QUALITY CONTROL REVIEW OF THE DEPARTMENT'S IMPLEMENTATION OF EARNED VALUE MANAGEMENT AND SECURITY COST REPORTING

Department of Transportation

Report Number: QC-2009-048
Date Issued: April 24, 2009

Memorandum

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

Subject: ACTION: Report on Quality Control Review of the Department's Implementation of Earned Value Management and Security Cost Reporting
Report Number: QC-2009-048

Date: April 24, 2009

From: Rebecca C. Leng
Assistant Inspector General for Financial and Technology Audits

Reply to Attn. of: JA-20

To: Acting Chief Information Officer, DOT

This report summarizes the results of the audit of the Department of Transportation's implementation of earned value management (EVM), and the supportability of estimated security costs for major information technology (IT) investments.[1] The Department requested about $2.4 billion for 46 major IT investments in its Fiscal Year 2009 budget submission, including about $116 million in security funding.

The Clinger-Cohen Act of 1996 requires Federal agencies to establish effective management structures to govern IT investments and to improve their implementation and management. The Office of Management and Budget (OMB) developed Federal policy for planning, budgeting, acquiring, and managing Federal IT assets. In addition, OMB's Capital Programming Guide directs agencies to develop, implement, and use a capital programming process that (1) fully implements EVM[2] for IT projects, with emphasis on those designated as high-risk; (2) integrates IT security into their strategic and operational planning processes; (3) institutes performance measures and management processes that monitor actual performance and compares them against planned results; and (4) provides senior agency management and OMB with a Capital Asset Plan and

[1] A major IT investment is one that requires special management attention because of its importance to an agency's mission or the magnitude of the investment.
[2] Earned value management is a management tool that is used to plan, execute, and control the costs and schedules of IT projects.

Business Case (Exhibit 300) that documents the justification, management oversight practice, and status for each major IT investment.[3]

OMB requires agencies to employ EVM to calculate cost and schedule variances from the approved baseline for all major IT investments in the development phase appearing on Exhibit 300s. When properly implemented, EVM provides insight on program performance by comparing the value of work accomplished in a given period against the planned value of work scheduled for that period.

An independent firm—KPMG, LLP, of Washington, D.C.—carried out this performance audit under contract to the Office of Inspector General (OIG). The objectives were to determine whether (1) the earned value management measures included in the OMB Exhibit 300 submissions properly reflected project performance, and (2) security costs included in the submissions were supported.

KPMG's report can be found in its entirety in Appendix A. KPMG's scope and methodology and review results are included in Appendix A, starting on pages 15 and 18, respectively. We performed a quality control review of the audit work to ensure that it complied with generally accepted government auditing standards as prescribed by the Comptroller General of the United States. In our opinion, KPMG's audit work complied with applicable standards.

The following summarizes KPMG's findings.

FINDINGS

KPMG concluded that the EVM measures included in Exhibit 300 submissions could not be relied upon to properly reflect project performance. KPMG found that the Department lacked a standard approach for implementing EVM systems because the implementation guide specified in the departmental policy was never issued. KPMG reviewed six major investment projects and found them deficient in meeting the requirements specified by OMB. For example, EVM requirements were not specified in acquisition contracts, and certification reviews of contractor systems used to compile EVM data were not conducted, as required by OMB.

Further, KPMG concluded that the Department had no assurance that the security cost estimates included in the budget submission were adequate to protect its information systems. The Department has not established a standard method to

[3] OMB Circular A-11 (section 300) and OMB's Capital Programming Guide (supplement to Part 7 of Circular A-11).

accurately and consistently estimate the costs of implementing IT security. According to the Operating Administrations, they estimate security funding needs through historical cost data, yet they were unable to provide support or justification for their security cost figures.

Departmental EVM Policy and Implementation Guide Are Incomplete, Leaving the Department without a Roadmap to Guide Proper EVM Implementation

Per OMB, agencies were to develop a comprehensive EVM policy no later than December 31, 2005. In January 2008, DOT issued its EVM policy.[4] The policy contained pre-established dollar thresholds mandating at what levels of expenditure IT projects must implement EVM, as well as general guidance for implementing an earned value management system (EVMS). Yet specific implementation guidance to ensure consistent and reliable EVM implementation across the Operating Administrations was lacking.[5] For example, guidance is needed for:

- Provisions for EVM training to ensure that program office staff and contractor personnel are properly trained on the analysis of generated earned value data.

- Integration of EVM practices with portfolio management to ensure that EVM data are used in capital planning and investment control decisions.

- Standards to capture project scope/work assignments and use of standard work breakdown structure (WBS) to ensure that large projects are properly broken down into smaller components for compiling EVM data. This allows a program manager to more precisely identify which components are causing cost overruns or schedule delays, and more effectively mitigate their root causes.

- Enforcement of joint government/contractor consultation with respect to the Integrated Baseline Review to support cost and schedule rebaselining. This ensures that integrated baseline reviews are conducted regularly and with proper personnel to adjust cost, schedule, and performance goals.

[4] A memorandum jointly issued by the departmental Chief Information Officer, Chief Financial Officer, and the Deputy Chief Acquisition Officer entitled *DOT Earned Value Management Policy*, January 14, 2008.

[5] In the absence of Departmentwide implementation guidance, the Federal Aviation Administration and the Federal Motor Carrier Safety Administration developed EVM implementation guidance for their own use.

- Protection of EVM data from unauthorized changes. It should describe any templates, tools, and systems utilized and controls needed to ensure that data are collected consistently and protected from unauthorized changes.

The Department had planned to complete the draft EVM implementation guide by March 31, 2008. However, according to the former Chief Information Officer, a lack of dedicated resources impeded the planned action. The Department has not established a revised target date for completing the implementation guide. Until this guide is developed and disseminated across the Department, the Operating Administrations will lack a roadmap for full and consistent EVM implementation as intended by OMB to ensure the integrity and reliability of EVM data.

Operating Administrations Did Not Meet OMB Requirements for EVM Implementation, Rendering EVM Data Unreliable in Measuring Project Performance

To ensure reliable EVM implementation for major IT investment projects, OMB requires agencies to (1) include EVM requirements in acquisition contract provisions, (2) conduct EVM certification and surveillance reviews,[6] (3) use work breakdown structure for work decomposition, and (4) conduct performance reviews using EVM data. KPMG selected a judgmental sample of six major IT investments, with a total life-cycle value of $4.2 billion. These investment projects are managed by three Operating Administrations—the Federal Aviation Administration (FAA), the Federal Motor Carrier Safety Administration (FMCSA), and the Pipeline and Hazardous Materials Safety Administration (PHMSA).

As shown in Table 1 below, KPMG found that Operating Administrations did not consistently meet OMB requirements when implementing EVM for these major investments. Specifically, the six sampled major IT investments were deficient in performing one or more of the four required key EVM components. As a result, the Department has no assurance that the EVM data used to measure the cost, schedule, and performance of these investments properly and realistically reflect accurate project performance.

[6] These reviews are required to ensure that the system used to compile EVM data meets OMB requirements and can be relied upon for measuring program performance.

Table 1. Extent to Which Sample Investments Met OMB EVM Requirements

Operating Administration Major IT Investments [a]	Planning			Controlling
	Standard EVMS Language Included in Contracts?	EVMS System Certification Performed?	WBS for Major Investments Used?	EVMS Contractor Surveillance Performed?
FAA—TAMR	Yes	*No*	Yes	Yes
FAA—ASOS/AWOS	*No*	*No*	Yes	Yes
FAA—ATOP	*No*	Yes	Yes	*No*
FAA—ATM/TFM	Yes	Yes	Yes	*No*
PHMSA—SMART	*No*	*No*	*No*	*No*
FMCSA—Modernization	*No*	*No*	Yes	*No*

[a] For full names of Operating Administrations and their IT systems, see Tables 2 and 3 on pages 15 and 16 (Appendix A), respectively.

The Department Had No Assurance That Security Cost Estimates Included in Its Budget Submission Were Adequate To Protect Its Information Systems

National Institute of Standards and Technology Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process,* directs agencies to estimate security costs based on a process that identifies, prioritizes, and corrects security weaknesses identified with their computer systems. KPMG found that the Department had not established guidance or practices to ensure consistent estimation of IT security costs for its major IT investments. According to the Operating Administrations, they estimate security funding needs only through historical cost data. Yet they were unable to show how such historical data support their security cost estimate figures.

Further, in a matter related to the adequacy of security cost estimation but not part of the KPMG review, we found that Operating Administrations did not request adequate funding to correct security deficiencies. As disclosed in our annual information security audit, the Operating Administrations had not estimated the costs for remediating more than half (2,493 out of 4,286) of the security

deficiencies found in departmental information systems.[7] In addition, security cost estimates varied significantly among the Operating Administrations—ranging from less than 1 percent to 23 percent of their IT budget requests. In our opinion, such a disparity signals inconsistent and potentially unreliable estimation practices in the Department (see Table 2). Accordingly, the Department has no assurance that the security cost estimates included in the budget submission are adequate to protect its information systems.

Table 2. FY 2009 Budget Requests for IT and IT Security Spending

Operating Administration[a]	Total IT Budget (in millions)	Estimated IT Security Costs (in millions)	% of IT Security Costs
FAA	$2,518.21	$40.14	1.59%
FHWA	18.59	1.19	6.42%
FMCSA	26.41	1.29	4.89%
FRA	15.19	1.20	7.90%
FTA	12.57	0.37	2.97%
MARAD	4.09	0.03	0.80%
NHTSA	20.79	1.49	7.18%
OST[b]	342.97	80.20	23.38%
PHMSA	8.74	0.35	4.04%
RITA	12.97	0.36	2.80%
Total	**$2,980.53**	**$126.62**	**4.25%**

[a] For full names of Operating Administrations, see Table 2 in Appendix A.
[b] Security estimates for OST comprise departmentwide operations such as the Cyber Security Management Center.

. Source: OIG analysis based on DOT's Exhibit 53, Agency IT Investment Portfolio, submission to OMB.

RECOMMENDATIONS

On page 41 in Appendix A, KPMG made a series of recommendations to DOT management for improving EVMS processes/practices and security cost estimation. We agree with KPMG's recommendations and have summarized them below (Recommendations 1 and 3). We also supplemented KPMG's recommendations to ensure that deficiencies identified during the audit are corrected (Recommendation 2).

[7] *Audit of DOT Information Security Program,* OIG Report Number FI-2009-003, October 8, 2008.

Based on KPMG's findings, we recommend that the departmental Acting Chief Information Officer:

1. Establish a target date to complete and distribute the DOT EVM implementation guidance to Operating Administrations. This guidance should document processes and practices consistent with guidelines published by OMB and address the detailed recommendations included in KPMG's report in Appendix A.

2. Require Operating Administrations to review all major IT investments in the development phase for compliance with key OMB requirements for EVM implementation and report results to the CIO office. Ensure that Operating Administrations establish a target date for correcting deficiencies found.

3. Establish security cost estimation standards consistent with the National Institute of Standards and Technology, require Operating Administrations to follow the standards, and verify compliance with the standards by performing a sample review of Operating Administrations' security cost estimate submissions.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided a draft of this report to the Acting DOT Chief Information Officer for comment on March 25, 2009, and received her response on April 10. She concurred with all of our recommendations, and stated that her office is in the process of developing new policy and guidance to ensure full compliance with earned value management as directed by the Office of Management and Budget. This includes implementation of standards for security estimation techniques across the Department. The response can be found in its entirety in Appendix B.

In general, management actions—begun and planned—adequately address the intent of our recommendations. The Acting DOT Chief Information Officer's responses to our recommendations are summarized below:

Recommendation 1: Concurred. The Acting Chief Information Officer stated that a new DOT earned value management policy and associated guidelines will be issued by September 30, 2009. The new guidelines will include standards, processes, templates, and techniques for implementation and use of EVM consistent with Office of Management and Budget requirements.

Recommendation 2: Concurred. The Acting Chief Information Officer stated that each Operating Administration has a plan of action and milestones established for EVM implementation, and is required to report to the CIO all progress toward meeting the Department's goal of full compliance by December 31, 2009. Additionally, the Acting Chief Information Officer is in the process of enhancing program management review tools to provide a complete picture of the health of investment projects for decision-making. EVM measures submitted by Operating Administrations will be included for the health evaluation.

Recommendation 3: Concurred. The Acting Chief Information Officer stated that by June 30, 2009, new guidance to standardize security cost estimating techniques in accordance with the National Institute of Standards and Technology approach will be disseminated Departmentwide. In addition, by August 30, 2009, the Office of the Chief Information Officer will conduct sample reviews to verify that the departmental security cost estimating guidelines are used by Operating Administrations in preparing Exhibit 300 budget submissions for FY 2011.

ACTIONS REQUIRED

Management actions taken and planned are responsive to our recommendations, and are considered resolved subject to follow-up provisions in DOT Order 8000.1C.

We appreciate the courtesies and cooperation of representatives from the departmental Chief Information Officer's office, the Operating Administrations, and KPMG during this audit. If you have any questions concerning this report, please call me at (202) 366-1407 or Michael Marshlick, Project Manager, at (202) 366-1476.

#

cc: Martin Gertel, M-1
CIO Council Members

Department of Transportation
Earned Value Management and Security Cost Reporting Performance Audit

Prepared for: DOT Office of Inspector General

As of Date: July 31, 2008

Prepared By:
KPMG LLP
2001 M Street NW
Washington DC 20036

Table of Contents
FINAL REPORT

REPORT

Appendix A. KPMG LLP Report

KPMG LLP
2001 M Street, NW
Washington, DC 20036

FINAL REPORT

EXECUTIVE SUMMARY

February 13, 2009

OFFICE OF INSPECTOR GENERAL
U.S. DEPARTMENT OF TRANSPORTATION
1200 NEW JERSEY AVENUE, SE
WASHINGTON, D.C. 20590

KPMG LLP (KPMG) was contracted by the Department of Transportation (DOT) Office of Inspector General (OIG) under Contract No. DT0S59-06-A-00031, Order No. 2007-Z-0003 to conduct a performance audit of the department's adoption and use of Earned Value Management Systems (EVMS) across the Departmental Operating Administrations (OAs), (i.e., modes), and specifically for certain Information Technology (IT) investments. This performance audit report presents the results of our work conducted to address the performance audit objectives relative to the DOT. Our work was performed during the period of March 3, 2008 to July 31, 2008, and our results are as of July 31, 2008.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and recommendations based on our audit objectives.

The audit objectives of the notification dated February 19, 2008 related to project number 07F3017F000 are to determine whether (1) the EVMS measures included in the Exhibit 300 submissions properly reflect project performance, (2) security costs included in the Exhibit 300 submissions are supported, and (3) OA management actively monitors its major IT investments to meet departmental requirements. We were tasked to review DOT's EVMS capability to assess how mature the Department is in EVMS as it relates to guidelines referenced in legislation, policy, and standards pertaining to EVMS. The results of this performance audit address objectives (1) and (2) referenced above. The Office of Inspector General (OIG) is addressing objective (3) and EVMS data being used for program oversight and control in a separate report.

The DOT has established an EVMS policy that contains pre-established dollar thresholds and guidance for IT investment owners to consider when implementing EVMS. In addition, various modes have improved their use of EVMS by establishing supporting materials, such as IT project management and EVMS implementation guidance, providing EVMS training and conducting EVMS lessons learned. While these items help provide a foundation of EVMS guidance for modes to follow and investments to use, there are opportunities for improvement to further implement and use EVMS to help manage major IT investments.

Overall, based on the interviews conducted, documents inspected, and test procedures performed within the audit program guide, we determined that the DOT has inconsistently applied controls across the ten (10) departmental modes and seven (7) IT investments. As a result, the EVMS-related processes used to collect and report EVMS data cannot be relied on to properly reflect project performance in Exhibit 300

submissions. In addition, we found that project management practices related to EVMS are not consistently applied across the OAs and major IT investments. Finally, the security cost estimates that are derived for Exhibit 300 submissions cannot be fully supported. Timely implementation of the recommendations is needed to fulfill departmental requirements and achieve maturity in managing IT investments.

We currently report, for the DOT's consideration, three recommendations from this performance audit. These recommendations include 1) Controls over the reliability of EVMS data should be strengthened, 2) Controls over the reasonableness of security cost estimates should be strengthened, and 3) Controls over the implementation and use of EVMS in project oversight should be strengthened. EVMS provides organizations with the methodology needed to integrate the management of project scope, schedule, and cost. Implementation of these recommendations should enable DOT to improve reliability of data needed to oversee IT projects and make investment decisions. The detailed objectives of this performance audit are enumerated within Section II. Findings and Recommendations are enumerated within Section IV.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards.* KPMG was not engaged to, and did not render an opinion on the DOT's internal controls over financial reporting or over financial management systems (for purposes of OMB's Circular No. A-127, *Financial Management Systems*, July 23, 1993, as revised). KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

Sincerely,

KPMG LLP

I. BACKGROUND

FINAL REPORT

The Department of Transportation (DOT) mission is to serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future.[1] DOT invested approximately $2.7 billion annually in information technology (IT). In order to derive the intended benefits of the programs and projects within the IT portfolio, project planning and execution processes should be in place to control the establishment of baseline performance measures and manage deviations from expected performance plans. Earned Value Management (EVM) data is a critical component of the control phase of the IT capital planning process, because it provides investment managers with the cost, schedule, and performance data necessary to help ensure that DOT investments are delivered on time and perform within budget and scope. The addition of the variance and trend analysis aspect of EVM permits an evaluation that monitors deviation from the baseline plan, which may indicate potential threats or opportunities. Proper application of EVM also increases the level of confidence of management that the investment is being managed in accordance with sound project management practices and is consistent with DOT goals and objectives.

The Office of the Secretary of Transportation (OST) is responsible for establishing the requisite policies and procedures to govern the DOT modes within the department for managing investments within the IT portfolio, including policies and procedures related to IT capital planning and investment control (CPIC), program management and project management. These policies and procedures should reflect Office of Management and Budget (OMB) guidance, including provisions for using EVM and estimating IT security costs for investments. In addition, the Operation Administrations (or modes) within DOT are responsible for implementing the policies and procedures promulgated by OST in a manner consistent with both the underlying objectives. Table 2 contains a listing of the key legislation, policies, and standards pertaining to EVMS and IT investment and project management.

[1] www.dot.gov

Table 1: EVMS Legislation, Policies and Standards

Criteria	Description
Legislation	➢ *Government Performance and Results Act of 1993* – mandates the use of performance metrics. ➢ *Federal Acquisition Streamlining Act of 1994* – requires agency heads to achieve, on average, 90% of the cost and schedule goals established for major and non-major acquisition programs of the agency without reducing the performance or capabilities of the items being acquired. ➢ *Clinger Cohen Act of 1996* – requires establishment of the processes for executive agencies to analyze, track, and evaluate the risks and results of major investments in IT and requires reporting on the net program performance benefits achieved by agencies.
Policies	➢ *Office of Management and Budget (OMB) Circular A-11 (Part 7, Planning, Budgeting, Acquisition and Management of Capital Assets)* – outlines a systematic process for program management, which includes integration of program scope, schedule, and cost objective; requires use of earned value techniques for performance measurement during execution of the program; specifically identifies ANSI/EIA Standard 748. ➢ *OMB Memorandum M-04-24, "Expanding Electronic Government (E-Gov) President's Management Agenda (PMA) Scorecard Cost, Schedule and Performance Standards for Success"* – provides additional information on the President's Management Agenda Expanded Electronic Government initiative and the standard for success concerning cost, schedule and performance goals. ➢ *OMB Memorandum M-05-23, "Improving Information Technology (IT) Project Planning and Execution"* – provides guidance to assist agencies in monitoring and improving project planning and execution and fully implementing EVMS for major IT projects.
Standards	1. *ANSI/EIA Earned Value Management System (EVMS) Standard 748* – industry process for use of EVMS including integration of program scope, schedule and cost objectives, establishment of a baseline plan for accomplishment of program objectives, and use of earned value techniques for performance measurement during the execution of a program. 2. *Project Management Institute (PMI) Standard for Earned Value Management* – developed as a supplement to "*A Guide to the Project Management Body of Knowledge (PMBOK Guide).*" The Practice Standard for EVM is designed to provide a fundamental understanding of the principles of EVM and its role in facilitating effective project management.

II. OBJECTIVE, SCOPE, AND METHODOLOGY *FINAL REPORT*

KPMG LLP (KPMG) was contracted by the Department of Transportation (DOT) Office of Inspector General (OIG) under Contract No. DT0S59-06-A-00031, Order No. 2007-Z-0003 to conduct a performance audit of the department's adoption and use of Earned Value Management Systems (EVMS) across the departmental Operating Administrating (OAs), (i.e., modes), and specifically for certain Information Technology (IT) investments.

Objectives

The audit objectives of the notification dated February 19, 2008 related to project number 07F3017F000 are to determine whether (1) the EVM measures included in the Exhibit 300 submissions properly reflect project performance, (2) security costs included in the Exhibit 300 submissions are supported, and (3) OA management actively monitors its major IT investments to meet departmental requirements. We were tasked to review DOT's EVMS capability to assess how mature the Department is in EVMS as it relates to guidelines referenced in legislation, policy, and standards pertaining to EVM. The results of this performance audit address objective's (1) and (2) referenced above. The OIG has addressed objective (3) and EVM data being used for program oversight and control in a separate report.

Scope

The performance audit procedures were designed to evaluate the implementation of EVM and security cost estimating and reporting practices over ten OAs and seven major[2] IT investments selected by the OIG summarized in Table 2 and 3 below.

Table 2: Scope of EVM and Security Cost Reporting Analysis by Mode

Modes	Earned Value Management (Y/N)	Security Cost Reporting (Y/N)
Federal Aviation Administration (FAA)	Y	Y
Office of the Secretary of Transportation (OST)	Y	Y
Federal Highway Administration (FHWA)	Y	Y
Federal Motor Carrier Safety Administration (FMCSA)	Y	Y
National Highway Traffic Safety Administration (NHTSA)	Y	Y
Federal Transit Administration (FTA)	Y	Y
Maritime Administration (MARAD)	Y	Y
Federal Railroad Administration (FRA)	Y	Y
Research and Innovative Technology Administration (RITA)	Y	Y
Pipeline and Hazardous Materials Safety Administration (PHMSA)	Y	Y
Surface Transportation Board (STB)[3]	N	N
Saint Lawrence Seaway Development Corporation (SLSDC)[3]	N	N

[2] "Major" investment refers to an IT investment requiring an OMB Exhibit 300 business case.
[3] During our analysis, OA management informed us that they do not have any major IT investments nor have they implemented any EVMS over their IT portfolio. Therefore, the OIG determined to exclude these modes from the scope of this performance audit.

Table 3: Scope of EVM and Security Cost Reporting Analysis for Major Investments

Major Investments	Earned Value Management (Y/N)	Security Cost Reporting (Y/N)
FAA: Terminal Automation Modernization and Replacement (TAMR)	Y	Y
FAA: Automated Surface Observing System/Automated Weather Observing System (ASOS & AWOS)	Y	Y
FAA: Automated Traffic Management/Traffic Flow Management (ATM/TFM)	Y	Y
FAA: Advanced Technologies and Oceanic Procedures (ATOP)	Y	Y
PHMSA: Safety Monitoring and Analysis Reporting Tool (SMART)	Y	Y
FMCSA: Federal Motor Carrier Safety Administration (FMCSA) Modernization	Y	Y
OST: IT Combined Infrastructure	N	Y

We designed the procedures to gain an understanding of how each mode and IT investment in scope has instituted practices related to EVM and security cost reporting, divided into the following sections:

- **EVM Governance:** Includes the policies and supporting guidance (i.e., project and program management) available to implement and use EVM.

- **EVM Tools & Technology:** Includes the EVM tools and related technologies used for IT projects (i.e., EVM-related tools, EVM engines, cost accounting tools, scheduling and resource management tools and technology integration).

- **EVM Implementation & Performance:** Includes EVM supporting standards and practices (e.g., work breakdown structure and use, contract and scope management, resource planning and management, and EVM analysis techniques), EVMS certification[4], EVMS surveillance[5], EVM training, and EVM lessons learned.

- **Security Cost Governance:** Includes the policies and procedures in place for security cost analysis and estimation.

- **Security Cost Estimating, Analysis and Reporting:** Includes the practices used in analyzing, estimating, and reporting security costs.

Our fieldwork was performed during the period of March 3, 2008 to July 31, 2008 and our results are as of July 31, 2008 at Washington, D.C. headquarters and Federal Aviation Administration (FAA) locations.

Methodology

We performed this performance audit in accordance with the *Government Auditing Standards* issued by the Government Accountability Office (GAO). In particular, we designed our procedures to conform to a performance audit defined by the *Government Auditing Standards.* We performed our engagement in three phases: (1) planning, (2) testing and interviewing, and (3) report writing.

[4] EVMS certification refers to the process by which the EVMS is evaluated to verify that it meets the full intentions of the guidelines presented in the ANSI EIA-748 standard. *Source: www.ndia.org*

[5] EVMS surveillance refers to the process of reviewing the health of the EVMS as it is applied to one or more programs. *Source: www.ndia.org*

The planning phase was designed to help ensure that team members developed a collective understanding of the EVM and security cost reporting practices in place for the ten OAs and the seven major investments. We provided separate questionnaires to each mode and to each investment program team. The questionnaires were designed to provide a foundational understanding for conducting interviews and for identifying additional documentation requests.

During the testing and interviewing phase, we conducted interviews, collected and inspected provided artifacts, participated in process walk-throughs, and designed and performed test procedures. We conducted these test procedures primarily at DOT headquarters and FAA facilities in Washington D.C. Testing procedures over the EVM and security cost reporting practices were based on the Federal legislation, policies and industry standards.

When our test procedures required us to select a sample of items from a population for testing, we used a judgmental sample selection methodology. Accordingly, our recommendations are applicable to the sample we tested and were not extrapolated to the population (i.e., all OAs and all major investments).

The report writing phase entailed writing a draft report, conducting an exit conference, providing a formal draft report to OIG for review, and preparing and issuing the final report.

III. RESULTS

Feedback is critical to the success of any project. Timely and targeted feedback can enable project managers to identify problems early and make adjustments that can keep a project on time and on budget. In addition, early identification of cost and schedule variance information is needed by agency executives to monitor and control risks within its investment portfolio. Earned Value Management (EVM) has proven to be one of the most effective performance measurement and feedback tools for managing projects. EVM provides organizations with the methodology needed to integrate the management of project scope, schedule, and cost.[6]

Cost data on security spending is necessary to help ensure IT investments have adequately identified and budgeted for security in a federal IT investment.

In the following section of the report, we provide the results of our performance audit across the following sections: Earned Value Management (EVM) Governance; EVM Tools & Technology; EVM Implementation & Performance. In addition, we provide the results of our performance audit within the sections Security Cost Governance and Security Cost Estimating, Analysis and Reporting.

EVM Governance

EVM Governance consists of the policies, procedures and practices in place to establish requirements for EVM implementation and performance management within project and program management practices. The Office of the Secretary of Transportation (OST) is responsible for providing this guidance to the operational administrations (OAs), (i.e., modes), with the exception of the Federal Aviation Administration (FAA), discussed further below. The FAA has created its own policy and guidance for EVM.

OST EVM Policy
The Department of Transportation (DOT) EVM Policy was made effective on January 14, 2008. This version of the policy (i.e., first phase of implementation) is to be exclusively applied to IT projects and programs and only to work performed under contract. Management represents that future policy updates will broaden the scope to include all DOT programs and work performed by both federal employees as well as contractors.

[6] *Project Management Institute (PMI) Standard for Earned Value Management, 2005.*

The degree to which EVM is applied to IT investments will vary depending on the size and complexity of the IT investment, as depicted in Table 4 below:

Table 4: DOT EVM Requirements

Investment Tier	Total Contract Value	Description
Tier I	≥ $20M	IT investments with total development, modernization and enhancement (DME) life-cycle acquisition costs equal to or greater than $20 million and/or those on the OMB High Risk List. Tier I investments must implement an EVMS that fully complies with American National Standard ANSI/EIA Standard 748 EVMS Guidelines.
Tier II	≥ $3M < $20M	IT Investments with total DME life-cycle acquisition costs equal to or greater than $3 million but less than $20 million (excluding level of effort tasks). Tier II investments must apply EVM principles for tracking investment cost, schedule, and technical performance but need only comply with a subset of ANSI/EIA Standard 748 Guidelines, as detailed in the DOT EVM Implementation Guide.
Tier III	< $3M	IT investments with total DME life-cycle acquisition costs of less than $3 million (excluding level of effort tasks). Tier III investments must apply EVM principles to track investment cost, schedule and technical performance, but are not required to comply with the ANSI/EIA 748 Guidelines. The extent to which EVM is required for each Tier III investment is determined by the risk, dollar amount, and complexity of the investment, as detailed in the DOT EVM Implementation Guide.

Additional DOT EVM policy requirements include:

- EVM is to be applied to contractor work, regardless of contract type.
- Where applicable, EVM requirements must be clearly indicated in the investment's solicitation and the resulting contract. The Contracting Officer (CO) shall insert requirements provided by the Program Manager (PM) or Contracting Officer's Technical Representative (COTR) into the contract for Integrated Baseline Reviews (IBR's)[7] for Tier I and Tier II investments, and for Tier III investments, as deemed necessary by the Contracting Officer and Program/Project Manager. The Contract Data Requirements List (CDRL) must provide that EVM data for these investments be submitted via the Contractor Performance Report (CPR).
- EVM implementation shall be consistent with all DOT IT Governance processes and related procedures.
- Waivers to this policy are to be submitted by the Program Manager (PM)/CO in writing to the OA CIO, prior to submission to DOT CIO for approval. Processing of waivers will be detailed in the to-be released DOT EVM Implementation Guide[8]. Grant of waivers in no way implies exemption from sound and rigorous management practices, or from continuous monitoring of program/project cost, schedule, and technical performance.

While the DOT policy contains these requirements, it does not address certain other EVM considerations. For example, the policy does not include provisions related to assigning work elements to Federal employees; does not contain provisions for training, integration with portfolio management, and the use of templates and tools; does not require the FAA to follow the policy even though FAA's EVM policy requirements are more stringent and are accompanied by EVM implementation guidance; and the EVM implementation guidance referenced throughout the DOT EVM policy has not yet been created nor

[7] An Integrated Baseline Review (IBR) refers to a government-led review that is intended to ensure the government and contractor mutually understand program scope, schedule, resources, inherent risk, and management approach, and to ensure early and adequate planning. *Source: DOT EVM Policy dated January 18, 2008.*

[8] After fieldwork concluded, management informed us that the DOT Implementation Guide was discontinued in June 2008 in favor of a more robust and detailed EVM policy. We were not informed of the discontinued effort, nor were we provided with the updated EVM policy.

promulgated to assist the OAs and major investments. We have included this weakness in the Findings section of this report.

Additionally, OST management has not implemented standards to support an enterprise approach for managing and applying EVM across the modes. This includes the promotion of standards for articulating and capturing project scope and work assignments and enforcing this through the IBR, decomposing work using a standard work breakdown structures (WBS)[9] for IT development projects, managing concurrent efforts through an Integrated Master Schedule (IMS)[10], guidelines for retaining rebaselining documentation, and conducting EVM training and lessons learned. We have included this weakness in the Findings section of this report.

FAA EVM Policy

The FAA has its own acquisition system known as the Acquisition Management System (AMS), which establishes the FAA's acquisition policy. In 2005, the FAA developed its own EVMS policy and incorporated it into the AMS. The key requirements of the policy include:

- Contractor EVM implementation must be consistent with the program's acquisition strategy. All capital investment programs must use table 5 to determine the application of EVM to the DME[11] work assigned to contractors. The requirements apply to all contract types. On an exception basis, low-risk contractor efforts, i.e., firm fixed price production, may implement EVM within a FAA program office at the program level. Contractor EVM implementation must be based on an assessment of the cost, schedule, and technical performance risk of each contract.

Table 5: FAA Contract EVMS Requirements

EVMS Requirements	Total Contract Value ($M) >$10	Total Contract Value ($M) <$10
Contract Performance Report	R	O
Integrated Master Schedule	R	O
Integrated Baseline Reviews	R	O
EVMS Standard Compliance	R	O
EVM System Certification	R	O

Notes:
R = Required by approving authority
O = Optional

- Capital investment programs required to use an EVMS must be certified as meeting the guidelines of ANSI/EIA-748. The EVM Focal Point assesses and validates EVM implementation and monitors application to ensure compliance. The AIO Value Management Office certifies program EVM systems. FAA contractors required to use an EVM system must be certified as meeting the guidelines of ANSI/EIA-748. Contractor EVM implementation must be validated by the Contracting Officer, assisted by the EVM Focal Point. The EVM Focal Point determines whether a contractor requires an EVMS certification review or whether an existing certification and EVM surveillance

[9] A Work Breakdown Structure (WBS) is a deliverable-oriented hierarchical decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables. *Source: PMBOK Guide – Third Edition.*
[10] An Integrated Master Schedule refers to a multilayered schedule showing all the detailed tasks required to accomplish the work effort contained with a set of projects or program(s). *Source: Defense Acquisition Guidebook.*
[11] Development, Modernization and Enhancement (DME) means the project cost for new investment, changes or modifications to existing systems to improve capability or performance, changes mandated by the Congress or agency leadership, personnel costs for investment management, and direct support. For major IT investments, this amount should equal the sum of amounts reported for planning and acquisition in the Exhibit 300. *Source: DOT EVM Policy dated January 18, 2008.*

process are acceptable. The EVM Focal Point will establish agreements with other government agencies to recognize contractor EVM certifications and surveillance reports.

The FAA has also issued an EVM Implementation Guide dated February 2006 that addresses EVM implementation on FAA programs, FAA contracts, and EVM certification and surveillance. FAA programs are to apply EVM methodologies to the total program effort, including both government and contractor work, to better manage complex, high-risk, high-cost, or high-visibility efforts. FAA programs may utilize multiple sources to accomplish the work of the program and commonly assign work to the following performing organizations that must be included in the EVMS as depicted in Table 6:

Table 6: EVMS methodologies for organizations

Performing Organization	EVMS consideration
Government Organizations:	Government organizations and personnel (Full-Time Equivalents – FTEs), while commonly used to perform program management and oversight, may also perform engineering, testing, deployment, and logistics support functions. All work and program activities performed by government personnel are assigned using the program baseline work breakdown structure (WBS) and are managed using EVM. FAA programs required to use EVM must include resources for all government DME effort included in the JRC-approved program baseline.
Major Contractors	Major contractors commonly are employed in the areas of design, engineering, development, deployment, and support functions. All work and program activities performed by major contractors are assigned using the program baseline WBS and are managed using EVM. FAA programs required to use EVM must include resources for all major contractor effort included in the JRC-approved program baseline. When a program awards a contract greater than $10M for development, modernization, and enhancement work, the contract effort is managed by an EVMS. A Contractor Performance Report (CPR) and Integrated Master Schedule (IMS) are obtained consistent with the JRC-approved OMB-300. These reports may be tailored and customized in accordance with their respective Data Item Descriptions (DID), specific program risks, and performance measurement metrics/reports included in the OMB-300. The contractually required EVMS used by each contractor must meet the guidelines in American National Standard ANSI/EIA-748 and be certified.
Support Contractors	Support contractors commonly perform support roles in one or more areas of program management, engineering, configuration management, test, and logistics. All work and program activities performed by support contractors are assigned using the program baseline WBS and are managed using EVM. FAA programs required to use EVM must include resources for all support contractor effort included in the JRC-approved program baseline. Implementation of EVM on support contractor effort must be consistent with AMS Earned Value Management policy.
Small contracts and subcontracts	When a program awards a contract less than $10M for DME work, the contract may be managed using an EVMS following the optional policy guidelines outlined in AMS. A CPR and IMS are optional requirements on the contract. IBRs may be performed to ensure planning is adequate. The EVMS, if required, should follow the guidelines of American National Standard ANSI/EIA-748, and a certification of the EVMS may be required.

The FAA also requires the use of a standard lifecycle WBS. The use of EVMS during the planning phases (WBS 1.0 and 2.0) is considered by FAA management to be a best practice when the work involves prototyping or testing software. EVM is used during the solution development phase (WBS 3.0), solution implementation phase (WBS 4.0), and in service management phase activities (WBS 5.0). The FAA also has provided guidance on program management practices such as Quality Assurance for Program Management, Measurement and Analysis, Evaluation (Verification), Requirements, Risk Management, Program Management, and Contractor Management.

EVM Tools and Technology

EVM tools consist of the tools used to create and manage the cost and schedule of projects, including those for developing WBS elements, tracking the completion of project activities, and performing EVM related calculations (e.g., cost variance (CV), cost performance index (CPI), schedule variance (SV), schedule performance index (SPI)). Currently, there are no prescribed or standard tools selected by OST for managing projects, performing project level EVM calculations or reporting EVM data.

Across the OAs, management informed us that each project is managed differently and the tools used to report EVM data may also differ for the IT investments. For the majority, the modes and investments use Microsoft Excel to calculate or report the EVM data and the project WBS and schedule of activities are managed within Microsoft Project or, with the case of FAA, Primavera. A breakdown of the various tools used to report project information and EVM data is included in Table 7 below.

Table 7: EVM tools and technology across modes and IT investments

Mode or (Investment)	EVM calculations/reporting (project level)	EVM portfolio reporting	Schedule / WBS
FAA (ATOP) (ATM/TFM) (ASOS/AWOS) FAA (TAMR)	MS Excel Primavera	eCPIC / Worklenz (FY2009)	MS Project Primavera
OST	MS Excel	eCPIC / Worklenz (FY2009)	MS Project
FHWA, NHTSA, MARAD, FRA, RITA, PHMSA (SMART)	MS Excel	eCPIC	MS Project
FMCSA (FMCSA Modernization)	MS Excel	eCPIC	MS Project MS Excel

According to OA management, for the EVM data being reported through MS Excel, controls to prevent unauthorized changes to these tools have not been identified to protect the EVM data validity or integrity. We have included this weakness in the Findings section of this report.

EVM Implementation and Performance

The effective use of EVM requires that it is used on projects where the principles of good project management are being applied. Project management is primarily a matter of planning and controlling work.[12] EVM considerations through each project include the following:

Project Process – Planning

- *Standard EVMS requirements exist in contracts for major investments* - This consideration helps ensure that applicable contractor statements of work (SOW) include EVM policy requirements. This is a requirement by the Office of Management and Budget (OMB).
- *EVMS system certification should be performed for major investments* – This consideration helps ensure that the EVMS being used by the contractor has been thoroughly evaluated by the government and adheres to requirements established in relevant policies and SOW (e.g., ANSI/EIA 748). This is a requirement by OMB.
- *Standard work breakdown structure (WBS) and practices are used for major investments* – This consideration helps ensure that a consistent and repeatable manner is used to decompose work, estimate resource requirements for project work elements, estimate project activity duration and sequencing, establish EVM credit techniques, and assign work elements within the WBS through

- the use of Organizational Breakdown Structures (OBS)[13] and Responsibility Assignment Matrices (RAM)[14]. This is considered a leading practice but is not a requirement.

[12] *Project Management Institute (PMI) Standard for Earned Value Management, 2005.*

[13] An Organizational Breakdown Structure (OBS) depicts the organization hierarchy, allowing the project's work packages to be related to be performing organizational units. *Source: PMI's Practice Standard for Work Breakdown Structures, 2nd edition.*

Project Process – Controlling

- *EVMS system surveillance should be used for contractors managing EVMS for major investments* –This consideration helps ensure that the EVMS being used by contractors, through EVM reporting and periodic evaluation, continue to meet EVMS certification and SOW requirements. This is a requirement by OMB.

- *EVMS is analyzed minimally monthly in accordance with OST's requirement* - This consideration helps ensure that EVM data is being evaluated on a consistent monthly basis, per OST requirements. This is considered a leading practice but is not a requirement.

As noted above, these EVM implementation and performance practices either are required by OMB policy, DOT policy, or are related to industry-based practices. We evaluated these EVM related attributes across each mode and IT investment in order to verify the implementation and performance is contained in Table 8 below.

[14] A Responsibility Assignment Matrix (RAM) is a structure that relates the project OBS to the WBS to help ensure that each component on the project's scope of work is assigned to a responsible person/team. *Source: PMI's Practice Standard for Work Breakdown Structures, 2nd edition.*

Table 8: EVMS Implementation & Performance Management by Mode/Investments [15]

Project Processes	Planning			Controlling	
Mode / EVM attribute	Standard EVMS contract language required for majors (Y/N)	EVMS system certification required (Y/N)	Standard WBS for major investments (Y/N)	EVMS contractor surveillance required (Y/N)	EVMS analysis frequency
FAA	Y	Y	Y	Y	Monthly
OST	Y	N	N	N	Monthly
FMCSA	Y	N	Y	N	Monthly
NHTSA	N	N	Y	N	Quarterly
PHMSA	N	N	N	N	Monthly
IT investment / EVM attribute	**Standard EVMS contract language for majors (Y/N)**	**EVMS system certification required (Y/N)**	**Standard WBS for major investments (Y/N)**	**EVMS contractor surveillance required (Y/N)**	**EVMS analysis frequency**
FAA (TAMR)	Y	N	Y	Y	Monthly
FAA (ASOS/AWOS)	N	N	Y	Y	Monthly
FAA (ATOP)	N	Y	Y	N	Monthly
FAA (ATM/TFM)	Y	Y	Y	N	Monthly
PHMSA (SMART)	N	N	N	N	Monthly
FMCSA (FMCSA Modernization)	N	N	Y	N	Monthly

This analysis indicates that the modes and investments are inconsistently applying EVMS implementation and performance practices. With regard to the modes,

- PHMSA, and NHTSA did not fully specify standard EVMS contract language for investments;
- OST, NHTSA, FMCSA, and PHMSA did not fully enforce EVMS certification over contractor operated EVMS;
- OST and PHMSA do not use a standard WBS for major IT investments;
-

[15] FHWA and FTA management represents that for their mode, major investment(s) are in a steady state other than development, modernization or enhancement (DME) and do not require EVM; therefore the EVMS attributes listed in table 8 above currently are not in place. FRA and RITA management represents that EVMS is not currently required based on the investment tier of their major investments as required in the DOT EVM policy. Finally, MARAD management represents that there are no major investments currently in their portfolio; therefore, EVMS is not required.

- OST, NHTSA, FMCSA, and PHMSA did not fully implement EVMS contractor surveillance practices;
- NHTSA EVMS reporting frequency is not being performed monthly, as prescribed by OST.

For the investments we analyzed,

- ASOS/AWOS, ATOP, SMART and FMCSA Modernization IT investments did not fully specify standard EVMS contractor language. For example,
  - In the IAA with the National Weather Service (NWS), the ASOS/AWOS program does not contain any provisions for EVMS or the data required to be collected in order to support FAA EVMS measurements.
  - For contract line item number (CLIN) 7270, several ATOP statements of work do not contain EVMS reporting requirements. While EVMS was not required in the statements of work, EVMS is a requirement in the prime contract.
  - In the Inter-Agency Agreement (IAA) with the Volpe Center for the SMART investment, EVMS reporting requirements are unclear such as what EVM metrics are to be collected and at what level of the project; what earned value credit techniques are to be used; what reporting formats are to be used.
  - For the FMCSA Modernization investment, the SOW does not contain requirements for EVMS to be certified, be subject to surveillance, or consideration for EVM metrics and EVM credit techniques.
- TAMR, ASOS/AWOS, SMART and FMCSA Modernization IT investments did not fully enforce EVMS certification. For example,
  - While the EVMS for the contractor (Raytheon) for TAMR was DCMA certified on January 28, 2008, the FAA has not evaluated/audited the contractors EVMS specific to the STARS contracts which includes TAMR nor have they fully accepted the DCMA validation.
  - The ASOS/AWOS contractors EVMS is not certified. The contract was awarded prior to the FAA Acquisition Management Policy requirement for contractor EVMS certification in 2005. In addition, ASOS/AWOS had prepared a Plan of Action and Milestones (POAMs) to improve EVM processes and procedures identified through surveillance activities to achieve EVM compliancy; however, the implementation plan has not been developed.
  - The SMART investment contractor's (i.e., the Volpe Center within DOT) EVMS has not been certified consistent with ANSI standards, nor are their SOW requirements for this to occur.
  - The FMCSA Modernization EVMS has not been certified.
- SMART has not fully considered the use of a standard WBS.
- ATOP, ATM/TFM, SMART and FMCSA Modernization IT investments did not fully implement EVMS surveillance. For example,
  - EVMS reporting requirements have not been prescribed by the ATOP program for their prime contractor. Reporting requirements have continued to emerge as the projects continues to run.
  - Management represents that, although standard reporting is used for the ATM/TFM investment, SMART investment and FMCSA Modernization investment, EVMS surveillance is not occurring to help ensure the EVMS continues to meet required standards (e.g., ANSI/EIA STD 748).

These weaknesses have been included in the Findings section of this report.

Governance for Estimating, Analyzing and Reporting Security Costs

OST is responsible for providing policies and procedures over the modes for estimating, analyzing and reporting IT security costs. According to OST, there are no specific policies or procedures in place for estimating, tracking and reporting security costs. This includes provisions for distributing resources based on assessed risks; provisions for using risk analysis, earned value and return on investment to determine which security controls should be funded and implemented; provisions for linking information security expenditures to the strategy and mission of the program; provisions for linking the security costs to OMB A-11 categories; and provisions for developing a performance plan that addresses security resources including budget, staffing and training. This weakness is included in the Findings section of this report. In 2003, OST provided the Cost Estimating Tool for Information Security (CETIS) for use by all OAs; however, management represents that the figure being estimated by the tool was above any historical estimates, so the tool was discontinued because OST would not approve the requested amounts. Subsequently, the OAs used a fixed percentage to represent estimated security costs; however, all of the OAs requested the same percentage.

Across the modes, management represents that historical information and a risk-based approach to addressing security weaknesses are being used to estimate security costs. The major IT investments follow the modes methods for estimating security costs (i.e., TAMR, ASOS/AWOS, ATOP and ATM/TFM follow FAA, SMART follows PHMSA, and FMCSA Modernization follows FMCSA). These security costs are funded through the investment that has to address security weakness, are centrally funded through the program office if they are broader scope security costs, or a combination of the both. Table 9 contains a summary of how management represents each mode is reporting their security costs as (A) embedded into project budgets, (B) funded separately, or (C) both.

Table 9: Security Cost Estimating and Reporting by Mode

Mode/Investment	Policy for developing security estimates? (Y/N)	Security related costs	(A) Security embedded in projects (B) Security funded separately (C) Both
OST *Major Investment:* IT Combined Infrastructure	N	*Mode-level:* Security awareness training, privacy training, and FISMA reporting tool use (i.e., DOJ's CSAM). Funds are requested by OST from the OAs for these services. *Major Investments:* The cost of activities associated with certification and accreditation, risk assessment, and risk mitigation.	C *Major investment:* System POA&Ms go with the investment
FAA *Major Investment(s):* TAMR, ATM/TFM, ATOP, ASOS/AWOS	N	Each individual investment team manages security costs as part of the entire program's life-cycle cost. Specific costs include, among others, as appropriate: • Risk assessment • Certification and accreditation • Specific security controls • Authentication or cryptographic applications • Education, awareness, and training • Contingency planning and testing • Physical controls for hardware and software	C *Major investment (s):* System POA&Ms go with the investment
FMCSA *Major Investment:* FMCSA Modernization	N	Government FTEs in IT Security; contractors supporting IT Security; WBS items in EVM systems that align with the WBS dictionary for IT Security.	C *Major investment (s):* System POA&Ms go with the investment
FTA	N	(Security) The cyclical schedule for security " Certification and Accreditation"; data encryption requirements; compliance with HSPD-12, compliance with E-Authentication standards; and corrective actions based on IG, GAO, C&A, FMFIA audits are inputs to security costs for an Information Technology Investment.	C System POA&Ms go with the investment
FHWA	N	Operational Cost, to maintain security controls costs and to comply with FISMA (NIST SP-800-53 annual control testing, annual DR testing, security plan review, etc.). It also depends on other annual DOT and OMB requirements.	C System POA&Ms go with the investment
RITA	N	The cost of activities associated with certification and accreditation, risk assessment, and risk mitigation.	B Most security costs are borne at the RITA CIO level and not embedded in the project budgets.
FRA	N	FRA develops cost estimations based on historical information for the program, remediation's required (if any) and economies of scale for shared components.	C System POA&Ms go with the investment.
PHMSA *Major Investment:* SMART	N	PHMSA PMs work with the ISSO and CIO team to help ensure security costs are funded. This includes C&A activities and completing POA&Ms.	A *Major Investment:* System POA&Ms go with the investment.
NHTSA	N	Risk assessments performed in eRAMS identify risks that map to individual 800-53 security controls which are in turn evaluated for mitigation potential, to include costs.	C System POA&Ms go with the investment typically
MARAD	N	Security and Privacy issues are addressed. A privacy impact assessment is provided when applicable, and certification and accreditation is conducted for all IT systems.	C Security is included within projects. Currently C&A efforts are funded separately.

From a policy standpoint, OST management represents that this is an area that needs greater attention. Management represents that they have started evaluating security costs across the IT investment portfolio to begin gaining an understanding around what types of security areas are costing the agency the most money. For example, during this fiscal year (FY), management has started to evaluate the security costs over the IT portfolio and have potentially identified certification and accreditation (C&A) activities as one of the most expensive items related to IT security. As a result, management has represented that they would consider reengineering the C&A process and promulgating these requirements to the modes with the goal of creating a streamlined and consistent approach to performing C&A activities which should provide a more predictable measure of security costs for estimating. In addition, management is considering collecting and estimating security costs across a common reporting format to be based on the NIST SP 800-53 control categories. Management believes this reporting format will provide insight into what security costs represent opportunities to improve the process of estimating security costs and refining security related policy.

With regard to the IT Combined Infrastructure investment, the investment is a mixed lifecycle investment that aggregates DOT IT infrastructure and office automation expenditures into a single Exhibit 300 submission to OMB. There are currently 43 investments from 12 subordinate administrations (see Table 10) that contribute to this consolidated investment. This includes 12 investments, which account for subordinate Operating Administration participation in the DOT Common Operating Environment and their investment in Common IT Services that are available across the Department. This investment also includes alternative criteria and performance results of the IT consolidation activities and steady state operations of the newly established DOT Consolidated Operating Environment (COE) as well as FAA IT consolidation and cost containment efforts. The investment also includes planning activities for the extension of the COE to DOT field sites (excluding FAA). The investment excludes infrastructure telecommunications services that is considered mission specific.

For the 12 COE investments, these security costs are funded through the Working Capital Fund (WCF). These investments are represented as “Common IT Services” in the table below. Management represents that current security-related expenditures for the 12 represented OST security investments include:

1. A cost center named “Information Assurance and Privacy” that includes the associated costs of an Interagency agreement (IAA) with FAA to support the Cyber Security Management Center (CSMC), FISMA training and reporting, and contractor support and HSPD-12 costs.
2. Network security costs are included in the “Campus Area Network”. This includes Security Operations Center personnel as well as software and hardware security-related purchases.
3. There are security costs for messaging that are in “Directory and Messaging Services”. This is for software and appliances to protect against spam and viruses.
4. The cost center “Enterprise network operations Center” includes personnel who operate the Network Operations Center.

In FY2010, the IT Combined Infrastructure has requested approximately $43M in funding, 21% of which represents IT security costs. Table 10 below contains the breakdown of the IT security costs for each of the 43 investments.

Table 10: IT Combined Infrastructure security spend by mode

Mode/Investment Name	IT Security dollars requested	Total Investment budget	% IT security of the total investment request	% IT Security of the IT Combined Investment	Total # of representative investments
OST	**$ 2,047,062.40**	**$ 9,185,000.00**	**22.29**	**4.74%**	**4**
OSTXX777 Common IT Services (CONSOLIDATED WITH DOTXX070)	*$ 1,062,062.40*	*$ 6,928,000.00*	*15.33*		
OSTXX041 - Logical Access Capability (CONSOLIDATED WITH DOTXX070)	$957,000	$ 957,000.00	100		
OSTXX043 – Cyber Security Management Center (CSMC) (CONSOLIDATED WITH DOTXX070)	$ 28,000.00	$ 28,000.00	100		
WCFXX011: Departmental Print services(CONSOLIDATED WITH DOTXX070)	$0.00	$ 1,272,000.00	0		
FAA	**$ 37,327,222.80**	**$ 105,454,000.00**	**35.4**	**86.37%**	**13**
FAAXX777: Common IT Services (CONSOLIDATED WITH DOTXX070)	*$879,912.80*	*$9,272,000*	*9.49*		
FAAXX101: FAA ELECTRONIC MAIL [ATO AN014] (CONSOLIDATED WITH DOTXX070)	$ 643,500.00	$ 12,870,000.00	5		
FAAXX199: ATO Workstations [ATO AN018 AN029 AN033] (CONSOLIDATED WITH DOTXX070)	$ 1,779,800.00	$ 35,596,000.00	5		
FAAXX202: AHR OFFICE AUTOMATION (CONSOLIDATED WITH DOTXX070)	$ 17,360.00	$ 868,000.00	2		
XX220: LAN SUPPORT FOR THE ASSOCIATE ADMINISTRATOR FOR COMMERCIAL SPACE TRANSPORTATION (CONSOLIDATED WITH DOTXX070)	$60,000	$600,000	10		

Mode/Investment Name	IT Security dollars requested	Total Investment budget	% IT security of the total investment request	% IT Security of the IT Combined Investment	Total # of representative investments
FAAXX231: ABA Operations and Infrastructure (CONSOLIDATED WITH DOTXX070)	$75,200	$1,504,000	5		
FAAXX261: ARP LAN (CONSOLIDATED WITH DOTXX070)	$3,800	$190,000	2		
FAAXX298: Information Systems Security Program (CONSOLIDATED WITH DOTXX070)	$ 33,600,000	$ 33,600,000	100		
FAAXX375: Aeronautical Center Office Automation Support (CONSOLIDATED WITH DOTXX070)	$ 68,274	$ 3,793,000	1.8		
FAAXX409: Aeronautical Center Infrastructure Modernization (CONSOLIDATED WITH DOTXX070)	$95,040	$1,584,000	6		
FAAXX464: CMEL LAN/WAN Office Automation (CONSOLIDATED WITH DOTXX070)	$4,760	$238,000	2		
FAAXX620: ASH Infrastructure (CONSOLIDATED WITH DOTXX070)	$0.00	$ 1,190,000	0		
FAAXX700: ARC Information Technology Infrastructure (CONSOLIDATED WITH DOTXX070)	$99,576	$4,149,000	2.4		
FHWA	**$ 1,791,242.40**	**$ 34,751,000.00**	**5.15**	**4.14%**	**4**
FHWAX777: Common IT Services (CONSOLIDATED WITH DOTXX070)	*$76,982.40*	*$7,776,000*	*.99*		

Mode/Investment Name	IT Security dollars requested	Total Investment budget	% IT security of the total investment request	% IT Security of the IT Combined Investment	Total # of representative investments
FHWAX034: User Profile and Access Control System (UPACS) (Consolidated with DOTXX070)	$933,000	$933,000	100		
FHWAX036: FHWA Web Development and Support Services (Consolidated with DOTXX070)	$105,660	$3,522,000	3		
FHWAX040: FHWA IT Infrastructure Initiatives (Consolidated with DOTXX070)	$675,600	$22,520,000	3		
PHMSA	**$47,490.50**	**$3,910,000**	**1.21**	**.11%**	**2**
PHMSA777 Common IT Services (CONSOLIDATED WITH DOTXX070)	*$11,140.50*	*$3,183,000*	*.35*		
PHMSA011: OFFICE AUTOMATION FOR ADMINISTRATIVE SYSTEMS SUPPORT (CONSOLIDATED WITH DOTXX070)	$36,350	$727,000	5		
FMCSA	**$260,142.20**	**$6,907,000**	**3.77**	**.6%**	**2**
FMCSA777: Common IT Services (CONSOLIDATED WITH DOTXX070)	*$35,142,20*	*$2,407,000*	*1.46*		
FMCSA011: Field IT Infrastructure (CONSOLIDATED WITH DOTXX070)	$225,000	$4,500,000	5		
STB STBXX003: LOCAL AREA NETWORK (CONSOLIDATED WITH DOTXX070)	**$0.00**	**$934,000**	**0**	**0%**	**1**
MARAD	**$59,721.00**	**$8,622,000**	**.69**	**.14%**	**2**
MARAD777 Common IT Services (CONSOLIDATED WITH DOTXX070)	*$20,361.00*	*$3,702,000*	*.55*		

Mode/Investment Name	IT Security dollars requested	Total Investment budget	% IT security of the total investment request	% IT Security of the IT Combined Investment	Total # of representative investments
MARAD015: Operating Environment (CONSOLIDATED WITH DOTXX070)	$39,360.00	$4,920,000	.8		
SLSDC *SLSDC777 Common IT Services (CONSOLIDATED WITH DOTXX070)*	***$1,899.70***	***$157,000.00***	***1.21***	***.004%***	**1**
FRA	**$728,381.20**	**$4,936,000**	**14.76**	**1.69%**	**3**
FRAXX777 Common IT Services (CONSOLIDATED WITH DOTXX070)	*$28,381.20*	*$4,236,000.00*	***.67***		
FRAXX022: Infrastructure-General Hardware/Software Support (CONSOLIDATED WITH DOTXX070)	**$0**	**$0**	**0**		
FRAXX304: Infrastructure-Information Technology Security Program (CONSOLIDATED WITH DOTXXO70)	$700,000	$700,000	100		
FTA	**$461,776.80**	**$8,271,000.00**	**5.58**	**1.07%**	**3**
FTAXX777 Common IT Services (consolidated with DOTXX070)	*$12,076.80*	*$3,774,000.00*	*.32*		
FTAXX002: FTA-COE/ Infrastructure (consolidated with DOTXX070)- was General Support System	$276,900.00	$2,769,000.00	10		
FTAXX022: FTA - Voice, Data & Wireless Communications (breakout of FTAxx002) (consolidated with DOTXX070)	$172,800.00	$1,728,000.00	10		

Mode/Investment Name	IT Security dollars requested	Total Investment budget	% IT security of the total investment request	% IT Security of the IT Combined Investment	Total # of representative investments
RITA	**$355,038.80**	**$12,013,300.00**	**2.96**	**.82%**	**3**
RITAX777: Common IT Services (consolidated with DOTXX070)	*$17,173.00*	*$5,922,000.00*	*.29*		
RITAX013: Volpe ADP Institutional Support Services Contract (AISSC) (previously RSPAX010; consolidated with DOTXX070)	$300,865.00	$6,017,300.00	5		
RITAX016: IT Support for Transportation Safety Institute (consolidated with DOTXX070)	$37,000.00	$74,000.00	50		
NHTSA	**$60,149.80**	**$5,993,000.00**	**1**	**.14%**	**2**
NHTSA777 Common IT Services (consolidated with DOTXX070)	*$28,549.80*	*$5,598,000*	*.51*		
NHTSA008: VEHICLE RESEARCH AND TEST CENTER (VRTC) COMPUTER SYSTEM (consolidated with DOTXX070)	$31,600.00	$395,000.00	**8**		
OIG	**$79,910.00**	**$1,199,000.00**	**6.66**	**.18%**	**3**
OIGXX777 Common IT Services (consolidated with DOTXX070)	*$7,910.00*	*$799,000.00*	*.99*		
OIGXX001: Transportation Inspector General Reporting (TIGR) (consolidated with DOTXX070)	$0.00	$0.00	0		
OIGXX002 OIG General Support/Maintenance of Network, ADP Hardware and Software (consolidated with DOTXXO70)	$72,000.00	$400,000.00	18		
GRAND TOTALS	**$43,220,037.70**	**$202,332,300.00**	**21.36%**	**100%**	**43**

Of the $43,220,037.70 in security costs for the IT Combined Infrastructure investment, the common IT services represent $2,146,449.60 or approximately 5%. The remaining $41,073,588.10 represents the remainder of the investment.

Because DOT has not provided guidance on estimating IT security costs, the security estimates are being self-reported by the OAs and do not follow any consistent, predictable methodology from which future projections can be based by OST. In addition, there is no accountability over the reasonableness of the estimates provided by the OAs that represent the investments that are not related to the common operating environment. Finally, the security costs for the common IT services do not follow a consistent methodology that provides a reasonable estimate of future security costs based on the services rendered as the subordinate investments are migrated to the common operating environment. This weakness is noted in the Findings and Recommendations section this report.

IV. FINDINGS and RECOMMENDATIONS

We conducted procedures related to the Earned Value Management (EVM) and security cost estimating policies, procedures and controls in place over certain Department of Transportation (DOT) Operating Administration's (OAs) and major IT investments and have reported our overall findings and recommendations within this report. We performed this performance audit at the Department's headquarters and at the Federal Aviation Administration (FAA) locations in Washington D.C. This performance audit consisted of reviewing applicable policies and procedures, which included interviewing key personnel and reviewing key reports.

The DOT has established an EVM policy that contains pre-established dollar thresholds and guidance for IT investment owners to consider when implementing EVM. In addition, various modes have improved their use of EVMS by establishing supporting materials, such as IT project management and EVM implementation guidance, providing EVM training and conducting EVM lessons learned. While these items help provide a foundation of EVM guidance for modes to follow and investments to use, there are opportunities for improvement to further implement and use EVM to help manage major IT investments. In addition, we identified weaknesses in the security cost estimating process across the modes. Our 2008 performance audit communicates three recommendations related to controls over the reliability of EVMS data, the reasonableness of security cost estimates, and the controls over the implementation and completeness of EVMS. The three findings are further described in the table below. Each finding contains a description of the condition(s) or weaknesses/observations, the cause and effect, the criteria used to support the noted weaknesses/observations, and the recommendation(s).

2008 Notice of Findings and Recommendations

	2008-1: Controls Over the Reliability of EVMS Data Should Be Strengthened	**2008-2: Controls Over the Reasonableness of Security Cost Estimates and Reporting Should Be Strengthened**	**2008-3: Controls Over the Implementation and Use of EVMS In Project Oversight Should Be Strengthened**
Condition	During our review of the EVMS used at the Department of Transportation (DOT), we identified the following exceptions related to the reliability of EVMS data: A. Controls to prevent unauthorized changes to the spreadsheets (i.e., key cells and spreadsheets used to calculate EVM) have not been identified. B. OST has not promoted nor provided standards for estimating project requirements for IT projects. This includes considerations for: • Estimating resource requirements for project work elements • Assigning management	During our review of the security cost reporting practices performed at the Department of Transportation (DOT), we identified the following exceptions: A. There are no DOT specific policies or procedures for estimating, tracking and reporting security costs. This includes: a. Provisions for distributing resources based on assessed risks b. Provisions for using risk analysis, earned value and return on investment to determine which security controls should be funded and implemented	During our review of the implementation and completeness of EVMS practices performed at the Department of Transportation (DOT) we identified the following exceptions: A. The Department of Transportation (DOT) Earned Value Management policy: a. The EVM Implementation Guidance referenced throughout the DOT EVM policy has not yet been created nor promulgated; b. Does not accurately recognize FAA applicability even through FAA's requirements for implementing and using EVM are more stringent and are accompanied by EVM Implementation guidance; and c. Does not contain provisions for

	2008-1: Controls Over the Reliability of EVMS Data Should Be Strengthened	2008-2: Controls Over the Reasonableness of Security Cost Estimates and Reporting Should Be Strengthened	2008-3: Controls Over the Implementation and Use of EVMS In Project Oversight Should Be Strengthened
	resource/using an Organizational Breakdown Structure (OBS) and Responsibility Assignment Matrices (RAM) for control accounts and work elements • Estimating project activity duration and sequencing • Establishing EVM credit techniques, EVM performance analysis and reporting requirements including specific requirements for EVMS certification and surveillance procedure.	c. Provisions for linking information security expenditures to the strategy and mission of the program d. Provisions for linking the security costs to OMB A-11 categories e. Provisions for developing a performance plan that addresses security resources including budget, staffing and training B. Security estimates for the IT Combined Infrastructure are self-reported by the OAs and do not follow any consistent, predictable methodology from which future projections can be based by OST. In addition, there is no accountability over the reasonableness of the estimates provided by the OAs. Lastly, the estimates for the common IT services also do not follow a consistent methodology that provides a reasonable estimate of the future security costs based on the services rendered as the subordinate investments are migrated to the common operating environment.	Training, Integration with Portfolio Management, the use of templates and tools. B. There is no consistent enterprise approach to managing and applying EVM data across modes. C. OST has not promoted nor provided standards for applying EVM in IT projects. This includes considerations for: a. Articulating and capturing project scope and work assignments through integrated baseline reviews b. Decomposing work using a standard work breakdown structures (WBS) for IT development projects (e.g., following a standardized software development lifecycle or SDLC) c. Managing concurrent efforts through an Integrated Master Schedule (IMS) d. EVM rebaselining guidelines and documentation retention requirements e. Conducting EVM training and lessons learned D. There are inconsistent EVMS practices being followed across modes and investments. Specifically, a. Standard contract language for EVMS is not being used for PHMSA and NHTSA modes and the ASOS/AWOS, ATOP, SMART and FMCSA Modernization investments. b. Certain modes and investments have not performed EVMS certification over their EVMS operated by contractors. Specifically the OST, NHTSA, FMCSA, and PHMSA modes and the TAMR, ASOS/AWOS,

	2008-1: Controls Over the Reliability of EVMS Data Should Be Strengthened	2008-2: Controls Over the Reasonableness of Security Cost Estimates and Reporting Should Be Strengthened	2008-3: Controls Over the Implementation and Use of EVMS In Project Oversight Should Be Strengthened
			SMART and FMCSA Modernization investments. c. Inconsistent contractor surveillance of EVMS practices for OST, NHTSA, FMCSA, PHMSA modes and ATOP, TFM, SMART and FMCSA Modernization investments. d. Standard WBS for development activities are not consistently used by PHMSA or the SMART investment. e. EVMS reporting frequency performed quarterly for NHTSA.

	2008-1: Controls Over the Reliability of EVMS Data Should Be Strengthened	2008-2: Controls Over the Reasonableness of Security Cost Estimates and Reporting Should Be Strengthened	2008-3: Controls Over the Implementation and Use of EVMS In Project Oversight Should Be Strengthened
Cause	A. EVM certification and surveillance activities generally do not include specific considerations for protecting EVM data and tools from unauthorized access or changes or for monitoring the accuracy and completeness of EVM data being collected and reported in EVM policy or in contractor statements of work (SOW). B. OST, who has responsibility for coordinating and promulgating EVM requirements, has not had adequate resources dedicated to creating and promulgating EVM requirements.	A, B. OST, who has responsibility for coordinating and promulgating security cost estimating, tracking and reporting requirements, has not had adequate resources dedicated to creating and promulgating these requirements.	A. OST, who has responsibility for coordinating and promulgating EVM requirements, has not had adequate resources dedicated to creating and promulgating EVM requirements. B. There are no DOT requirements to apply an enterprise approach to EVM for projects. C. OST, who has responsibility for coordinating and promulgating EVM requirements, has not had adequate resources dedicated to creating and promulgating EVM requirements. D. OST, who has responsibility for coordinating and promulgating EVM requirements, has not had adequate resources dedicated to creating and promulgating EVM requirements.
Effect	A. Without adequate controls over the tools being used, EVM data being calculated or reported can be altered, intentionally or unintentionally, making EVM data accuracy and reliability questionable. B. Without completed policies, certain provisions may be inconsistently applied.	A, B. Without completed provisions for estimating, analyzing, and reporting security costs, modes are left to estimate costs using self-approved techniques. This may result in security cost estimates that are inefficient, unnecessary or redundant and inconsistent across modes.	A. Without completed policies, certain provisions for using and managing projects using EVM may be incomplete and inconsistently applied for EVM benefits to be obtained. B. DOT may not be recognizing the benefits of consistent and reliable information by leveraging an enterprise approach to implementing EVM in projects. C. Without completed policies, certain provisions may be inconsistently applied. D. Without completed provisions for EVMS standardization and implementation, EVMS may be inconsistently applied across projects requiring its use.

	2008-1: Controls Over the Reliability of EVMS Data Should Be Strengthened	2008-2: Controls Over the Reasonableness of Security Cost Estimates and Reporting Should Be Strengthened	2008-3: Controls Over the Implementation and Use of EVMS In Project Oversight Should Be Strengthened
Criteria	A. *CIO Council A Framework for Developing Earned Value Management Systems (EVMS) Policy for IT Investments, Section 4.2.1 EVM Data Collection*, "The agency EVM policy should outline a systematic way to collect data necessary to support EVM. The agency EVM policy should describe any templates, tools, and systems utilized and additionally provide controls to ensure the data is collected consistently and reliably to inform management decisions. The agency EVM policy should detail any systems used to track data and the process for tracking actual costs at the control account level. The agency EVM policy should additionally address collection of data from both government and contractor resources." A. *Office of Budget Circular A-11, p.9 of section 230 Data Limitations,* "In order to assess the progress towards achievement of performance goals, the performance data must be accurate and reliable. Significant or known data limitations	A, B. OMB Circular A-11, Exhibit 53: "Federal agencies must consider the following criteria to determine security costs for a specific investment: The products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Do not include activities performed or funded by the OIG. When determining the percentage of IT security include the costs of: - Risk assessment; - Security planning and policy; - Certification & Accreditation; - Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security); - Authentication or cryptographic applications; - Education, awareness, and training; - System reviews/evaluations (including security control testing and evaluation); - Oversight or compliance inspections; - Development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment; - Contingency planning and testing; - Physical and environmental controls for hardware and software; - Auditing and monitoring; - Computer security	A. OMB memo M-05-23 Improving Information Technology (IT) Project Planning and Execution, "Full Implementation of EVMS for IT projects includes… comprehensive agency policies." CIO Council A Framework for Developing Earned Value Management Systems (EVMS) Policy for IT Investments, Section 4.2.3 Integration with Portfolio Management, "Agency EVM policy should address the use of EVMS data and analysis to make management and IT portfolio management and Capital Planning and Investment Control (CPIC) decisions (i.e., how and when is performance data received by the agency; who reviews it; is further analysis done; does the agency use a tool to manage the data reported; how is performance information reported to senior management; and what they do with the information)." Section 4.2.4 Training, "Agency EVM policy should outline guidelines on training for program office staff and contractor personnel on the analysis of generated earned value data. Suggestions for training include: formal training classes; contractor-sponsored training; on-the-job training; and training materials, available on performance management websites." Section 4.4 Templates and Tools, "Templates and tools are not a substitute for the establishment and adherence to EVMS processes but can be used to

	2008-1: Controls Over the Reliability of EVMS Data Should Be Strengthened	2008-2: Controls Over the Reasonableness of Security Cost Estimates and Reporting Should Be Strengthened	2008-3: Controls Over the Implementation and Use of EVMS In Project Oversight Should Be Strengthened
	should be identified in the performance plan and include a description of the limitations, the impact it has on goal achievement, and the actions that will be employed to correct the limitations. Performance data need not be perfect to be reliable; however significant data limitations can lead to inaccurate assessments and distort performance results." B. PMI's Earned Value Management (EVM) Practice Standard, "The key practices of EVM include 1) Establishing a performance measurement baseline (PMB) that includes decomposing work scope to a manageable level; assigning unambiguous management responsibility; developing a time-phased budget for each work task; selecting EV measurement techniques for all tasks; maintaining integrity of PMB throughout the project and 2) Measuring and analyzing performance against the baseline that includes record resource usage during project execution; objectively measure the physical work progress; crediting EV according to EV techniques; analyzing and forecasting cost/schedule performance; reporting performance problems and/or take action.	investigations and forensics; and - Reviews, inspections, audits and other evaluations performed on contractor facilities and operations. Other than those costs included above, security costs may also include the products, procedures, and personnel (Federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security, systems administrator functions, and, for example, system upgrades within which new features obviate the need for other standalone security controls."?	assist in the management and reporting of EVMS data. The agency EVM policy should address the development and review of any templates and specify all agency tools used to collect, manage, and report on EVMS data." B. Unknown. C. PMI's Earned Value Management (EVM) Practice Standard "The key practices of EVM include: • Establishing a performance measurement baseline (PMB) that includes decomposing work scope to a manageable level; assigning unambiguous management responsibility; developing a time-phased budget for each work task; selecting EV measurement techniques for all tasks; maintaining integrity of PMB throughout the project. • Measuring and analyzing performance against the baseline that includes record resource usage during project execution; objectively measure the physical work progress; crediting EV according to EV techniques; analyzing and forecasting cost/schedule performance; reporting performance problems and/or take action> "? D. Unknown.

	2008-1: Controls Over the Reliability of EVMS Data Should Be Strengthened	2008-2: Controls Over the Reasonableness of Security Cost Estimates and Reporting Should Be Strengthened	2008-3: Controls Over the Implementation and Use of EVMS In Project Oversight Should Be Strengthened
Recommendation	A. Ensure that controls over the process of collecting and reporting EVM data contain adequate provisions for controlling access and changes to the EVM data. In addition, adequate controls should be included over the analysis and monitoring processes in order to verify the accuracy and completeness of the EVM data. These provisions should be contained in related EVM policy and implementation procedures and in corresponding SOW with contractors. B. Consider incorporating the standards for estimating project requirements as described in the observations and incorporate in the to-be released EVM Implementation Guide.	A, B. Consider incorporating the standards for security budgeting as described in the observations, promulgate and monitor the use of the standards across modes.	A. Evaluate, complete and promulgate the EVM policy and Implementation Guide. B. Evaluate the cost/benefits of leveraging an enterprise technology for managing projects and calculating EVM project level data. C. Consider incorporating the standards for applying EVM in project requirements as described in the observations and incorporate in the to-be released EVM Implementation Guide. D. Consider incorporating the standards for implementing and using EVM as described in the observations and incorporate in the to-be released EVM Implementation Guide.
Applicable Modes	A. FMCSA, PHMSA, FAA B. OST	A. OST B. OST	A. OST B. OST C. OST D.a. PHMSA, NHTSA D.b. OST, NHTSA, FMCSA, PHMSA D.c. OST, NHTSA, FMCSA, PHMSA D.d. OST, PHMSA D.e. NHTSA
Applicable major IT investments	A. FAA (ASOS/AWOS, ATM/TFM, ATOP; PHMSA (SMART); FMCSA (FMCSA Modernization) B. N/A	A. IT Combined Infrastructure B. IT Combined Infrastructure	A. N/A B. N/A C. N/A D.a. FAA (ASOS/AWOS, ATOP); PHMSA (SMART); FMCSA (FMCSA Modernization) D.b. FAA (TAMR, ASOS/AWOS); PHMSA (SMART); FMCSA (FMCSA Modernization) D.c. FAA (ATM/TFM, ATOP); PHMSA (SMART); FMCSA (FMCSA Modernization) D.d. PHMSA (SMART) D.e. N/A

MANAGEMENT RESPONSE TO REPORT

The Office of Inspector General (OIG) will be issuing a separate report for which this performance audit report will be included as an appendix. The Department of Transportation's (DOT) management response, including concurrence or non-concurrence to the findings and recommendations in this performance audit report, will be included as part of the OIG's overall report.

Memorandum

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

Subject: ACTION: Management Response to Office of Inspector General Draft Report, "Quality Control Review of the Department's Implementation of Earned Value Management and Security Cost Reporting."

Date: April 10, 2009

From: Jacquelyn Patillo
Acting Chief Information Officer, DOT

Reply to Attn. of: S-81, x69201

To: Rebecca C. Leng
Assistant Inspector General for Financial and Information Technology Audits

Thank you for providing us with the draft report of your audit, "Quality Control Review of the Department's Implementation of Earned Value Management and Security Cost Reporting." We appreciate the recommendations in your report and will use them to help achieve full compliance with key OMB requirements for Earned Value Management (EVM) implementation.

Recommendation 1. Establish a target date to complete and distribute the DOT EVM implementation guidance to Operating Administrations This guidance should document processes and practices consistent with guidelines published by OMB and address the detailed recommendations included in KPMG's report in Appendix A.

Concur. The Office of the Chief Information Office will issue an expanded DOT Earned Value Management policy and associated guideline no later than September 30, 2009. The DOT EVM policy will include EVM best practices to ensure controls over collecting and reporting EVM data are established, implemented, and monitored. The controls will include techniques for planning, estimating, change control, integrated baseline reviews, reporting, conducting operational analysis and taking corrective actions. The EVM guideline will include the standards, processes, and templates to be used by the DOT Operating

Administrations. The EVM guideline will be developed in accordance with OMB A-11 requirements and in consideration of the recommendations detailed in KPMG's report.

Recommendation 2. Require Operating Administrations to review all major IT investments in the development phase for compliance with key OMB requirements for EVM implementation and report results to the CIO office. Ensure that Operating Administrations establish a target date for correcting deficiencies found.

Concur. Each Operating Administration currently has a POA&M for full implementation of EVM and progress on the actions is reported to the CIO office. DOT has already begun incorporating EVM as a topic of discussion during Investment Review Board meetings. In addition, the DOT Health of the Investment / Program Management Review monitoring and reporting tools are being consolidated to ensure a holistic view of each investment is reviewed and evaluated by DOT senior management. 'This consolidated assessment will be the primary EVM monthly data submission platform, allowing data discrepancies at the investment level to be quickly identified and mitigated and require that operating administrations establish target dates. DOT expects to reach the goal of full compliance with key OMB requirements for EVM implementation by December 2009.

Recommendation 3. Establish security cost estimation standards consistent with the National Institute and Standards and Technology, require Operating Administrations to follow the standards, and verify compliance with the standards by performing a sample review of Operating Administrations' security cost estimate submission.

Concur. DOT's analysis of security cost estimating practices has also shown that while, the Operating Administration are using cost estimating techniques as part of their IT investment processes, they would benefit from greater consistency across organizations. By June 30, 2009, the DOT CIO will issue a guidance document to identify Department wide expectations intended to standardize the Operating Administration security cost estimating techniques to in accordance with National Institute of Standards and Technology Control Families. In order to help ensure compliance with this guidance, by August 30, 2009, DOT will conduct sample reviews to verify that the security cost estimating guidelines are being utilized in preparing the Exhibit 300s for Budget Year 2011.

#