	0	0	0	19	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**20**	**0**	**0**	**0**	**20**	**0**	**0**		**0**		**0**	
FTA	High	0	0	0	0	0	0	0		0		0	
	Moderate	3	0	0	0	3	0	0		0		0	
	Low	2	0	0	0	2	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**5**	**0**	**0**	**0**	**5**	**0**	**0**		**0**		**0**	
MARAD	High	0	0	0	0	0	0	0		0		0	
	Moderate	7	3	0	0	7	3	1	33%	0	0%	0	0%
	Low	4	0	0	0	4	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**11**	**3**	**0**	**0**	**11**	**3**	**1**	33%	**0**	0%	**0**	0%
NHTSA	High	0	0	0	0	0	0	0		0		0	
	Moderate	7	0	3	1	10	1	1	100%	0	0%	1	100%
	Low	8	0	0	0	8	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**15**	**0**	**3**	**1**	**18**	**1**	**1**	100%	**0**	0%	**1**	100%
OIG	High	0	0	0	0	0	0	0		0		0	
	Moderate	2	0	0	0	2	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**3**	**0**	**0**	**0**	**3**	**0**	**0**		**0**		**0**	
OST	High	5	2	0	0	5	2	2	100%	1	50%	0	0%
	Moderate	23	2	0	0	23	2	2	100%	1	50%	0	0%
	Low	14	0	0	0	14	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**42**	**4**	**0**	**0**	**42**	**4**	**4**	100%	**2**	50%	**0**	0%
PHMSA	High	0	0	0	0	0	0	0		0		0	
	Moderate	3	1	0	0	3	1	1	100%	0	0%	1	100%
	Low	2	0	0	0	2	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**5**	**1**	**0**	**0**	**5**	**1**	**1**	100%	**0**	0%	**1**	100%
RITA	High	0	0	0	0	0	0	0		0		0	
	Moderate	9	0	0	0	9	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**10**	**0**	**0**	**0**	**10**	**0**	**0**		**0**		**0**	
SLSDC	High	0	0	0	0	0	0	0		0		0	
	Moderate	0	0	0	0	0	0	0		0		0	
	Low	1	0	0	0	1	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
STB	High	0	0	0	0	0	0	0		0		0	
	Moderate	2	0	0	0	2	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**		**0**		**0**	
Agency Totals	**High**	**31**	**2**	**0**	**0**	**31**	**2**	**2**	100%	**1**	50%	**0**	0%
	Moderate	**268**	**11**	**11**	**1**	**279**	**12**	**8**	67%	**2**	17%	**4**	33%
	Low	**115**	**6**	**4**	**1**	**119**	**7**	**7**	100%	**6**	86%	**0**	0%
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**414**	**19**	**15**	**2**	**429**	**21**	**17**	81%	**9**	43%	**4**	19%

Question 3: Evaluation of Oversight of Contractor Systems and Quality of 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.** 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. Response Categories: - 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	Almost Always (96-100% of the time)
3.b.	**The agency has developed a complete 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.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 96-100% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG 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 or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually.** **Yes or No.**	Yes
3.f.	**If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**	

Question 4: Evaluation of Plan of Action and Milestones (POA&M) Process		
Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided. **For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.** Response Categories: - 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		
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.**	Sometimes (51-70% 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).**	Sometimes (51-70% of the time)
4.c.	**Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).**	Almost Always (96-100% of the time)
4.d.	**Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.**	Almost Always (96-100% of the time)
4.e.	**IG findings are incorporated into the POA&M process.**	Almost Always (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.**	Frequently (71-80% of the time)
Comments:		

Question 5: IG Assessment of the Certification and Accreditation Process			
Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate. 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, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.			
5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory	
5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:**	Security plan	Yes
		System impact level	Yes
		System test and evaluation	Yes
		Security control testing	Yes
		Incident handling	Yes
		Security awareness training	Yes
		Configurations/patching	Yes
		Other: Contingency Planning	
Comments: Item 5.a. We identified a concern with FAA's risk-impact analyses of air traffic control systems in both FYs 2006 and 2007. Specifically, of about 100 systems used to direct air traffic control operations, none were reported as having a high-risk impact. Systems identified by FAA as high-risk impact are primarily for administrative functions, such as the procurement system. After this issue was brought to management's attention again this year, the departmental CIO, the FAA Acting Deputy Administrator, and the FAA CIO all agreed to collaborate with Air Traffic Organization business owners to ensure that air traffic control systems are individually reviewed and categorized in accordance with NIST standards and DOT policy, as a key priority for FY 2008. We considered this commitment in our evaluation of the overall quality of the Department's certification and accreditation process. We plan to follow up with FAA on this issue throughout FY 2008.			

Question 6: IG Assessment of Privacy Program and Privacy Impact Assessment (PIA) Process		
6.a.	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments:		
6.b.	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments:		

Question 7: Configuration Management		
7.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
Comments:	Currently, the Department has a draft policy called DOT Information Technology and Information Assurance policy 2007-XX: FISMA Information System Security Baseline configuration policy. When it becomes the final, this policy supersedes departmental IA/IT policy, issued on April 3, 2006	
7.b.	**Approximate the extent to which applicable information systems apply common security configurations established by NIST.** **Response categories:** - 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	Rarely (0-50% of the time)

Question 8: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
8.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	Yes
8.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
8.c.	**The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.**	Yes
Comments:	While we answered "Yes" to item 8a, we found that FAA did not report 40 security incidents, which account for approximately 14% of the total security incidents in the first three quarters of FY 2007, to the Department. FAA claimed that 31 of these 40 incidents were either repeated or duplicated incidents. However, FAA was not able to provide any evidence that the original incidents had been reported. In addition, FAA indicated that two incidents were false-positives and did not need to be reported, even though they were not recorded as false-positives in FAA's official log.	

Question 9: Security Awareness Training	
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees	Frequently (71-80% of employees)
Question 10: Peer-to-Peer File Sharing	
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 or No.	Yes
Question 11: E-Authentication Risk Assessments	
The agency has completed system e-authentication risk assessments. Yes or No.	Yes

EXHIBIT B. SCOPE AND METHODOLOGY

During FY 2007, we fulfilled the requirements of the Federal Information Security Management Act of 2002 by reviewing the progress made in meeting the minimum Government security standards to protect sensitive information systems and data, determining whether the network operating environment at the Department's new Headquarters building is secure, identifying corrections made to security weaknesses previously identified, and evaluating the Department's use of earned value management for its major IT investment projects. In addition, we sampled 21 systems that had undergone system security reviews to determine whether the Operating Administrations had complied with governmental and departmental standards in assessing system risks, identifying security requirements, testing security controls, and accrediting systems to support business operations.

We assessed the Department's progress in correcting weaknesses identified in last year's FISMA review and contributed to the FISMA report by rating departmental 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 the National Institute of Standards and Technology. We also used commercial scanning software to assess network vulnerabilities.

We performed our information security review work throughout FY 2007, focusing on FISMA evaluation between March and September 2007 at departmental and Operating Administration 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 the Department'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-2007-002, October 23, 2006;
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. DEPARTMENTAL OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

Operating Administration	Acronym	FY 2006	FY 2007
Federal Aviation Administration	FAA	263	264
Federal Highway Administration	FHWA	23	25
Federal Motor Carrier Safety Administration	FMCSA	22	23
Federal Railroad Administration	FRA	22	20
Federal Transit Administration	FTA	6	5
Maritime Administration	MARAD	12	11
National Highway Traffic Safety Administration	NHTSA	18	18
Office of Inspector General	OIG	3	3
Office of the Secretary	OST	40	42
Pipeline and Hazardous Materials Safety Administration	PHMSA	5	5
Research and Innovative Technology Administration	RITA	9	10
Saint Lawrence Seaway Development Corporation	SLSDC	1	1
Surface Transportation Board	STB	2	2
Total Systems		**426**	**429**

Data Source: OIG report "Audit of Information Security Program," Report Number FI-2007-002, October 23, 2006, and Enterprise Security Portal as of 9/5/2007

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Ed Densmore	Program Director
Michael Marshlick	Project Manager—Senior Computer Science Adviser
Joann Adam	Project Manager
Nathan Custer	Project Manager
Dr. Ping Z. Sun	Project Manager
Michael P. Fruitman	Communications Adviser
Lynn Dowds	Senior Auditor
Jim Mallow	Senior Auditor
Tim Roberts	Senior Auditor
Henry Lee	Computer Scientist
Mitchell Balakit	Information Technology Specialist
Christopher Cullerot	Information Technology Specialist
Atul Darooka	Information Technology Specialist
Vasily Gerasimov	Information Technology Specialist
Ann Moles	Information Technology Specialist
Martha Morrobel	Information Technology Specialist
Raj Singh	Information Technology Specialist

APPENDIX. MANAGEMENT COMMENTS

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

Memorandum

Subject: Office of the Chief Information Officer Response to Office of Inspector General Federal Information Security Management Act (FISMA) Audit Draft Report

Date: 10/4/07

From: Daniel G. Mintz
DOT Chief Information Officer, S-80

To: Rebecca Leng
Technology and Computer Security, (JA-20)

The Department of Transportation (DOT) Chief Information Officer (CIO) officials reviewed the Office of Inspector General (OIG's) draft final FY 2007 Information Security Program Audit Report and provided oral comments.

CIO officials generally concurred with the report's findings and recommendations and will provide written comments describing the specific actions and milestones that will be taken to implement the recommendations, 30 days after the signing date of the official FY 2007 FISMA Report.

The OCIO office appreciates the working relationship developed during this audit and looks forward to the OIG's continued involvement during FY 2008 with "Getting back to Green" remediation efforts.

If you have any questions, please contact Phillip Loranger, Chief Information Security Officer and Deputy Associate CIO for IT Investments, at phillip.loranger@dot.gov or (202) 366-5636.

The following pages contain textual versions of the graphs and charts found in this document. These pages were not in the original document but have been added here to accommodate assistive technology.

Information Security Program
Section 508 Compliance Presentation

Figure 1. Operating Administrations With Highest Ratios of Overdue Corrections

- For FHWA 282 POA&Ms are open and 246 POA&Ms are 6+ months overdue
- For FRA 287 POA&Ms are open and 269 POA&Ms are 6+ months overdue
- For PHMSA 105 POA&Ms are open and 104 POA&Ms are 6+ months overdue

Figure 2. Operating Administrations' Total Systems and Percentages of Systems Reported as Having Met Baseline Security Configuration Standards

- For FAA the total number of systems is 264 and number of systems reported to have met security baseline configuration standards is 15. 6% of FAA systems met baseline security configuration standard.
- For FHWA the total number of systems is 25 and number of systems reported to have met security baseline configuration standards is 3. 12% of FHWA systems met baseline security configuration standard.
- For FMCSA the total number of systems is 23 and number of systems reported to have met security baseline configuration standards is 22. 96% of FMCSA systems met baseline security configuration standard.
- For FRA the total number of systems is 20 and number of systems reported to have met security baseline configuration standards is 19. 95% of FRA systems met baseline security configuration standard.
- For FTA the total number of systems is 5 and number of systems reported to have met security baseline configuration standards is 5. 100% of FTA systems met baseline security configuration standard.
- For MARAD the total number of systems is 11 and number of systems reported to have met security baseline configuration standards is 0. 0% of MARAD systems met baseline security configuration standard.
- For NHTSA the total number of systems is 18 and number of systems reported to have met security baseline configuration standards is 16. 89% of NHTSA systems met baseline security configuration standard.
- For OIG the total number of systems is 3 and number of systems reported to have met security baseline configuration standards is 3. 100% of OIG systems met baseline security configuration standard.

- For OST the total number of systems is 42 and number of systems reported to have met security baseline configuration standards is 29. 69% of OST systems met baseline security configuration standard.
- For PHMSA the total number of systems is 5 and number of systems reported to have met security baseline configuration standards is 5. 100% of PHMSA systems met baseline security configuration standard.
- For RITA the total number of systems is 10 and number of systems reported to have met security baseline configuration standards is 9. 90% of RITA systems met baseline security configuration standard.
- For SLSDC the total number of systems is 1 and number of systems reported to have met security baseline configuration standards is 0. 0% of SLSDC systems met baseline security configuration standard.
- For STB the total number of systems is 2 and number of systems reported to have met security baseline configuration standards is 0. 0% of STB systems met baseline security configuration standard.

Table 7. Departmental Major IT Investment EVM Status

- FAA has 21 major IT investments requiring EVM, out of which 6 investments or 29% met 50 percent or greater OMB EVM criteria in FY 2006 and 10 investments or 48% met 50 percent or greater OMB EVM criteria in FY 2007
- Other Operating Administrations have 10 major IT investments requiring EVM, out of which 1 investment or 10% met 50 percent or greater OMB EVM criteria in FY 2006 and 1 investment or 10% met 50 percent or greater OMB EVM criteria in FY 2007
- Out of total 31 major IT investments requiring EVM, 7 investments or 23% met 50 percent or greater OMB EVM criteria in FY 2006 and 11 investments or 35% met 50 percent or greater OMB EVM criteria in FY 2007