U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Assessment of the SEC Information Technology Investment Process

March 26, 2010
Report No. 466

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 26, 2010

To: Mary L. Schapiro, Chairman
Charles Boucher, Director, Office of Information Technology

From: H. David Kotz, Inspector General, Office of Inspector General (OIG)

Subject: *Assessment of the SEC Information Technology Investment Process,* Report No. 466

This memorandum transmits the U.S. Securities and Exchange Commission, OIG's final report detailing the results of our audit of the Commission's information technology process. This audit was conducted in accordance with our annual audit plan.

Based on written comments received to the draft report and our assessment of the comments, we revised the report accordingly. This report contains nine recommendations to which the Offices of the Chairman and Information Technology concurred with all. Management's full comments to this report are included in the appendices.

Within the next 45 days, please provide OIG with a written corrective action plan that is designed to address the recommendations. The corrective action plan should include information such as the responsible official/point of contact, time frames for completing the required actions, milestone dates identifying how you will address the recommendations cited in this report, etc.

Should you have any questions regarding this report, please do not hesitate to contact me. We appreciate the courtesy and cooperation that you and your staff extended to our auditor.

Attachment

cc: Kayla J. Gillan, Deputy Chief of Staff, Office of the Chairman
Diego Ruiz, Executive Director, Office of the Executive Director
Lewis W. Walker, Deputy Director, Chief Technology Officer, Office of Information Technology

Assessment of the SEC Information Technology Investment Process

Executive Summary

Background. The U.S. Securities and Exchange Commission (SEC or Commission) has established a Capital Planning and Investment Control (CPIC) process and structure for the approval and oversight of Information Technology (IT) investments. The CPIC process provides for the ongoing identification, selection, control, and the evaluation of information resource investments. The process links budget formulation and execution functions, and is focused on the agency's missions and achieving specific program outcomes. Specifically, the CPIC process addresses the decision criteria used in selecting IT investments, as well as the use of defined performance measures in assessing the investment outcomes in implementation and operation.

Objectives. The objectives of the audit were to determine whether the CPIC process and procedures, and the IT investment structure made up of three governing boards: the Project Review Board (PRB), Information Officers Council (IOC), and Information Technology Capital Planning Committee (ITCPC), adhere to governing Commission policy and applicable federal laws and regulations. We also examined whether adequate procedures exist to ensure that major IT investments are properly approved within the process. Lastly, we assessed whether major IT investment projects were properly approved by the appropriate IT board**.**

Prior OIG Audit Report. The OIG issued *IT Capital Investment Decision-Making Follow-up*, Report No. 365, on the IT investment process on March 29, 2004, and the report consisted of 25 recommendations.[1] The report noted that the Commission had made progress in the IT investment area, but found that the Commission's process still did not meet the minimum criteria of the Government Accountability Office's (GAO's) Information Technology Investment Management Maturity Model and was not in full compliance with applicable laws and regulations. The report further found that the SEC's IT investment decision-making process remained a "significant problem" for the Commission, and that the governance of this critical Commission function needed to be strengthened. The OIG recommended that the Commission assign specific responsibility and delegate appropriate authority for establishing a compliant and effective IT decision-making process. The report further recommended that the SEC ensure that the necessary changes were completed in a timely manner by the implementation of a performance accountability process. However, at the time

[1] The audit was conducted as a follow-up to a previous review of the IT capital investment decision-making process. Report No. 334, "IT Decision Making Process," August 28, 2001.

we conducted our audit work for this audit, several recommendations in the prior OIG report were not completely addressed; specifically, the recommendations regarding the publishing of an IOC charter and establishing the Chief Information Officer's (CIO's) authority. As of this date, five years later, we found that the CIO still lacks the necessary authority to manage the CPIC process adequately.

Results. The audit found that several program improvements are needed within the CPIC process regarding the Commission's implementation of its CPIC policies and procedures and the CIO's authority. Specifically, we found that two out of four investments we reviewed in a judgmentally-selected sample did not follow the process prescribed in the CPIC policies and procedures and led to significant decisions being made regarding IT investments without a meaningful review by the appropriate boards. We also found that a lack of effective project management is contributing to the agency's failure to properly manage IT projects.

In addition, we found that the CPIC policies need to be revised to create an enforceable mechanism that divisions and offices within the Commission must follow. Further, based on an OIG survey of IT investments within SEC, we found the need for more direct involvement from the divisions and offices in IT investments.

Finally, we found that the CIO's authority is limited in contravention of pertinent statute and the Office of Management and Budget guidance and, as a result, is not able to manage and oversee the CPIC process adequately.

Summary of Recommendations. This report found significant concerns with the IT investment process and makes 9 specific and concrete recommendations to improve the process.[2]

These recommendations are for the Commission to:

(1) Improve the Office of Information Technology's (OIT) oversight of IT investments to ensure that the requirements in the CPIC policies and procedures are followed.

(2) Require that status updates on all ongoing projects be provided every six months to manage resources for IT investments.

(3) Immediately fill a critical vacant project management position with an experienced and qualified candidate.

(4) Perform an assessment of the project management functions to ensure an appropriate ratio of projects to project managers.

[2] The audit also re-issues and expands upon two OIG recommendations contained in its 2004 report regarding the CIO's position.

(5) Delegate to the CIO authority necessary for the management and oversight of the CPIC process, including full authority to develop and execute all IT policies.

(6) Revise the Code of Federal Regulations to provide the CIO with full authority to develop IT policies.

(7) Revise the SEC's internal regulations to create an enforcement mechanism for the CPIC process.

(8) Conduct periodic internal reviews to ensure that requirements applicable to IT investment management are properly enforced.

(9) Require that all SEC divisions and offices use OIT's project management system, and update and maintain the data in the system for the investments within their program areas.

Table of Contents

Tables

Figure

Background and Objectives

Background

The U.S. Securities and Exchange Commission (SEC or Commission) has established a Capital Planning and Investment Control (CPIC) process and structure for the approval and oversight of Information Technology (IT) investment projects. The primary mission of the CPIC process is to establish a strategic approach as to how the Commission uses its IT funds. It serves as a means of ensuring that the SEC's IT investments achieve specific outcomes. The CPIC process provides for the identification, selection, control, and evaluation of investments in information resources. The process also addresses the decision criterion that is used in selecting IT investments and the use of defined performance measures in assessing an investment's progress.

The process is controlled by three governing boards:

1. Information Technology Capital Planning Committee (ITCPC);
2. Information Officers Council (IOC); and the
3. Project Review Board (PRB).

All projects must be reviewed initially by the PRB and must then be approved by the IOC. Each board has a charter that outlines its role in the IT investment process at various levels within the investment process.

CPIC Boards Roles and Responsibilities. The ITCPC meets quarterly and serves as the highest IT investment body within the CPIC process. Its role is to achieve the SEC's mission and goals, maximize value, manage risk, achieve efficiency and effectiveness, and assign responsibility and accountability. The ITCPC provides strategic direction to the IOC and PRB on executive level selection, control, and evaluation of agency-wide IT investments. The ITCPC is charged with ensuring that the Office of Information Technology (OIT) publishes CPIC policies, procedures, and selection criteria, and will periodically review those materials to ensure they comply with external mandates and effectively support the SEC's decision-making process.

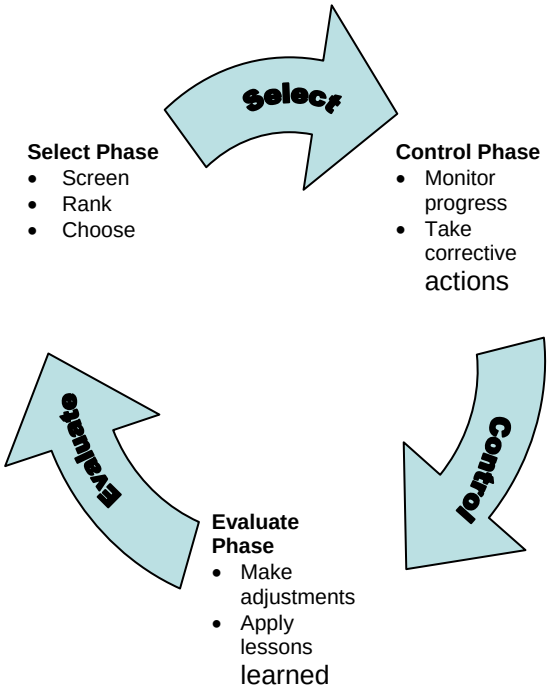
The IOC meets every month and is comprised of senior officers within the Commission. Its primary role is to select and evaluate IT investments that meet the strategic direction of the agency and to provide sound and diverse advice to the Chief Information Officer (CIO) on the Commission's IT portfolio. The IOC is responsible for providing recommendations to the investment sponsor prior to the presentation of the investment proposal and periodically reviewing the results of completed investments. The IOC is also responsible for conducting periodic reviews of the entire IT portfolio and assigns action items to IOC members or OIT

staff for resolution and reporting. The IOC takes different roles with respect to IT investments depending on the cost of the project.

The PRB meets weekly and is charged with ensuring that IT investments are selected, controlled, and evaluated after completion. The PRB is also required to: (a) Ensure the soundness and viability of proposed IT investments prior to selection; (b) Make sure that staff and budget resources for projects are fully planned before, and managed during, project execution; (c) Inform, advise, and make recommendations to the CIO and OIT senior management; and (d) Provide guidance and assistance to project managers to ensure the full scope of each project is completed on time and within budget.

Federal IT Investment Management Model. A central tenet of the federal approach to IT investment management has been the select/control/evaluate model, as illustrated in Figure 1, Fundamental Phases of the IT Investment Approach. The Government Accountability Office (GAO) initially identified this model, which provides a systematic method for agencies to minimize risks while maximizing the returns of investments.[3]

Figure 1: Fundamental Phases of the IT Investment Approach



Source: GAO

[3] GAO-04-394G, GAO Executive Guide, "Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity, Version 1.1, March 2004 at pgs. 7-8.

During the select phase, as noted in Figure 1, the organization (1) identifies and analyzes a project's risks and returns before committing significant funds to a project; and (2) selects those IT projects that will best support the organization's mission needs. This process should be repeated each time funds are allocated to projects, even when reselecting ongoing investments.[4]

During the control phase, the organization ensures that, as a project develops and investment expenditures continue, the project continues to meet the organization's mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems have arisen, steps should be taken quickly to address the deficiencies. If mission needs have changed in the control phrase, the organization is able to adjust its objectives for the project and appropriately modify expected project outcomes.[5]

During the evaluate phase, actual and expected results are compared after a project has been fully implemented. The purpose of this comparison is to (1) assess the project's impact on mission performance, (2) identify any necessary changes or modifications to the project, and (3) revise the investment management process based on lessons learned.[6]

Contracting Officer's Authority. Contracting Officers have the authority to enter into, administer, and terminate contracts. They may bind the Government only to the extent of the authority delegated to them. Contracting Officers receive clear instructions in writing from the appointing authority, regarding of the limits of their authority. Contracting Officers must ensure that no contract is entered into unless all requirements of law, executive orders, regulations, and all other applicable procedures including clearances and approvals, have been met.

Objectives

The objectives of the audit were to examine whether SEC divisions and offices have established procedures to ensure that major IT investments are properly approved by the CPIC boards, specifically, the PRB, IOC and/or the ITCPC. The audit objectives also were to:

- Determine whether the CPIC process and procedures and the PRB, IOC, ITCPC structures adhere to governing Commission policy and applicable federal laws and regulations;

- Examine whether procedures exist to ensure that major IT investments are properly approved within the CPIC process and are presented to the PRB, IOC and/or ITCPC as appropriate; and

[4] Id. at p. 8.
[5] Id.
[6] Id.

- Assess whether major IT investment projects are properly approved by the appropriate CPIC board(s).

Findings and Recommendations

We determined that the SEC has a documented structure, approval process and adequate procedures that adhere to governing Commission policy and applicable federal laws and regulations. We also found that comprehensive procedures are documented for major IT investments, but that the procedures are not consistently followed throughout the Commission. In this audit, we assessed whether major IT investments were properly approved by the appropriate CPIC board and identified some deficiencies and areas of non-compliance. Specifically, we found that although the Commission has established a comprehensive CPIC process and structure for the approval and oversight of IT investments, there are still some areas that should be enhanced. The SEC has gone to great lengths, and expended significant resources to develop an IT CPIC structure, approval process and procedures that adhere to federal laws and regulations. However, the Commission is not adequately implementing all phases of the CPIC process and procedures that are contained in its regulations and implementing instructions. More specifically, we found that:

1) IT investments did not always follow the formalized CPIC process;
2) IT projects were not adequately managed;
3) The CIO's control is limited because he lacks the necessary authority required by statute;
4) The CPIC policy needs to be enforced throughout the SEC; and
5) A need exists for more direct involvement in IT investments by the Divisions and Offices.

Finding 1: IT Investments Did Not Follow the Formalized Process Prescribed in the CPIC Policy and Procedures

Two of four investments selected for OIG review did not follow the formalized process prescribed in the Capital Planning and Investment Control policies and procedures.

The SEC's CPIC Process. All projects regardless of budget must initially be reviewed by the PRB for soundness and viability within the Commission's architecture.[7] As the scope of this audit covered calendar year 2007 to June 2009, OIG reviewed two different threshold requirements, because the

[7] This information was obtained from an internal OIT restricted SharePoint site that has Capital Planning and Investment Control data, such as an overview of the process, meeting information, board links, portfolio/project data and threshold information by fiscal year.

requirements changed for 2009. IT investments approved in 2007 and 2008 were subject to the approval thresholds shown in Table 1 as follows:

Table 1: 2007/2008 Investment Approval Thresholds

Investment Amount	Who Reviews?
Less than $200,000	With approval from the CIO, the PRB may review and approve the investments.
Above $200,000	The IOC must approve.

Source: OIT

Table 1 illustrates in 2007 and 2008, investments costing $200,000 or less were approved by the PRB if they met the technical requirements of the Commission's architecture, as determined by the CIO. The PRB consists of managers within OIT and a representative from the Office of Acquisitions. Investments of $200,000 or more were required to be presented to the IOC for approval.[8]

Investments approved or presented in 2009 were subject to the approval thresholds shown below in Table 2:

Table 2: 2009 Investment Approval Thresholds

Investment Amount	Who Reviews?
Less than $100,000	With approval from the CIO, the PRB will review and oversee these investments.
$100,000 to $250,000	With approval from the CIO, the PRB will review these investments and determine if they need to be forwarded to the IOC or can be approved at the PRB level.
Above $250,000	The IOC must approve any projects that are greater than $250,000.

Source: OIT

In 2009, if an investment was less than $100,000, the PRB would oversee the investment after it had been approved by the CIO. The same process applied for investments ranging from $100,000 to $250,000, unless the PRB chose to forward them to the IOC for approval due to visibility, impact on the agency or other reasons. Finally, all investments greater then $250,000 had to be approved by the IOC.[9]

When an investment is forwarded to the IOC, the IOC reviews the investment presentation from the requesting division or office and considers any advice given from the PRB. The IOC then determines whether the investment is in-line with the SEC's strategic direction and the funds are available to execute the

[8] Id. at 2008 review thresholds.
[9] Id. at 2009 review thresholds.

project. If these criteria are met, the investment is formally approved. For all projects presented to a CPIC board, an approval or disapproval document is prepared detailing the reason for the board's decision.[10] If the project is approved, the approval document, the project purpose, approval amount and agreed upon timeframes for completion, are put into OIT's project management system for monitoring.[11]

IT Project Verification. During our audit, we assessed whether major IT investment projects were properly approved by the appropriate CPIC board. We developed a web-based IT investment project questionnaire, which we sent to 34 divisions and offices within the Commission.[12] We utilized an online tool to develop the survey, which consisted of multiple choice and short answer questions. We also asked SEC divisions and offices to populate an accompanying spreadsheet if they had any major IT investment(s) costing $200,000 or more during January 2007 to June 2009. We received populated spreadsheets from 7 of 34 SEC divisions and offices. Based on the seven populated spreadsheets we received, OIG judgmentally selected four IT investment projects for verification.[13]

Table 3, shown below, identifies the four IT investment projects OIG selected for verification: (1) Momentum Upgrade; (2) Regional Office Backup; (3) Automated Procurement System; and the (4) Risk and Surveillance Data Analysis and Reporting.

Table 3: SEC IT Investment Projects Selected For Verification

SEC Division/ Office	Name of Investment Project	CY	Total Projected Contract Cost	Followed CPIC Process
1. OFM	Momentum Upgrade	2007	$3.4M	Yes
2. OIT	Regional Office Backup	2008	$200K	No
3. OAS	Automated Procurement System	2008	$3.5M	No
4. OCIE	Risk and Surveillance Data Analysis and Reporting	2009	$300K	Yes

Source: SEC/OIT Clarity system and verification documentation.

For the IT investment projects selected for verification, the OIG conducted interviews with the investment sponsors and/or project managers of those

[10] Implementing Instruction (II) 24-02.01.02 T01, Record of Decisions for IT Investments form. This document is used to officially record IT investment decisions and to provide the necessary authorization to proceed with the CPIC process.
[11] See Clarity system in the portfolio/project management information module.
[12] These included both divisions and offices at headquarters and the regional offices.
[13] In our survey, we defined major investments as projects costing $200,000 or more, or projects that were highly visible within the Commission. The Executive offices, such as the Offices of the Chairman and the Commissioners were not included in the survey results because they do not sponsor large IT investments.

projects. We also reviewed support documentation for the projects, proposal requests, board meeting minutes and presentation slides. Our verification process found that two of the four investment projects did not follow the formalized process prescribed in the CPIC policies and procedures. A detailed review of the IT investment projects OIG selected for verification follows.

OIG Verification of IT Investment Projects

Momentum Upgrade. The IOC approved the Momentum Upgrade project for $2.1 million in March 2007. The Office of Financial Management (OFM) requested an emergency waiver from the CIO in August 2007 for additional funding of $595,560 to fund the upgraded contract fully. In September 2007, OFM asked OIT for an additional $500,000 for hardware and software and to combine an IT project entitled, "Momentum Upgrade Licenses and Servers," which already had an investment of $87,500, with the overall Momentum upgrade project. This addition increased the total funding for the project to $3.2 million. At the end of Fiscal Year 2007, the project received $200,000 in additional "swept funds,"[14] increasing the total funding for the project to $3.4 million. Our audit of this project revealed that the formalized process and procedures of the CPIC process were followed. We found two occasions in which the project manager discovered an issue with the investment. In the first instance, the project manager made a proper change request with the IOC for the additional funds and, in the second instance, he requested an emergency waiver from the CIO.

Risk and Surveillance Data Analysis and Reporting. The Risk and Surveillance Data Analysis and Reporting project is a 2009 IT investment that the IOC approved in April 2009 for $300,000. The Office of Compliance Inspections and Examinations (OCIE) requested this investment to develop reporting capabilities for risk management. To date, there have been no change requests for this investment, and our audit revealed that the project complied with the CPIC formalized process and procedures. Therefore, we determined this project appears to be running smoothly and on target for an April 2010 completion date.

Regional Office Backup Project. The PRB approved the Regional Office Backup project in June 2008 as a pilot to improve backup capabilities at the regional offices, and it was funded for $200,000. At the time the project was approved, the regional offices were having trouble storing data from past and ongoing cases, and the project was intended to increase the storage capacity at the offices. In September 2008, the sponsor appropriately submitted a change request to the PRB because the delivery schedule for the equipment was

[14] "Swept funds" refer to a situation where a project previously approved did not require all the funds that had been approved for the project and, accordingly, the funds are "swept" back into the budget and used for other projects. The Momentum Upgrade project received additional funds that were swept from another project.

delayed and would impact the milestones established for the project. However, during performance testing in March 2009, the sponsor discovered that the project had major problems with overheating and performance. The server room in a regional office was oversubscribed by approximately 19,000 BTU/hour[15] and the additional equipment needed for the backup project would have made the room worse. Also, the equipment purchased to improve the regional office backup capability did not have the adequate performance levels needed by the regional office and, in fact, would lower the regional offices' case system performance instead of improving it. The IT security group rated the project as a high risk due to the problems identified during the security testing. Where significant problems are found, the sponsor of a project is required to go back to the PRB immediately and submit a change request.[16] In this case, the testing highlighted problems with both (a) performance and delivery expectations; and (b) documented technical and operational risks and expectations, either of which would constitute a significant baseline change.[17]

However, our audit found that contrary to the prescribed process, the sponsor did not submit a change request in March 2009. Instead, the sponsor decided in April 2009 to reuse the equipment to support the Alternate Data Center (ADC) project and cancelled the Regional Office Backup project. Only in August 2009 did the sponsor finally return to the PRB, one year and two months after the initial approval of the project and five months after the problems had been discovered during the performance testing, to submit a change request and to inform the board that the pilot did not work, the project was being cancelled and the equipment purchased for the project was being used to support another ongoing IT project.

At the time a project is approved, IT investment baselines are established. The established "baselines document an agreement between the investment sponsor and the CPIC decision authority to deliver, within a defined time frame, a specific product or service at a specific cost."[18] From our perspective the purpose of the requirement that sponsors inform the CPIC decision authorities of significant baseline changes in a project is to ensure that the changes to the documented agreement are known and adequate for all parties involved.[19] In this case, the PRB was not afforded an opportunity to state whether it approved the equipment being used to support the ADC project because the sponsor decided to cancel the project and re-purpose the equipment without notifying the PRB. This resulted in the PRB incorrectly believing that the Regional Office Backup project was on target and would address the regional offices' storage problems. Consequently, the SEC has expended $200,000 for equipment that did not work

[15] British thermal unit (BTU) is an imperial unit of measurement for heat.
[16] II 24-02.01.02, "Information Technology Investment Control" at p. 7.
[17] Id. at p. 7 requires CPIC Decision Authority Approval for Baseline Changes.
[18] II 24-02.01.02 at p. 6.
[19] The roles and responsibilities of the CPIC Decision Authorities (ITCPC, IOC, CIO) are described on p. 14 of II 24-02.01.02.

for its intended purpose, and the regional offices still have a storage problem that needs to be addressed.

Automated Procurement System. The Automated Procurement System (APS) project was not formally approved by any CPIC board. The project evolved from a multiple year project, the Strategic Acquisition Manager (SAM) project sponsored by the Office of Administrative Services (OAS), which was approved by the IOC in April 2005 to automate the SEC's acquisition process and to close out an outstanding audit finding.[20] Although the SAM project was eventually cancelled, our review of the project management system's (Clarity) status reports for the SAM system did not reveal any problems identified by the sponsor that were not resolved by the contractor. While the status comments revealed defects identified during testing, they show that the contractor resolved all the defects. For example, the January 2007 status comments provided that the system failed User Acceptance Testing (UAT) and 88 critical system defects were recorded by the test team during the UAT. The February 2007 comments reflect that the contractor had remedied 100 percent of the 88 critical defects found during the UAT.

In addition, documents establish that in April 2007, the SAM system owners had completed re-testing of the repaired application, and the sponsor conditionally accepted the system. The February 2007 comments further indicate that all critical defect fixes had been applied to the system. We also learned from reviewing status comments and discussions with the project manager that in April 2007, the critical and non-critical items were addressed and the sponsor fully accepted the system. As a result, SAM was placed into production with limited use on May 16, 2007.[21]

We also found that in January 2008, the OAS director requested from the IOC $350,000 in additional funding for customer support for SAM, which the IOC approved.

OAS staff provided OIG with documentation highlighting the system's poor performance, as well as many concerns they encountered with the developer once the system was fielded. OIG was informed that SAM was in use for over a year; however, production was limited due to problems that were encountered. Specifically, OAS staff provided the OIG with:

- Emails addressed to the developer communicating significant problems with the system that were not or could not be resolved;
- Screen shots of problems with the SAM modules; and

[20] *Administration of Information Technology Contracts*, Report No. 350, dated December 16, 2002, Recommendation P.

[21] Discussions with the Office of the Executive Director (OED), OAS and OIT revealed that the system was in production with limited use because it was never deployed to the entire contracting office.

- Dates of meetings held with the developer in an attempt to resolve the identified problems.

Further, OAS officials informed us that after several attempts to address the problems with SAM, the system still had major problems that could not be resolved. According to OAS, at a meeting in April 2008, the developer indicated that a possible solution would be to upgrade the system at significant additional cost to the Commission and hope that all of the problems would be addressed.[22] However, OAS indicated that the developer could not guarantee that all the identified problems would be resolved with the upgrade. Therefore, OAS management determined the only solution was to cancel the project. Although OAS officials showed us email documentation of concerns about the performance of the SAM system, these concerns were not documented in the project management system's (Clarity) status reports.

On June 23, 2008, OAS gave a "lesson learned" presentation to the IOC and informed it of the SAM system's cancellation, due to performance issues and a plan to solicit companies to implement a new procurement system, the APS. This presentation occurred three years and one month after the initial approval of the SAM project and one year and five months after the problems were discovered during the UAT. Moreover, this was merely a "lessons learned" presentation. A formal request was never made for any IOC approval.

Because the APS project flowed out of the SAM project cancellation, OAS commenced the APS project without formal approval from any CPIC board. OAS management informed us that they did not believe IOC approval of the APS project was required because, from their perspective it was not a new project but a recompete, the SAM project had serious problems that would have cost millions to correct, and OIT had already received approved funding from the SEC Executive Director for the APS project.[23] However, our audit found that the APS project was a separate and distinct project that according to CPIC policy required IOC approval. On September 22, 2008, OAS awarded a contract to CompuSearch for $3.5 million to implement the APS project.

Our audit found that similar to what occurred with the Regional Office Backup project, major decisions to cancel the SAM project and start the APS project were made without IOC approval. In our view, OAS should have gone back to the IOC when it discovered SAM's performance problems and provided the IOC with the following options:[24]

[22] Per the charts provided by OAS, this meeting was held in April 2008.
[23] Memorandum from the Executive Director (ED) to CIO dated June 25, 2008 stating during the mid-year budget review that $3.5M was provided to OIT for the new acquisition system to replace SAM.
[24] II 24-02.01.02 at pgs. 6-7, provides that after an investment enters the execution phase, its baseline may not be materially changed unless the appropriate CPIC decision authority (ITCPC, IOC, CIO) approves such a change.

- Correct the performance problems with the SAM system, which the testing showed had been corrected, and establish performance measures for the contract, explaining the costs that would be incurred in connection with this approach; or

- Cancel the SAM project and begin a new project, detailing the costs of this approach.

If the IOC had been provided these options, it would have been aware of the issues and had the opportunity to make a sound decision as to the direction it deemed appropriate based on the facts presented by OAS. Instead, the IOC was deprived of this information and opportunity, as OAS informed the IOC of the situation only after canceling the SAM project and making the decision to begin the new APS project.

Accordingly, our audit found two of the four projects (Regional Office Backup and APS) selected for verification did not comply with applicable processes and procedures, and the IT boards were not afforded opportunities to conduct meaningful reviews of them. These two projects had a combined total of almost $4 million and are examples of projects that should have gone back to the boards for approval before any action to cancel the projects, or to begin new projects, were taken because both projects underwent significant baseline changes.

According to Section C of CPIC Implementing Instructions, an investment team is required to return to the boards for approval of material baseline changes.[25] The Implementing Instructions contains the following information for Baseline Changes Requiring either PRB/Project Management Office (PMO) or CPIC Decision Authority Approval:

- A baseline schedule change may be approved by the PMO or PRB --
    - A baseline schedule change is needed because of delay in contract award (or in the delivery terms of the contract) and the time delay does not increase the investment's cost. In such cases, the PMO may approve the schedule baseline change.
    - The PRB directs a change of an investment's baseline schedule on the basis that there are no additional costs or technical impacts associated with the schedule change, and the investment's sponsor approves of the change.
    - The PRB directs a baseline schedule change to re-allocate needed resources to another investment

[25] Id. at pgs. 6-7.

based on overall portfolio priorities or other operational considerations. The decision and rationale shall be recorded in the PRB minutes.

- An investment team shall request a change in the approved baseline when it is no longer advisable or feasible to meet an established baseline commitment because conditions exist that adversely affect:
  - Costs, including those associated with a related investment(s);
  - Scope of the approved investment;
  - Delivery schedules, other than those due to contract award, or delays due to delivery terms of the contract;
  - Performance and delivery expectations;
  - Documented technical and operational risks and expectations; and/or
  - Other critical factors essential to the investment.[26]

In the Regional Office Backup project, the testing highlighted problems with both performance and delivery expectations and documented technical and operational risks and expectations, either of which would constitute a significant baseline change.

In the APS project, OAS cancelled the SAM project and started an entirely new APS without formal approval from the IOC. According to the CPIC Implementing Instruction, only the CPIC decision authorities (ITCPC, IOC and CIO), have the authority to determine whether to continue, change or terminate an investment when it fails to achieve its approved baselines.[27] OAS' decision to cancel the SAM project without proper approval resulted in an additional $3.5 million (SAM had already cost $3 million) being spent to automate the acquisition process. Also, in accordance with the Implementing Instruction, OAS should have gone to the IOC when the UAT for the SAM system identified major problems because the testing highlighted problems with both (a) costs, and (b) performance and delivery expectations.

In summary, our audit found that despite the significant baseline changes, the sponsors for both projects did not go to the PRB or IOC for approval before the changes were made, as the CPIC policy requires. Instead, the sponsors went to the board after the fact to inform them that the approved projects had been cancelled, and they were either:

[26] Id. at p. 7.
[27] Id. at pgs. 6-8.

- Utilizing the equipment for another project, or
- Starting an entirely new project.

Both actions are a direct violation of the CPIC policy and made it impossible for the boards to conduct a meaningful review of the projects. Moreover, the fact that 50 percent of the projects we judgmentally selected failed to follow applicable procedures raises serious questions as to whether the CPIC policy is being properly implemented and IT investments overall are being appropriately and sufficiently evaluated and approved by the pertinent CPIC board.

Recommendation 1:

The Office of Information Technology should improve its oversight of information technology investments to ensure that projects are in compliance with the requirements in its Capital Planning and Investment Control policies and procedures specifically dealing with the implementation of the control and evaluate phases of the Capital Planning and Investment Control process.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

Recommendation 2:

The Office of Information Technology should require status updates be provided for all ongoing projects every six months to manage resources (staff, cost and time) for information technology investments over $200,000 and above.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

Finding 2: IT Projects Have Not Always Been Properly Managed

IT investments are not being properly managed because the project managers are overloaded with assignments, resulting

in projects not following the SEC's formalized policies and procedures.

As discussed above, two of the four IT investments projects OIG selected for verification found they were not appropriately managed and failed to follow CPIC policies and procedures. We also learned through interviews with business sponsors and project managers from OIT, OAS, OFM and OCIE, as well as data obtained from the Clarity system,[28] that IT projects often have been plagued with problems due to:

- The lack of a dedicated technical project manager;
- Unexpected cost overruns;
- Delays with software/hardware;
- System performance; and
- Inadequate development of requirements.

Project Management Resources. The effectiveness of the CPIC process depends to a great extent on project management. Project management is the application of knowledge, skills, tools and techniques to a broad range of activities to meet the requirements of the particular project. It is a crucial element in implementing any system or service, especially one involving a significant IT investment.[29] Successful project management involves effective management of nine knowledge areas, as illustrated in Table 4 below.

Table 4: Project Management Nine Knowledge Areas

Scope Management—defining and managing all work required to successfully complete the project.
Time Management—ability to complete the project in a structured timeframe.
Cost Management—preparing and managing a budget for the project and managing costs throughout the project's life.
Quality Management—ensuring the project will satisfy stated or implied needs of the organization and its stakeholders.
Human Resources Management—making effective use of people to complete the project. This area involves delegating the most qualified and skilled person(s) to a specific task of the project to ensure the project is implemented effectively.
Communications Management—generating, collecting, disseminating and storing project information for all stakeholders.
Risk Management—identifying, analyzing, and responding to risks.
Procurement Management—acquiring or procuring goods and services that are needed from outside the organization.

[28] Clarity is a comprehensive project management system. It is a web-based Project/Portfolio Management information system and is used to support the Capital Planning Investment Control (CPIC) and project management processes. Its purpose is to provide a central location to view all investment projects.
[29] Farm Credit Administration audit report 04-02, *Project Management*, dated September 9, 2004 at p. 1.

Project Integration Management—overarching function that affects and is affected by all other knowledge areas. The collaborative effort of all the knowledge areas in executing the project.

Source: Project Management Book of Knowledge[30]

Effective project management is essential to ensuring that IT projects are adequately managed and historical problems with these projects are remedied. With the numerous IT-related initiatives currently being implemented to meet the challenges facing the SEC and its increased dependence on IT solutions, effective project management is more critical than ever. However, our audit found that as the need for development, oversight and continuous monitoring of IT investments has increased, the resources available to accomplish this work have decreased. We learned from interviews with OIT management that they were required to give up four slots during 2009, despite the fact that the office was already understaffed. Moreover, we were informed that the Commission had approximately 220 IT projects from 2007 to June 2009, and OIT only had a staff of 12 technically certified project managers[31] to oversee IT projects.

Additionally, through interviews with business sponsors and project managers within OAS, OCIE, OFM, the Office of Human Resources (OHR) and staff within OIT, we found that project managers were assigned several in-depth projects (220 projects to 12 project managers), but due to resource constraints, they could not possibly dedicate the necessary time to manage the projects properly and provide adequate oversight of them. As a result, IT investments were not being managed during the control and evaluate phases of the IT investment process.

Further, our audit found that OIT's project management staff has been so overloaded with assignments that, in many cases, they were unable to devote sufficient time to a single project. In fact, the problems we identified with the two projects discussed above may be directly attributed to inadequate project management. The Regional Office Backup project was the result of poorly-defined requirements resulting in the purchase of equipment with performance problems that could not meet the needs of the agency. Although this was a relatively small investment, sound management practices would have identified the capacity needed prior to purchasing the equipment and potentially prevented the expenditure of funds on inadequate equipment. More importantly, adequate project management resources could have resulted in successfully addressing the project's need, i.e., the improvement of backup capabilities within the regional offices, which still remains unaddressed.

[30] The Project Management Book of Knowledge guide is the considered to be the broadest and most widely used standard reference of industry best practices for project management. *A Guide to Project Management Body of Knowledge*, 3rd edition *PMI Standards Committee* at appendix F at pgs. 338-341.
[31] Certified project managers are individuals who have received a PM Certification, per SEC Operating Directive (OD) 24-02.04.T01, "IT Project Manager Qualification Checklist," May 30, 2006 at pgs. 2-4.

Regarding the APS project, the system performance issues with SAM may have been resolved if the project manager had the proper amount of time to devote to the project, which could have prevented the loss of $3 million and avoided the cost of a new investment. According to OAS, the failures of the SAM system were not only performance problems with the contractor and system, but also related to the lack of technical resources available to manage IT projects.

Based on the projects OIG verified, we found that OIT's inability to provide adequate technical resources for the IT projects forced the program offices to contract out the project management function, resulting in increased project costs.[32] In fact, OAS requested additional funds for APS project management, and it has stated in presentations to the boards that costs for APS may continue to increase due to the lack of resources within OIT.

Further, we found that the Project Management Office (PMO) Assistant Director position within OIT has been vacant for over 18 months. This management position is responsible for ensuring that the control and evaluate functions of the CPIC process are adequately addressed within OIT. According to OIT, the Assistant Director for the PMO also:

- Staffs the PMO branch (hires technical project managers);
- Ensures that approved projects are adequately staffed with the accurate mix of technical and program staff in order to successfully complete the project;
- Assigns the technical Project Managers(PM) within OIT to the projects;
- Establishes, oversees and manages the PM staff's training program to ensure we have the adequate expertise to manage IT projects; and
- Communicates the CPIC process throughout the SEC.

With this crucial management position being vacant for such a long period of time, the SEC has no one charged to ensure that the control and evaluation functions of the CPIC process are accurately addressed and managed. Our audit also revealed that the SEC hired a consultant, to perform an assessment of the CPIC process in 2007. In a Executive Briefing to the IOC, the consultant highlighted the same problem the OIG identified with the Commission's project management resources, stating that the IOC needed to assess the capacity of available project managers to oversee the portfolio of projects.[33] We found that as of the date our report was finalized, this issue has still not been resolved.

[32] Both the APS and Risk and Surveillance Data Analysis and Reporting projects have contracted out the project management function.

[33] The Consultant's Executive Briefing responses dated November 19, 2007.

Recommendation 3:

The Office of Information Technology should immediately fill the position of Assistant Director for the Project Management Office with an experienced and qualified candidate.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

Recommendation 4:

The Office of Information Technology should perform an assessment of the project management function to compare the current ratio of projects per project manager to the industry's acceptable ratio of projects per project manager.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

Finding 3: The Chief Information Officer's Control and Effectiveness Are Limited Because He Lacks the Authority Required by Statute to Manage IT Resources Adequately

The CIO lacks the necessary authority to manage and oversee the CPIC process adequately.

Chief Information Officer Authority within the SEC

Several concerns about the IT process that were identified in our audit may also be related to the CIO's authority within the Commission. We found that the CIO's control and overall effectiveness are limited because the CIO does not have the authority to enforce the Commission's CPIC process.

The CIO currently holds a dual responsibility at the SEC, serving as the CIO and the Director of OIT. Accordingly, while in his role as the OIT Director, the SEC organizational chart indicates the individual reports directly to the Chairman. Our

review of 17 CFR § 200.13 reveals that the Executive Director (ED) provides administrative authority over the OIT Director. Specifically, the CFR states that the ED provides "executive direction" in addition to "administrative control" and has ultimate responsibility to approve substantive and operational IT policy. We determined that the CIO/OIT Director reports to the ED and thus, does not have the authority to influence substantive IT decisions that his direct supervisor (the ED) makes.

The problem highlighted in Finding 1 with the APS project not following the prescribed CPIC process is related to limitations on the CIO's authority. OAS management informed us that they did not know that they were required to obtain the CPIC Board's approval for the APS project because they viewed it as a recompete and not a new project, and OIT had already received the funding from the ED to go forward with the new project.

OAS is a "direct" report to the ED and the ED allocated funding and gave OAS the approval to go forward with the new contract. Thus, the CIO was unable to play any role in ensuring that the CPIC process was followed.

Moreover, we found the CIO/OIT Director's dual-reporting structure as implemented within the SEC violates the statutory requirements of 44 U.S.C. §§ 3506(a) (2) (A) and (3)[34] which specifically provides that the CIO shall report directly to the head of the agency. We also determined the reporting structure limits his authority to manage IT resources for all Commission divisions and offices adequately. The current reporting arrangement further violates the Office of Management and Budget (OMB) guidance that provides that each Executive "Department or Agency has a designated executive-level CIO reporting to the head of the organization, with formal and full responsibility for all requirements set forth in [applicable statutes, regulations and guidance]."[35] The OMB guidance further provides that the agency CIO is to have "ultimate responsibility for the governance, management and delivery of IT mission and business programs" and "has an effective means of meeting this responsibility."[36]

The SEC has advised us that the Office of General Counsel has opined that the CIO's dual reporting relationship is not violative per se of the applicable statute, since that statute requires that the CIO must report to the agency head with

[34] Under, 44 U.S.C. § 3506(a)(2)(A), ". . . the head of each agency shall designate a Chief Information Officer who shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter [44 USCS 3501 et seq.]." 44 U.S.C. § 3506 (a)(3) provides that "[t]he Chief Information Officer designated under paragraph (2) shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under this subchapter [44 USCS 3501 et seq.] . . . ."

[35] Memorandum for the Heads of Executive Departments and Agencies, M-09-02, Information Technology Management Structure and Governance Framework, dated October 21, 2008, Attachment, Section I.A.

[36] Id. at Section I.B. It should be noted such "ultimate responsibility" on the part of the CIO remains subject to the overall direction of the head of the agency who according to statute, is ultimately responsible for all information technology operations and policies. See 44 U.S.C. §. 3544(a).

respect to the specified substantive responsibilities, and therefore a CIO could lawfully report to another senior executive with respect to purely administrative matters. While OIG takes no position on whether this legal interpretation is accurate, we found that at the SEC, the ED does in fact exercise substantive authority over the CIO by virtue of the current reporting relationship which violates the letter and intent of the statute as well as OMB guidance.

Furthermore, interviews revealed there is a perception within multiple Commission divisions and offices that OAS, OFM and OHR are able to evade the CPIC process without facing any consequences because the heads of these offices report directly to the ED. The CIO is supposed to be the custodian of the Commission's IT resources; however, his ability to perform this task effectively is limited by virtue of his reporting relationship with the ED.

OIG Prior IT Capital Investment Process Audit. The OIG issued *IT Capital Investment Decision-Making Follow*-Up, Report No. 365, in March 2004. The report made two recommendations to address the issue of the CIO's authority as follows:

- Recommendation 1 - The Chairman should delegate to the CIO the necessary authority to issue and enforce Commission-wide IT policy and regulations; and

- Recommendation 2 - The preparation of an Action Memorandum to the Commission to modify 17 CFR § 200.13 to formally delegate authority to issue IT policies and regulations to the CIO.[37]

In our review of assessing whether the recommendations were closed, we found that some work had been done in an effort to close out these old recommendations; however, the recommendations were not fully addressed. For recommendation 1, we found that the delegation authority states that the CIO is responsible for advising and assisting the Office of the Chairman and the Division Directors, Office Heads and Regional managers on IT and security related matters.[38] In our view this does not give the CIO/OIT Director the full authority needed to develop and approve IT policy throughout the Commission. Furthermore, we discovered that the CIO/OIT Director currently develops IT policy, but the ED approves and issues the policy.

For recommendation 2, a action memorandum was started, but it was never completed and according to the current version of 17 CFR § 200.13, the ED still maintains responsibility for developing and executing management policies of the

[37] *IT Capital Investment Decision-Making Follow-Up*, Report No. 365, issued March 29, 2004 at p. 9.
[38] CIO and ED delegation authorities signed by the Chairman on August 11, 2009.

Commission for all its operating divisions and staff offices, including OIT.[39] This regulation further illustrates the lack of authority that the CIO has when it comes to controlling IT resources, which are substantive aspects of his responsibilities.

Recommendation 5:

The Chairman should formally delegate authority to the Chief Information Officer necessary for the management and oversight of the Capital Planning and Investment Control process, to include the full authority to develop and execute all information technology policy, as approved by the Chairman.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that the Chairman's office has concurred with this recommendation.

Recommendation 6:

The Chairman should revise 17 CFR § 200.13 to provide the Chief Information Officer (CIO) with full authority to develop and issue Information Technology policies and carry out the prescribed substantive responsibilities under 44 U.S.C. § 3506 and OMB Guidance M-09-02 and remove the CIO/Director of the Office of Information Technology from under the supervision of the Executive Director or any position other than the Chairman for those substantive responsibilities.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that the Chairman's office has concurred with this recommendation.

[39] The language of 17 C.F.R. 200.13 clearly provides for the Executive Director to have more than simple administrative authority over the CIO in his role as head of OIT, as it specifies that the Executive Director provides "executive direction" in addition to "administrative control" and has ultimate responsibility approving substantive and operational IT policies. We reviewed 17 C.F.R. § 200.13 on LexisNexis, where it had been updated through the January 14, 2010 issue of the Federal Register.

Finding 4: The CPIC Internal Regulation Needs to be Revised to be Enforceable Throughout the Commission

> The formal CPIC policy document Securities & Exchange Commission Regulation (SECR) 24-02, does not have an enforcement mechanism to ensure that all Commission Divisions/Offices adhere to the policy.

The primary policy document governing the CPIC process applies to all SEC divisions and offices and to all IT investments regardless of size. Section 5(j) of SECR 24-02, states that "[t]he CIO shall hold all SEC personnel accountable for the IT investments and resources entrusted to them."[40] The provision further states that "[t]he CIO shall work with the Associate Executive Director for Human Resources to determine how to institutionalize such accountability."[41] While we commend OIT for having these statements in their policy, we could not determine how the requirements are being implemented.

We discussed this issue with the CIO, who stated that he did not believe that OIT and OHR have met to determine how to institutionalize the accountability requirement of the policy. Also, during interviews conducted with business sponsors from OAS, the Division of Enforcement, OCIE and OFM, we found they were not aware of any specific responsibility for the divisions and offices to follow the CPIC processes or policies.

Specifying in SECR 24-02 that it is the responsibility of Regional Directors, Division Directors and Office Heads to ensure that all IT investments within their control adhere to the formal CPIC policies would clarify this matter. Further, it is important that OIT and OHR take the necessary steps to determine how to enforce implementation of the policy adequately. Specifically, they need to develop and provide the CIO and/or IOC, with an enforcement mechanism applicable to investments that have been funded outside of the formalized CPIC process. Doing so would strengthen the regulation, make it an enforceable document and thus give the CIO further authority over the CPIC program.

[40] SECR 24-02, "Information Technology Capital Planning and Investment Control," June 14, 2006 at p. 4.
[41] Id. at pgs. 4-5.

Recommendation 7:

The Office of Information Technology should revise the SECR 24-02 to:

- Add a responsibility that the Division Directors, Office Heads, and Regional Directors ensure that all information technology investments within their responsibility adhere to the Capital Planning and Investment Control policies and procedures.

- Create an enforcement mechanism for the Chief Information Officer and Information Officers Council to utilize when they discover investments that have been funded outside of the Capital Planning and Investment Control process.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

Finding 5: The OIG Survey Revealed the Need for More Involvement with IT Investments by the Divisions and Offices on IT Investments

> Program offices could not populate OIG's generated worksheet with data for their projects because they were not directly involved in the day-to-day management of the projects.

The OIG developed and issued an IT Investment Project Questionnaire to 34 divisions and offices within the Commission.[42] Thirty of the 34 offices completed the survey, resulting in an 88.2 percent response rate. The survey focused on determining the number of major IT investments projects that are managed within the SEC and was intended to aid the OIG in identifying the universe of SEC's IT investment projects. What follows are some of the relevant questions asked in the survey and the responses OIG received.

[42] These 34 offices exclude the Chairman's Office, Commissioner's Offices, and offices with duplicative responses.

(Q4). Did your division/office acquire any IT Investment Projects during calendar year (CY) 2007 to 2009 (January to June) costing $200,000 or more?

Yes	No	Total Responses
12	18	30
40%	60%	100%

(Q5). Did your office exercise any "option years" during CY 2007 to 2009 (January - June), for IT Investment Projects costing $200,000 or more?

Yes	No	Total Responses
5	5	10
50%	50%	100%

(Q6.) During CY 2007, 2008, and 2009 (January - June), for any given year did your office acquire two or more related IT Investment Projects costing $200,000 or more from the same vendor?

Yes	No	Total Responses
5	8	13
38.5%	61.5%	100%

(Q7). Did your division/office have any IT Investment Projects costing $200,000 or more that were disapproved, cancelled, or suspended during CY 2007 to 2009 (January - June)?

Yes	No	Total Responses
2	9	11
18.2%	81.8%	100%

Results of OIG's Review of the Selected Survey Questions. For affirmative (yes) responses received to questions 4, 5, and 7, the divisions/offices were asked to populate a worksheet. Although survey responses for question 4 (Q4) indicated that 12 divisions/offices had IT investment projects costing $200,000 or more, only 7 of 12 divisions/offices completed and provided OIG with the required worksheets. Because all SEC divisions/offices did not complete the survey and we did not receive worksheets from all of the divisions/offices that

had IT investments of $200,000 or more, we could not determine the full universe of major IT projects from calendar year (CY) 2007 to June 2009. We used OIT's project management system, Clarity, to identify the number of IT investment projects that were managed from 2007 to 2009 and found there were approximately 220. The survey results revealed the need for more direct involvement from program offices and further supported the need for better oversight from OIT during the *control and evaluate* phases of the CPIC process.

Our analysis of the survey revealed that 4 of 7, or 57 percent of divisions/offices that provided OIG with a worksheet, could not populate the fields using their own internal data. The divisions/offices had to request data from OIT or ask OIT to provide data directly to the OIG. The fact that 57 percent of divisions/offices that provided worksheets could not provide comprehensive data for projects within their program areas is a significant concern. Clearly these divisions/offices were not sufficiently involved in their IT projects since they could not provide information on a particular project. While personnel in these program divisions/offices are not expected to be IT specialists or technical project managers, they should have some direct involvement in the IT investment that was approved and funded to meet a need or improve a process within their program area.

As the survey results illustrate, between CYs 2007 and June 2009, the Commission had 12 divisions/offices that either had current IT investments costing $200,000 or more; 5 divisions/offices exercised an option year, and 2 divisions/offices had an IT investment project that was disapproved, cancelled, or suspended. Yet, over half of the respondents that provided worksheets (4 of 7) could not provide detailed information on the projects for which they requested approval from the CPIC boards.

SEC Operating Directive and the Roles of the Investment Team. SEC Operating Directive 24-02.01 01.0 establishes and defines the roles and responsibilities for approved IT projects. According to the Operating Directive, when a project is approved, an investment team is assigned. The investment team is made-up of individuals who are responsible for managing and overseeing the project during the *control* and *evaluate* phases of the process.[43] An investment team can include 10 members, mostly OIT staff; however, two people must be from the program office.[44] Table 5, shown below, identifies and defines the roles within investment teams.

[43] OD 24-02.01," Information Technology Investment Management." dated August 14, 2006 at pgs. 6-11.
[44] Id.

Table 5: Investment Team Roles

Roles	Definition
Project Sponsor*	Champion of project approval and successful outcome. Primary owner of the system and stakeholder of the project. Provides constant vigilance to ensure that project continues to meet the business need. Defines project goals. Sponsor MUST provide adequate authority and support to enable PM to be successful.
Technical Lead (TL)*	Technical Expertise - Owner of technical action items and outcomes including solution's technical design, development, coordination of technical resources, execution of QA processes, and acceptance of technical deliverables.
Business Lead (BL)*	Functional business expertise - Owner of business action items and outcomes including solution's business requirements, coordination of business resources to support the project, and design, execution and acceptance of functional business deliverables. Drives user acceptance testing (UAT), user training and system deployment phases.
Project Manager (PM)*	Responsible for Successful delivery of project as approved. Manage project and team to successful project conclusion. Responsible for project planning, communication, coordination, dependencies, issue resolution and risk mitigation. Sponsor MUST provide adequate authority and support to enable PM to be successful.
Project Expediter	Administrative support tasks with no authority or responsibility for project delivery. Supports and assists the PM; tasks are essential and must be performed by the PM if no expediter is assigned.
OIT POC (Not TL)	Explains OIT processes and helps to facilitate introductions and meetings between Project team members and key OIT personnel. This person has no specific project related responsibility.
PMO Support*	CPIC and PM administration including entering project in Clarity; advice on CPIC activities, Clarity actions, monthly status reporting; and seeking management support. Not responsible for approval or outcome of this project.

Roles	Definition
COTR*	Technical Contract Administration of the project - Manage vendor, in accordance with COTR appointment, to comply with all contract terms and requirements. Review and approve vendor status reports, deliverables/milestones, invoices, and incentive payments (if applicable). Close interaction with PM to provide and receive shared information.
Maintenance Manager (MM)*	Owner of system maintenance. Responsible for system support once in production.
Other*	Alternative approaches to delineating responsibilities need to be clearly defined and agreed upon by all parties involved. Please use the attached "Roles by Tasks" worksheet to denote any variations.

Source: OP 24-02.01.01.01.A01, IT Investment Plan Instructions
*Required for each project. All others are ad-hoc roles invoked when necessary.

As illustrated in Table 5, OIT's documented procedures clearly define the roles needed for adequate project management. However, our audit found that these procedures are not being followed for all IT investments. The current Operating Directive requires that two positions (project sponsor and business lead) within the investment team be filled by program office staff. However, this requirement is not being followed for all IT projects.[45] For example, we could not find within the Clarity system an investment team assigned for the IT projects we reviewed. In addition, while we did find that in the four projects we reviewed, the sponsoring office had identified a business sponsor and a project manager, we did not find a business lead assigned for any of these projects. Furthermore, we discovered that the business sponsors are often at the Associate or Assistant Director level and do not have sufficient time to devote to the day-to-day management of an IT project. If the requirements of the current Operating Directive were followed such that two representatives of the investment team were actually from the program area, the sponsoring office would have more ownership in the project, which we determined would reduce the time and cost to complete an IT project.

The Project Management Book of Knowledge, a well-known guide for project management best practices, discusses the importance of project stakeholder/customer involvement throughout the life of a project. The guide also discusses the creation of two distinct roles; the enforcer and the supporter. The top-level "enforcers" are sponsors of the identified approach, along with "support" staff for consistent delivery according to the identified standards and procedures.[46] These roles illustrate the need to ensure that at least one individual on the program side serves as the business lead (or supporter) on an

[45] OP 24-02.01.01.01.A01, IT Investment Plan Instructions at pgs. 3-4.
[46] Project Management Best Practices: An Introduction to PMBOK, February 13, 2008 by Haydn Thomas Julie Tilke found at www.cioupdate.com.

IT project. The business lead will ensure that the business needs of the project are addressed and interact on a constant basis with the technical IT project manager, further supporting the need for more direct involvement from the office on an approved IT project. Additionally, we note that the consultant previously retained by the agency also identified the need for more program involvement as a problem in the 2007 briefing.[47]

Survey Results Pertaining to Policy. The OIG questionnaire also asked respondents if they were aware of the CPIC policies and procedures, as shown in question 8 (Q8).

> **(Q8). Are you or other personnel in your division/office aware of the Commission's policy and other external policy, laws, regulations such as OMB Circular A-130, Management of Federal Information Resources, etc., that governs major information systems?**

Yes	No	Total Responses
19	8	27
70.4%	29.6%	100%

Approximately 70 percent of respondents indicated they were aware of the policies and procedures that govern the CPIC process, but our audit has shown that they are not following all aspects of these governing policies and procedures. We found that OIT has a documented set of policies and procedures for the CPIC process and use the web-based Project and Portfolio Management information system known as Clarity, to support the CPIC and project management processes. The goal of the Clarity system is to provide a central location to view all Investment Projects with an automated governance review capability. All divisions/office should have an individual with access to the Clarity system, especially if that office has an ongoing IT project. We were informed by OIT that each project sponsor is encouraged to provide updates within Clarity on the progress of the projects; however, this is not required. Further, we found that OIT has offered training courses on the Clarity system seven times during 2008 and 2009, and staff members from only 14 of 34 SEC divisions/offices have attended the training courses. Full utilization of the Clarity system by the program divisions/offices would enhance the management of IT investments within the Commission and thus improve OIT's ability to address the *control* and *evaluate* phases of the CPIC process.

[47] The Consultant's SEC Executive Briefing Responses dated November 19, 2007.

Recommendation 8:

The Office of Information Technology should conduct periodic internal reviews to ensure that the requirements in Operating Directive 24-02.01, *Information Technology Investment Management,* are enforced, (e.g., the requirement that two representatives from the program area be identified for all ongoing projects).

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

Recommendation 9:

The Office of Information Technology should require that all divisions and offices use OIT's project management system and that they update and maintain the data in the system for the investments within their program areas.

Management Comments. Concur. See Appendix V for management's full comments.

OIG Analysis. We are pleased that OIT has concurred with this recommendation.

Acronyms and Abbreviations

APS	Automated Procurement System
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
CY	Calendar Year
ED	Executive Director
GAO	Government Accountability Office
IT	Information Technology
ITCPC	Information Technology Capital Planning Committee
IOC	Information Officers Council
OAS	Office of Administrative Services
OCIE	Office of Compliance Inspections and Examinations
OHR	Office of Human Resources
OFM	Office of Financial Management
OIG	Office of Inspector General
OIT	Office of Information Technology
PRB	Project Review Board
PM	Project Manager
PMO	Project Management Office
SAM	Strategic Acquisition Manager
SECR	Securities & Exchange Commission Regulation
SEC or Commission	U.S. Securities and Exchange Commission
UAT	User Acceptance Testing

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 determined that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope. We conducted this audit from June 2009 to November 2009. The scope of the audit included IT investments that were approved, disapproved, cancelled, suspended, or for which an option year was exercised between CYs January 2007 and June 2009 that cost $200,000 or more. We examined the SEC's IT investment process structure to determine whether it adhered to applicable laws and regulations. We assessed a selected number of IT investment projects to determine if they adhered to the established capital planning and investment control policies, procedures and process that were in place at the SEC.

Methodology. To address the objective of determining whether the CPIC process and procedures and the PRB, IOC, ITCPC structures adhere to governing Commission policy and applicable federal laws and regulations, we observed meetings of the three governing boards (PRB, IOC, CPC). We also determined if the structure and procedures used followed the procedures outlined in the SEC policies for the CPIC process. Furthermore, we reviewed the SEC's policies, procedures and processes for IT investments to determine if they adhered to governing federal laws.

To address the second objective of examining whether procedures exist to ensure that major IT investments are properly approved within the CPIC process and are presented to the PRB, IOC and/or ITCPC as appropriate, we utilized the information from the first objective and interviewed selected project sponsors, project managers, board members, the CIO, ED, and relevant OIT staff. We obtained access to OIT's project management system, Clarity, and the restricted CPIC SharePoint site to review pertinent documentation for selected IT projects such as, approval documentation, project proposals, status notes, and board meeting minutes.

Finally, to address the objective to assess whether major IT investment projects are properly approved by the appropriate CPIC board(s), we performed verification testing of the data housed in the project management system, the

restricted CPIC SharePoint site and information revealed during interviews with selected SEC staff.

We also developed an 11-question survey consisting of 8 multiple choice and 3 short answer questions. The questionnaire was designed to obtain feedback from SEC divisions and offices on the Commission's CPIC process. The survey was issued in August 2009 to 34 SEC division/office's technical point of contact (POC) in the Commission's Headquarters and its 11 regional offices, excluding the Chairman's and Commissioners' offices. Of the 34 technical POCs that received the questionnaire, 30 respondents or 88.2 percent, completed the survey. We also conducted interviews with some of the survey respondents and verified support documentation that was provided for the IT investment projects.

Management Controls. We reviewed the management controls that were considered significant within the context of the CPIC process and our audit objectives. We interviewed personnel from the:

- Office of the Executive Director,
- Office of Administrative Services,
- Office of Financial Management,
- Office of Compliance Inspections and Examinations,
- Office of Human Resources,
- Division of Enforcement, and;
- Office of Information Technology.

We also identified and reviewed applicable policies and procedures, obtained and reviewed available CPIC documentation, and verified support data of selected IT investments for compliance with the CPIC process.

Use of Computer-Processed Data. We used computer-processed data, such as reports generated by the Clarity system, information contained on the restricted CPIC SharePoint site, emails, and Excel spreadsheets. We did not perform extensive testing of system or application controls because it was not an audit objective. However, we did test the reliability of the data by testing an IT project from each year (2007-2009) and conducting a reasonableness test of the information by comparing the computerized data with source documents. We concluded that the data in the systems were reliable and accurate enough to state that overall system controls were reasonable.

Judgmental Sampling. We judgmentally selected four of seven offices/divisions from the IT Investment Projects Questionnaire that had projects costing $200,000 or more during calendar year 2007 to June 2009. We then determined whether these offices/divisions followed the CPIC policies and procedures for its IT Investment Projects.

Prior OIG Coverage. The OIG previously issued *IT Capital Investment Decision-Making Follow-Up*, Report No. 365, on March 29, 2004. The report noted that the Commission was making progress in the IT investment area, but found that its process still did not meet the minimum criteria of GAO's *Information Technology Investment Management Maturity Model* and was not in full compliance with applicable laws and regulations. The report consisted of 25 recommendations. According to the ARTS tracking system, 24 of 25 recommendations were completed, and the final recommendation was closed in January 2010. We reviewed the documentation and analyzed the support used to close the report's recommendations and concluded that two recommendations were not completely implemented, even though they had been formally closed. Therefore, this report's recommendations expand on two prior OIG recommendations made in Report No. 365, pertaining to the CIO's authority over the CPIC process.

Criteria

The Clinger-Cohen Act of 1996 (National Defense Authorization Act For FY 1996; Public Law 104–106, Division E, February 10, 1996), 40 U.S.C. § 1401 et seq.: Reformed the way in which federal agencies acquire and manage IT resources by establishing effective IT leadership within each agency. Requires each agency to establish clear accountability for IT management activities by appointing a CIO with the management responsibilities necessary to carry out the Act's specific provisions.

U.S. Code 44 § 3506(a): Establishes federal agency responsibilities for federal information policy. Requires the head of each agency to designate a CIO who will report directly to the head of the agency to carry out the responsibilities for federal information policy.

17 C.F.R. § 200.133, Executive Director: Describes the resonsibilities and functions of the Executive Director of the SEC.

OMB Memorandum M-09-02, Information Technology Management Structure and Governance Framework, October 21, 2008: Reaffirms and clarifies the organizational, functional and operational governance framework required within the Executive Branch for managing and optimizing the effective use of IT investments.

SEC Regulation (SECR) 24-02, Information Technology Capital Planning and Investment Control, June 14, 2006: Defines the SEC's IT CPIC policy and processes, and the responsibilities for complying with key provisions of the Clinger-Cohen Act of 1996 and other relevant authorities.

SEC Operating Directive (OD) 24-02.01, Information Technology Investment Management, August 14, 2006: Defines the processes used in the management of the SEC's IT investments, as mandated by the Clinger-Cohen Act and further specified in SECR 24-02.

SEC Implementing Instruction (II) 24-02.01.02, Information Technology Investment Control, January 9, 2008: Defines the roles, responsibilities and high-level workflows applicable to the control phase of the SEC's CPIC process.

SEC Operating Procedure (OP) 24-02.02.02.02.A01, Investment Plan Instructions, January 24, 2008: This guide show the various sections of the standard investment plan ad provides for contributions by the entire investment

team to the completion and maintenance of the plan, as coordinated by the designated project manager.

Project Management Institute, A Guide to the Project Management Body of Knowledge, 3rd edition, 2004: This guide identifies and describes the subset of terms that are generally accepted within the project management profession.

List of Recommendations

Recommendation 1:

The Office of Information Technology should improve its oversight of information technology investments to ensure that projects are in compliance with the requirements in its Capital Planning and Investment Control policies and procedures specifically dealing with the implementation of the control and evaluate phases of the Capital Planning and Investment Control process.

Recommendation 2:

The Office of Information Technology should require status updates be provided for all ongoing projects every six months to manage resources (staff, cost and time) for information technology investments over $200,000 and above.

Recommendation 3:

The Office of Information Technology should immediately fill the position of Assistant Director for the Project Management Office with an experienced and qualified candidate.

Recommendation 4:

The Office of Information Technology should perform an assessment of the project management function to compare the current ratio of projects per project manager to the industry's acceptable ratio of projects per project manager.

Recommendation 5:

The Chairman should formally delegate authority to the Chief Information Officer necessary for the management and oversight of the Capital Planning and Investment Control process, to include the full authority to develop and execute all information technology policy, as approved by the Chairman.

Recommendation 6:

The Chairman should revise 17 CFR § 200.13 to provide the Chief Information Officer (CIO) with full authority to develop and issue Information Technology policies and carryout the prescribed substantive responsibilities under 44 U.S.C. § 3506 and OMB Guidance M-09-02 and remove the CIO/Director of the Office of Information Technology from under the supervision of the Executive Director or any position other than the Chairman for those substantive responsibilities.

Recommendation 7:

The Office of Information Technology should revise the SECR 24-02 to:

- Add a responsibility that the Division Directors, Office Heads, and Regional Directors ensure that all information technology investments within their responsibility adhere to the Capital Planning and Investment Control policies and procedures.

- Create an enforcement mechanism for the Chief Information Officer and Information Officers Council to utilize when they discover investments that have been funded outside of the Capital Planning and Investment Control process.

Recommendation 8:

The Office of Information Technology should conduct periodic internal reviews to ensure that the requirements in Operating Directive 24-02.01, *Information Technology Investment Management,* are enforced, (e.g., the requirement that two representatives from the program area be identified for all ongoing projects).

Recommendation 9:

The Office of Information Technology should require that all divisions and offices use OIT's project management system and that they update and maintain the data in the system for the investments within their program areas.

Management Comments

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

THE CHAIRMAN

Memorandum

Date: March 12, 2010

To: David Kotz, Inspector General, OIG
Jacqueline Wilson, Assistant Inspector General, OIG

From: Mary L. Schapiro, Chairman

Subject: Response to OIG Report 466, *Assessment of the SEC Information Technology Investment Process*

I appreciate the opportunity to comment on certain aspects of your recent review of the SEC's information technology (IT) investment process (Draft Report No. 466, *Assessment of the SEC Information Technology Investment Process*, Feb. 23, 2010). My comments here focus on recommendations 5 and 6 and related findings, which are addressed to me. I understand the Director of the Office of Information Technology will be commenting on other aspects of the draft report.

The size and complexity of the U.S. capital markets the SEC is responsible for monitoring make it imperative that the SEC make the best possible use of technology to leverage its staff's expertise. A sound IT investment process must lead to strategically focused acquisitions that are both prudent and creative. I am, therefore, pleased to note the significant improvement your draft report found since the last such assessment in 2004 (Report No. 365, *IT Capital Investment Decision-Making Follow-up*, Mar. 29, 2004).

That progress continues. In January of this year, after an internal review of roles and responsibilities relating to the SEC's IT investments, I approved revised charters for the three distinct bodies that review and approve proposed IT investments. I am confident that these revised processes address a number of the concerns raised in this report, which was, of necessity, based largely on observations of practice under the now superseded IT investment processes.

I am committed to having a Chief Information Officer (CIO) who is fully empowered to meet the important responsibilities envisioned by the Clinger-Cohen Act (CCA) and other applicable laws and implementing guidance. As a result and subject to the comments that follow, I concur in recommendations 5 and 6 inasmuch as they point out that the SEC's CIO must have all authority required by law and necessary to discharge his responsibilities.

Recommendations 5 and 6 also assert that, even after the delegations of authority my predecessor made to the CIO in 2007, the CIO does not have the full authority mandated by the Clinger-Cohen Act and related Office of Management and Budget (OMB) implementing guidance. While I am informed that the intention of the 2007 delegations was to fully implement all applicable legal requirements, I am asking our General Counsel to advise me as to whether the current delegations do, in fact, give the CIO all authority the law and related implementing mandates require. Should the General Counsel conclude

1

that the current delegations of authority fall short in this regard, I will augment the current delegations to correct that deficiency.

In examining the issues raised in your report, I have found that the delegation of authority to the CIO in 2007 was not – though it was intended to be – followed by a corresponding revision to the SEC regulations that specify the authorities of its officials (17 CFR § 200.13 *et seq.*). It is likely that this omission accounts for a portion of any confusion relating to the CIO/OIT Director's authority with respect to that of other SEC officials, notably the Executive Director. I will ask the General Counsel, in conjunction with his review of the current delegations to the CIO, to begin the work necessary to revise the pertinent portions of the SEC's internal regulations contained in the Code of Federal Regulations.

The draft report also notes that the CIO, who is also the Director of the Office of Information Technology, has a dual reporting structure – responsible to the Chairman with respect to specified substantive responsibilities, and to the Executive Director for administrative matters. The report notes (p. 19), that the Office of General Counsel has confirmed that this dual reporting relationship is consistent with law. It is, moreover, a practical means of ensuring day-to-day management support for the CIO/OIT Director in discharging his many responsibilities, including meeting the disparate needs of the SEC's operating divisions and offices.

In that connection, I note that a principal objective of the applicable law and the implementing guidance from OMB is to ensure that IT investments are made with full awareness of the agency's broader business and operating needs, consistent with the SEC's strategic objectives, and evaluated in the context of their present and future budget implications. I am eager to see a closer partnership develop between OIT and the SEC's business lines and their IT-related projects. I believe the revised IT investment process charters noted above will assist us in meeting that objective. It is my intention that the newly-created Chief Operating Officer position that we are currently seeking to fill, will also play a key role in ensuring this close business-technology partnership.

In closing, let me underscore once again my commitment to ensuring that the SEC has a first-rate IT investment process – one that not only meets all applicable legal requirements, but also advances the SEC's overall strategic objectives across all division and office lines. I appreciate the efforts you and your staff have made to further that overriding objective.

cc: David Becker, General Counsel

Memorandum

Date: March 11, 2010

To: David Kotz, Inspector General, OIG
Jacqueline Wilson, Assistant Inspector General, OIG

From: Charles Boucher, Chief Information Officer, OIT

CC: Kayla Gillan, Deputy Chief of Staff, Office of the Chairman
Diego Ruiz, Executive Director, OED

Subject: Management Response to OIG Report 466, *Assessment of the SEC Information Technology Process*

The Office of Information Technology appreciates the opportunity to comment on the subject report. This memo responds to the seven recommendations directed to OIT only; as I understand, the Office of the Chairman will respond to the other two (#5 and #6).

We are pleased with the Office of Inspector General's acknowledgement of the significant progress that the SEC has made since the OIG previously examined the issue of information technology investment six years ago (Report No. 365, March 29, 2004). At that time, the OIG identified major deficiencies in the agency's IT capital investment decision-making process, including that a majority of spending on IT investments did not go through the established IT Capital Planning and Investment Control process (CPIC). The 2004 report contained 25 recommendations for agency action to address a broad range of deficiencies. To address these recommendations, the agency has since undertaken significant efforts, involving the commitment of substantial resources, to improve oversight and controls over IT decision-making. And as you know, the agency has in fact successfully completed corrective action on all of the recommendations from this previous report.

In contrast to 2004, the current OIG report concludes that the SEC has a documented structure, approval process, and adequate procedures for the approval and oversight of IT investments that adhere to governing Commission policy and applicable federal law and regulations. The OIG's report also acknowledges that the SEC "has gone to great lengths, and expended significant resources" to implement this improved IT Capital Planning and Investment Control process.

While these achievements demonstrate the real improvements that have been made in the past several years, we are committed to continue to work for further improvement in controls and oversight over IT capital decision-making. For this reason, we welcome the findings and recommendations of the Office of Inspector General, and are pleased to respond and provide comments on your final report.

We concur, with comment, on the seven recommendations directed to OIT. We agree with the intent of these recommendations: to strengthen compliance with capital investment policies and procedures; provide improved reporting on project status; further enhance OIT's project management capabilities; and ensure the active involvement of program offices in system design and implementation. These goals are consistent with our goals for OIT. I would like to share with you my comments on three issues in the report where I believe that clarifications or additional information are needed.

First, with respect to the discussion on pages 10-14 regarding the agency's 2008 decision to cancel the Strategic Acquisition Manager (SAM) IT project, I was not at the SEC at that time. However, I've been informed that the OIG report accurately notes that the SAM project, whose initiation had been approved by the Information Officers Council (IOC) in April 2005, was cancelled in the spring of 2008 as a result of poor performance. These performance problems included major unresolved system defects, little or no quality control over bug fixes, significant turnover of vendor personnel and lack of qualified customer service support. In accordance with the Federal Acquisition Regulation, a Cure Notice was issued to the vendor in March 2008. The decision to cancel the contract was made after the vendor indicated that an attempt to correct the problems could result in the expenditure of substantial taxpayer dollars and there was no guarantee that such problems could be fixed. As I also understand, throughout this process, the Office of Administrative Services (OAS), which is responsible for overseeing agency contracts, worked in close collaboration with OIT and the then-CIO, and relied extensively on OIT's technical expertise. After the decision to cancel the contract, OAS made a two hour presentation to the Project Review Board (PRB) and IOC on lessons learned and on its plans to re-compete the contract. Although the report is correct that the IOC never formally approved the replacement contract, I understand that the IOC was periodically apprised of further progress.

I also want to mention that both situations identified in your report as deviating from policy were projects that terminated either the contract or the entire project. It is important to note that, in the past, the agency's CPIC project approval activities overlapped with budget activities, and the roles and responsibilities of the SEC's Senior Procurement Executive were not integrated fully within the CPIC process. In January 2010, however, the SEC approved new charters for the PRB and IOC that, among other things, assign the panels new responsibilities to provide oversight and project management assistance to IT projects after they are selected. The new PRB charter, for instance, specifically requires reports to be provided if a project is not expected to meet cost, schedule or performance levels established in its baseline. With the new charters in place, the agency now has a suitable framework in place to review instances, such as was identified with SAM several years ago, of poor IT contractor performance. The new charter, for the first time, lists the Head of the Contracting Agency as a voting member of the Board.

Second, with respect to the report's findings on pages 15-18 regarding project management, over the past few years OIT has maintained a centralized project tracking system to help manage the delivery of technology projects, with a clear overall record of on time, under budget, and within scope results. While I agree with the two recommendations suggested by OIG, I do not believe that an accurate indication of OIT's project management capabilities can be measured merely by counting the number of OIT staff who have obtained non-required project management certificates. In addition, given the significant number of IT projects underway at any given time, as a general matter OIT has found it more effective to

assign project management responsibilities broadly throughout the office, rather than rely on a limited number of project management specialists to oversee IT projects. Finally, we would note that many OIT staff who perform core project management oversight also receive supplemental project management assistance from the contractors.

Finally, with respect to the results of OIG's survey reported on pages 23-28, while we agree with OIG on the vital importance of ensuring that program offices are fully involved with critical decisions, such as defining an IT project's requirements or its implementation, we do not agree with your conclusion that, because divisions and offices do not independently maintain information about IT projects and instead refer to the OIT project tracking system, this means that businesses "were not sufficiently involved in their IT projects." To the contrary, we strongly believe that keeping track of the status of IT projects in a single centralized system is a more efficient way to track progress, and we also have specialized staff to ensure consistency and perform management reporting. Further, while the report notes that "business sponsors are often at the Associate or Assistant Director level and do not have sufficient time to devote to day-to-day management of an IT project," in fact, day-to-day oversight of a project is properly the responsibility of the Project Manager, not the Business Sponsor, who is not expected to be involved with day-to-day management but instead to provide the business authority and overall support to implement the project. This being said, I also agree that the partnership between OIT and the SEC's businesses on technology projects can and should be strengthened, and made more consistent throughout the organization.

In closing, thank you for your work on this audit, and for the opportunity to provide comments on your review of the SEC's IT investment process. Because of the important role that information technology plays in enabling the SEC to successfully carry out its mission, I welcome the results of your review, and am committed to continuing to build on the significant progress that has been made to date.

Office of Inspector General
Response to Management's Comments

We are pleased that the Office of the Chairman and OIT have concurred with all of the report's 9 recommendations. We feel these recommendations when implemented will strengthen the CIO's authority as required by law and will improve the Commission's ability to comply with mandated statutes, regulations and guidance as they pertain to the management and oversight of capital investments. Below is OIG's response to OIT's management comments on Findings 1, 2, and 5.

In OIT's management comments to Finding 1, the CIO acknowledged that "the [OIG] report is correct that the IOC never formally approved the replacement contract," although the CIO stated that he understood that the IOC was periodically apprised of progress. However, as we found in our audit, and is not disputed by OIT, OAS was allowed to commence the APS project without formal approval from the CPIC boards. Providing the CPIC board members with a "lessons learned" presentation regarding cancelling the SAM IT project after the fact does not constitute compliance with the established IOC process and procedures. Moreover, these procedures clearly require formal approval, not simply being periodically apprised of the progress of a project. We would also note that OIT did not dispute in its management comments our concern that OIT had already received approved funding from the SEC Executive Director for the APS project before and without going through the Commission's established boards.

Secondly, in OIT management comments to Finding 2, the CIO stated "I agree with the two recommendations suggested by the OIG," although he noted he did not believe that an accurate indication of OIT's project management capabilities can be measured by counting the number of OIT staff who have obtained project management certificates. We would point out that the finding in our report that project managers were unable to dedicate the necessary time to manage projects properly was based not only on the fact that there were 220 projects assigned to only 12 certificated project managers, but also on direct feedback from project managers and specific and concrete examples where problems with projects were directly attributed to inadequate project management. Further, while we take no position on management's decision to assign PM responsibilities broadly throughout the office rather than relying upon a limited number of PM specialists, we must however highlight that the roles and responsibilities in CPIC policy requires a PM for IT investments, to meet PM

qualifications as described in OD 24-02.04, IT Project Management Qualification Standards.

Finally, with respect to the OIG survey issued and its results in Finding 5, we note that OIT misinterpreted this finding in its management comments. The CIO stated in the OIT comments that he does "not agree with [the OIG's] conclusion that, because divisions/offices do not independently maintain information about IT projects and instead refer to the OIT project tracking system, this means that businesses 'were not sufficiently involved in their IT projects.'" We must point out that our audit did not raise an issue with the program offices utilizing the project tracking system. We agree that keeping track of IT projects in a single centralized system is efficient and in fact, encourage use of the project tracking system as recommendation 9, states that "OIT should require all divisions and offices use the project management system . . . ." However, our audit found that the fact that a significant percentage (57%) of offices/divisions were unable to provide basic data about their projects without having to request the information from OIT was a strong indication that these divisions/offices were not sufficiently involved in their IT projects. In addition, with respect to the CIO's comment about the day-to-day oversight of a project being the responsibility of the project manager, not the business sponsor, we would note that in our view, and as discussed in the Project Management Book of Knowledge, the business lead should also play a significant day-to-day role in ensuring that the business needs of the project are addressed and in interacting on a constant basis with the technical IT project manager. Thus, our concern that these business sponsors are at the Associate or Assistant Director level remains.

Audit Requests and Ideas

The Office of Inspector General welcomes your input. If you would like to request an audit in the future or have an audit idea, please contact us at:

U.S. Securities and Exchange Commission
Office of Inspector General
Attn: Assistant Inspector General, Audits (Audit Requests/Ideas)
100 F Street, N.E.
Washington D.C. 20549-2736

Tel. # 202-551-6061 Freedom of Information Act (FOIA)
Fax # 202-772-9265
Email: oig@sec.gov

Hotline

To report fraud, waste, abuse, and mismanagement at Commission, contact the Office of Inspector General at:

Phone: 877.442.0854

Web-Based Hotline Complaint Form:
www.reportlineweb.com/sec_oig