U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

2009 FISMA Executive Summary Report

REDACTED PUBLIC VERSION

March 26, 2010
Report No. 472

Prepared by C5i Federal, Inc.

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 26, 2010

To: Charles Boucher, Director, Office of Information Technology

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

Subject: *2009 FISMA Executive Summary,* Report No. 472

This memorandum transmits the U.S. Securities and Exchange Commission, OIG's final report on the 2009 Federal Information Security Management Act of 2002 (FISMA) Evaluation. This report provides the Commission with a summary of the responses OIG reported in the FISMA Web Portal to the Office of Management and Budget on November 2009.

This report does not contain any recommendations. Based on the comments received to the formal draft report and our assessment of the comments, we revised the report accordingly.

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 contractor and 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 and Chief Technology Officer, Office of Information Technology
Todd Scharf, Chief Information Security Officer, Office of Information Technology
Barbara Stance, Chief Privacy Officer, Office of Information Technology

2009 FISMA Executive Summary Report

Executive Summary

In August 2009, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted with C5i Federal, Inc. (C5i) to assist with the completion and coordination of the OIG's input to the Commission's response to Office of Management and Budget (OMB) Memorandum M-09-29 *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* The OMB memorandum provides the instructions and templates for meeting the fiscal year (FY) 2009 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA), Title III, Pub. L. No. 107-347.

C5i commenced work on this project in September 2009, after the final FISMA questionnaires were promulgated by OMB. C5i's tasks included completing the OIG portion of the FISMA reporting template (Section C) and developing an Executive Summary Report that communicates the Inspector General's (IG) response to the 2009 FISMA submission. In addition, the OIG requested separate reports examining the Commission's implementation of encryption technology and the Commission's Privacy Program.

For 2009, OMB only accepted annual FISMA reports that were submitted online, using a new automated reporting tool. This tool was designed to allow manual data entry, as well as the automated upload of data. This report includes our recommended responses to the questions in the 2009 FISMA questionnaires, which were promulgated separately by OMB.

Background. FISMA, 44 U.S.C. § 3541, et seq., is a United States federal law enacted in 2002 as *Title III of the E-Government Act of 2002.* The statute recognizes the importance of information security to the economic and national security interests of the United States and requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FISMA requires agency program officials, chief information officers, and OIG's to conduct annual reviews of the agency's information security and privacy programs and report the results to OMB. OMB then uses the data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with the statute.

FISMA provides the framework for securing the federal government's information technology. All agencies must implement the requirements of FISMA and report annually to OMB and Congress on the effectiveness of their Privacy Program and Privacy Impact Assessment (PIA) processes. OMB uses the information to:

- Help evaluate agency-specific and government-wide privacy performance;
- Develop its annual security report to Congress;
- Assist in improving and maintaining adequate agency privacy performance; and
- Assist in the development of the E-Government Scorecard under the President's Management Agenda.

Objective. The objective for the FISMA assessment was to independently evaluate and report on how the Commission has implemented its mandated information security requirements. This report provides background information, clarification, and recommendations regarding the OIG's response and input to Section C of the OMB reporting template. The 2009 reporting categories and questions are generally the same as they were in 2008, however, some were updated based on security and privacy policies issued throughout the year.

Results. The key findings and results for the 2009 FISMA evaluation include:

- The Commission operates a total of 48 systems. Of those, 46 have been evaluated as having a moderate system impact level. The remaining two systems were evaluated as having a low system impact level.

- The SEC routinely performs oversight and evaluations to ensure information systems used or operated by a contractor of the agency, or other organizations on behalf of the agency, meet applicable requirements.

- The Commission has developed an inventory of major information systems. Performing a full inventory of all systems exceeded the scope of our effort, but through our interviews, document reviews, and research, we ascertained that the inventory is approximately 90 to 100 percent correct.

- The Commission's Plan of Actions & Milestones (POA&M) process provides an effective roadmap for continuous security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool.

- The Commission's overall Certification and Accreditation (C&A) program is assessed as being excellent, and in compliance with applicable regulatory and statutory requirements.

- The Privacy Office has made significant progress in its development of privacy resources, in outreach within the Commission and Regional Offices, and in benchmarking externally with other agencies. However, the policies are still in draft form and therefore, the program is not fully implemented throughout the Commission. Further details about this matter are provided in a separate report.

- The Commission has developed and disseminated formal, documented, configuration management policies and implementing guidance that satisfactorily addresses security configuration management requirements. While not a specific question in the configuration management section of the OMB reporting template, we found some areas of concern in the SEC's encryption policies and procedures that are further detailed in a separate report.

- Federal Desktop Core Configuration (FDCC) has been successfully implemented on all workstations and laptops and appropriate language from Federal Acquisition Regulation (FAR) 2007-004, which modified *Part 39—Acquisition of Information Technology*, is now included in all contracts related to common security settings.

- The Commission has robust incident prevention, detection, response, and reporting capabilities and follows documented policies and procedures for reporting incidents internally, to the United States Computer Emergency Readiness Team (US-CERT), and to law enforcement.

- As of November 15, 2009, Cyber Security Awareness training was successfully completed by 4,101 of 4,383 (94 percent) users.

- The Commission has monitoring systems and policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, and other agency-wide training.

Recommendations. This report does not contain any formal recommendations. However, the OIG proposes that OIT use this Executive Summary report to develop the Commission's annual consolidated FISMA Report, in accordance with OMB Memorandum M-09-29 Reporting *Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

TABLE OF CONTENTS

Tables

Chart

Background and Objective

Background

In June 2009, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted with C5i Federal, Inc. (C5i) to assist with the completion and coordination of the OIG's input to the Commission's response to the Office of Management and Budget (OMB) Memorandum M-09-29 *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* This memorandum provides instructions and templates for meeting the FY 2009 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA), Title III, Pub. L. No. 107-347.

C5i commenced work this evaluation in September 2009, though some activities where delayed until the final online FISMA reporting tools were promulgated by OMB in late October 2009. The purpose of this report is to provide background information, clarification, and recommendations regarding OIG's responses and input to Section C of the OMB reporting template. The 2009 reporting categories and questions are generally the same as they were in 2008. However, some areas were updated based on security and privacy policies issued during the year. Again this year, OMB developed a formal Privacy Assessment Questionnaire that allows agencies the ability to conduct privacy evaluations.

FISMA provides the framework for securing the Federal Government's information technology. All agencies must implement the requirements of FISMA and report annually to the OMB and Congress on the effectiveness of their Privacy Program and Privacy Impact Assessment (PIA) process. OMB uses the information to help evaluate agency-specific and government-wide Privacy performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency privacy performance, and assist in the development of the E-Government Scorecard under the President's Management Agenda.

The following additional documentation is also required to be forwarded, along with the consolidated annual FISMA report:

- Breach Notification Policy, if changed significantly since last year's report;
- Progress update on eliminating unnecessary use of Social Security Numbers (SSN); and

- Progress update on review and reduction of holdings of Personally Identifiable Information (PII).

Agencies are required to submit to OMB their most current documentation related to OMB Memorandum M-07-16, of May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* This information should be appended to the Commission's annual report and includes the agency's breach notification policy; implementation plan and progress update on eliminating unnecessary use of SSN; and implementation plan and progress updates on review and reduction of holdings of PII.

Tasks performed by C5i included completing the OIG portion of the FISMA reporting template (Section C); developing the Executive Summary Report of OIG's Input; and developing a report for the Senior Agency Official for Privacy (SAOP) that assessed the Commission's privacy program. In addition, C5i issued a report examining the Commission's implementation of encryption technology.

This is the third year that OMB guidance provided direction for OIG and Office of Information Technology (OIT) heads to coordinate a consensus with the SAOP on answers to the Privacy questionnaire. In previous years, the OIG independently reported on how the Chairman, Chief Information Officer (CIO), and program officials referred to Privacy training and creation of PIAs for the various information systems. Therefore, the agency's consolidated report presents a cohesive view of the Commission's IT privacy accomplishments and areas for improvement.

Objective

The objective for the FISMA assessment was to independently evaluate and report on how the Commission implemented its mandated information security requirements.

Results

Response to OMB Questions

C5i researched the applicable issue areas and gathered the information needed to complete the OIG's portion of the FISMA reporting template. Our responses to the template questions were based on the results we found.

Question 1: FISMA Systems Inventory

Identify the number of agency and contractor systems by component and Federal Information Processing Standards (FIPS) 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your agency but owned by another federal agency (i.e., ePayroll, etc.,) by component and FIPS 199 impact level.

Response. C5i identified a total of 48 systems. OIT evaluated 46 of these systems as having a moderate FIPS system level impact level and the remaining two systems as having low FIPS system impact levels. Forty-one of these systems are SEC systems and five are contractor-owned or operated systems. We found that the two low-level FIPS system impact systems are contractor systems, as illustrated in Table 1 below.

Table 1: SEC Agency and Contractor Systems and Impact Level

System Impact Level	Agency Systems	Contractor Systems	Total
High System Impact Level	0	0	0
Moderate System Impact Level	41	5	46
Low System Impact Level	0	2	2
Not Categorized	0	0	0
Total	**41**	**7**	**48**

Source: OMB FISMA Web Portal

Agency systems include all systems hosted internally to the SEC that have a signed Categorization Memorandum formally assigning it a FIPS-199 impact level. The SEC continues to investigate legacy applications, some of which may eventually be reported in the inventory as distinct enterprise systems. Others being investigated may include Microsoft Office-based spreadsheets or Access database tools that will be bundled as part of the General Support System (GSS), but are not reported as distinct systems. Similarly, the SEC considers all systems hosted at non-SEC facilities to be contractor systems. This includes both systems hosted by Federal agencies subject to FISMA and systems hosted by commercial firms that are not directly subject to FISMA.

Our results are based on data gathered from a number of sources including the Microsoft Excel spreadsheet entitled *Compliance Workbook* (a document the SEC/OIT office maintains and provided to the OIG), meetings and interviews that were conducted with OIT staff members. In addition, OIT officials reviewed and verified these numbers and concurred with our assessment.

We entered the data in Table 1 above, into the appropriate entry fields in the OMB on-line OIG FISMA reporting tool.

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

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

Response. Certification and Accreditation (C&A) is the process used to evaluate systems and major applications ensuring adherence to formal and established security requirements that are well documented and authorized. C&A is required by FISMA. All systems and applications that reside on U.S. government networks must be evaluated with a formal C&A before being put into production. Systems are re-accredited every three years or sooner if major changes are made.

As shown below in Table 2, C&A has been performed on 48 systems, and 41 systems security controls were tested and reviewed during the past year. We also found that in accordance with applicable policies, contingency plan testing was performed on 30 systems.

Table 2: System Impact Levels for C&A, Tested Systems, and Contingency Plans

System Impact Level	System with C&A	Tested Systems	Contingency Plan
High System Impact Level	0	0	0
Moderate System Impact Level	46	41	30
Low System Impact Level	2	0	0
Not Categorized	0	0	0
Total	**48**	**41**	**30**

Source: OMB FISMA Web Portal

For purposes of FISMA reporting, the Commission identified C&A for all agency and contractor's systems for which a formal authority to operate (accreditation) was granted by the SEC Designated Accrediting Authority (i.e., the Chief Information Officer (CIO)) within a three year period. An additional three month extension or grace period is further permissible. For example, a system that was accredited on September 1, 2005 would be counted as accredited if the re-accreditation was signed and approved within 39 months, (December 1, 2009). Also, the SEC counted all systems scheduled for accreditation on or before September 5, 2009, the cutoff date for the annual report. Beginning in April 2010, the SEC anticipates testing Disaster Recovery plans for systems that were not tested during the past 12 months.

The data in Table 2 was entered in the appropriate data entry fields on the OMB on-line FISMA reporting tool, as shown above.

Question 3: Agency Oversight of Contractor Systems and Quality of Agency Systems Inventory

- The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and National Institute of Standards and Technology (NIST) guidelines, national security policy, and agency policy.

- Does the agency have policies for oversight of contractors? Yes/No.
  If the answer above is Yes, Is the policy implemented?

- The agency has a materially correct inventory of major information systems (including national security systems) operated by or under the control of such agency. Yes/No.

- Does the agency maintain an inventory of interfaces between the agency systems and all other systems, such as those not operated by or under the control of the agency? Yes/No.

- Does the agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the agency? Yes/No.

- The IG generally agrees with the CIO on the number of agency-owned systems. Yes/No.

- The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes/No.
- The agency inventory is maintained and updated at least annually. Yes/No.

- If the IG does not indicate that the agency has a materially correct inventory, please identify any known missing major systems by Component/Bureau, the Unique Project Identifier associated with the systems as presented in the FY 2009 Exhibit 300 (if known), and indicate if the system is an agency or contractor system.

Response. C5i's analysis revealed that that the SEC always performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency, or other organization(s) on behalf of the agency, meet FISMA requirements, OMB policy, NIST guidelines, National Security policy, as well as agency policy.

C5i based its assessment on interviews conducted with several people who are responsible for managing and administering the Commission's information systems security program, our observations, and a review of policies and procedures provided by OIT. We also determined the SEC implemented appropriate policies 24-1.2 *Introduction of New Technology Into the Agency, 24-1.6 Enterprise Architecture,* OD 24-03.01 *Process and Product Assurance Management,* OD 24-03.01.01 *Process and Product Assurance Management: Quality Management,* to perform the oversight and evaluation of contractor information systems.

The quality management (QM) policy "identifies the use of QM for the systematic implementation and use of planning, control, assurance, and improvement activities to align the business goals, quality objectives, and process measures. QM may involve providing information on standards, facilitating a team, or identifying and analyzing a process. Another expectation of QM is to collect measurement data and lessons learned as input to other processes and product assurance management activities. QM resources act as consultants in continuous process improvement activities." QM has specific objectives, such as quality planning, quality control, quality assurance, quality improvement, and helping to ensure successful implementation of a defined program. OIT's Configuration Management and Quality Assurance (CM/QA) branch is responsible for conducting the review, control, and enforcement of processes and product assurance for IT products within OIT and the SEC. They further ensure that quality planning and quality controls are addressed.

In questions 3(c) and 3(d), we found that the Commission developed a complete inventory of major information systems that are operated by or under the control of the Commission. These include an identification of the interfaces between each of the systems and all other systems or networks, including those that are not operated by or under the control of the Commission. The accuracy of the inventory is impossible to assess within the scope of this effort. However, we estimate that the inventory is approximately 90 to 95 percent complete. In March 2008, the OIG conducted an inspection of OIT control over Commission laptops and found OIT did not, at that time, have the proper accountability over laptops.

Based on the finding from the 2008 OIG Inspection report, OIT established an asset management program and issued OD 24-05.09 (01.0) *IT Asset Management Program and OIT-00015-002.0 Asset Inventory Procedure* that clearly outlines the roles and responsibilities of SEC personnel for asset management and the accountability of assets. The directive supplements the prescribed property management control and accountability procedures contained in SEC Regulation (SECR) *9-2, Property Management Program.* We have also reviewed the OIT Asset Inventory report which fully documents all facets of the asset (type of asset, operating system, peripherals, owner, department/organization, serial number(s), associated inventory bar code, etc.). In addition, while we are unable to verify this inventory with 100 percent accuracy, the inventory spreadsheet is a comprehensive document and is updated on a regular basis. Additional documents reviewed: OIT-0056.001.0 *Employee Clearance and Termination Tracking Procedure* and OIT-00057.001.0 – *Maintenance and Update of IT Equipment in the Property Tracking System.*

Regarding question 3(e), we determined the SEC does require agreements to be in place for interfaces between systems it owns or operates and other systems not operated by or under the control of the agency. Several agreements were

provided for C5i's review. These agreements are comprehensive and include detailed information regarding the purpose of the connection, the responsibilities of each party, a description of the systems or networks to be interconnected, procedures for responding to security incidents, disaster and contingency plans, funding considerations, and numerous administrative details. As part of our review, we examined Memoranda of Understanding and Interconnection Security Agreements between the SEC and the Department of Justice, Department of Interior, and other government and contracting entities.

In questions 3(f), 3(g), and 3(h), the OIG generally agrees with the CIO on the number of agency-owned systems, as well as the number of information systems used or operated by SEC contractors. We also noted that the inventory is maintained and updated on an ongoing basis. As noted above, C5i reviewed the inventory processes and procedures. Although we obviously cannot assess the accuracy or completeness of the inventory without conducting an independent inventory, the inventory spreadsheet is a comprehensive document and is updated on a regular basis.[1]

Based on our review, we answered question 3 as depicted in Table 3 below.

Table 3: OIG Response to Question 3

ID	Questions from OMB Questionnaire	Recommended Response
3	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	Yes
3(a)	Does the agency have policies for oversight of contractors?	Yes
3(b)	If the answer above is Yes, Is the policy implemented?	Yes
3(c)	The agency has a materially correct inventory of major information systems (including national security systems) operated by or under the control of such agency.	Yes
3(d)	Does the agency maintain an inventory of interfaces between the agency systems and all other systems, such as those not operated by or under the control of the agency?	Yes
3(e)	Does the agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the agency?	Yes
3(f)	The IG generally agrees with the CIO on the number of agency-owned systems.	Yes

[1] Additional references: OIT-00057.001.0 Maintenance and Update of IT Equipment in the Property Tracking System and OIT-0056.001.0 Employee Clearance and Termination Tracking Procedure.

3(g)	The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3(h)	The agency inventory is maintained and updated at least annually.	Yes

Source: OMB FISMA Web Portal

Question 4: Evaluation of Agency Plan of Actions and Milestones Process

- Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.

- Has the agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts? Yes/No.

- Has the agency fully implemented the policy? Yes/No.

- Is the agency currently managing and operating a POA&M process?

- Is the agency's POA&M process an agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency? Yes/No.

- Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources? Yes/No.

- When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)? Yes/No.

- For systems reviewed:

    a. Are deficiencies tracked and remediated in a timely manner? Yes/No.
    b. Are the remediation plans effective for correcting the security weakness? Yes/No.
    c. Are the estimated dates for remediation reasonable and adhered to? Yes/No.

- Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)? Yes/No.

- Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis? Yes/No.

Response. In response to question 4 on the OMB template, we determined that the Commission maintains an effective POA&M process. The Commission effectively consolidates agency plans to correct security weaknesses found during various security reviews, including audits performed by the OIG, system certification and accreditation, Government Accountability Office (GAO) audits, financial system audits, and critical infrastructure vulnerability assessments. The POA&Ms are tracked using a comprehensive compliance spreadsheet which allows for quarterly tracking and updates. Our assessment is that the OIT's POA&M process provides an effective roadmap for continuous security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool.

In regards to questions 4(a) and 4(b), we found that the SEC's POA&M process is defined and enforced through SEC Policy II 24-04.10.01 (02.0) *IT Security Certification and Accreditation*, dated June 29, 2005. The process has been effectively extended throughout the Commission, including regional offices. The process is centrally managed, includes both Commission and contractor operated systems, and appears to include all known IT security weaknesses associated with Commission systems. In general, the plan will be developed by the C&A Coordinator, with assistance from the Chief Information Security Officer (CISO) and OIT Technical Liaison, and will capture the decisions made regarding mitigating and/or accepting each of the risks enumerated in the Risk Assessment Report. The POA&M describes each risk, lists the selected mitigation (if any) and its cost (in staff or other resources), assigns responsibility for implementing the mitigation, lists the completion date for the mitigation activity, and provides justification if the risk is to be accepted. The C&A Coordinator is responsible for ensuring resources are applied to POA&M activities to meet the milestones therein. The CISO is responsible for monitoring progress of mitigation activities described in the POA&M, and for periodic security compliance reviews of all information systems.

In questions 4(c), 4(f), 4(h), and 4(i), we observed an effective POA&M process has been implemented. When an IT security weakness is identified, program officials quickly develop, implement, and manage POA&Ms for Commission systems. The progress of IT security weakness is reported to the CIO on a quarterly basis, it is centrally tracked, maintained, and POA&M activities are reviewed on a quarterly basis. In addition, OIG recommendations are routinely

incorporated into the POA&M process. The POA&M process effectively prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and they receive appropriately resources to address the deficiency. While no systems were formally reviewed during this evaluation, our responses and conclusions are based on our review of selected POA&M, C&A packages, and interviews conducted with OIT personnel.

In question 4(d), we found the POA&M process has been extended throughout the Commission, to include the regional offices. The process is centrally managed and it includes both Commission and contractor operated systems. Further, it appears to also include known IT security weaknesses associated with the Commission's systems.

Concerning 4(e) and 4(f), we found the POA&M process effectively prioritizes IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner. We also noted that the POA&M process is fully supported by senior leadership, and that appropriate resources are engaged to manage risks to SEC systems and information.

In questions 4(g)1, 4(g)2 and 4(g)3, we found deficiencies are tracked and remediated in a timely manner, the remediation plans are effective in correcting security weaknesses, and the estimated dates for remediation are reasonable and are adhered to. While the SEC is no longer required to submit quarterly updates of their POA&Ms, they have continued to update their standard procedure quarterly to ensure timely remediation and closure of POA&M findings.

Based on our review, we entered the data shown below in Table 4, in response to question 4.

Table 4: OIG Response to Question 4

ID	Question from OMB Questionnaire	Recommended Response
4	Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.	Yes
4(a)	Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?	Yes
4(b)	Has the Agency fully implemented the policy?	Yes
4(c)	Is the Agency currently managing and operating a POA&M process?	Yes

ID	Question from OMB Questionnaire	Recommended Response
4(d)	Is the agency's POA&M process an agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency?	Yes
4(e)	Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?	Yes
4(f)	When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?	Yes
4(g)	For Systems Reviewed:	Yes
4(g) 1	Are deficiencies tracked and remediated in a timely manner?	Yes
4(g) 2	Are the remediation plans effective for correcting the security weakness	Yes
4(g) 3	Are the estimated dates for remediation reasonable and adhered to?	Yes
4(h)	Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?	Yes
4(i)	Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?	Yes

Source: OMB FISMA Web Portal

Question 5: OIG Assessment of the Certification and Accreditation Process

- Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February 2004), Standards for Security Categorization of Federal Information and Information Systems, to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.
- Has the Agency developed and documented an adequate policy for establishing a certification and accreditation process that follows the NIST framework? Yes/No.

- Is the Agency currently managing and operating a C&A process in compliance with its policies? Yes/No.

    - For systems reviewed, does the C&A process adequately provide: (Check all that apply)
        - o Appropriate risk categories
        - o Adequate risk assessments
        - o Selection of appropriate controls
        - o Adequate testing of controls
        - o Regular monitoring of system risks and the adequacy of controls

    - For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented? Yes/No.

Response. C5i found the overall C&A program is excellent. The C&A and risk management processes are well defined, mature, well managed, and compliant with applicable regulatory and statutory requirements. The full C&A packages for the GSS and Automated Procurement System (APS) were provided and were fully reviewed as part of the assessment. We reviewed security plans and the security planning processes, systems tests and evaluations, security control testing procedures and results, incident handling, security awareness training, and configuration and patch management. In 2008, the Commission purchased the U.S. Department of Justice sponsored Cyber Security Assessment and Management (CSAM) application. CSAM is a web-enabled system capable of assisting a Federal agency in meeting its obligations for C&A activities as defined by the OMB, NIST, and FISMA. A sample CSAM screen shot is shown in Figure 1, located in the Appendices of this report.

CSAM enables the SEC to accomplish the following tasks:

- Store information about each agency system and application (inventory of systems).
- Create and maintain the System Security Plan for each system.
- Store system-specific documents including Disaster Recovery/Contingency Plan, Authority to Operate Memo, Interface Agreements, etc.
- Store and track vulnerabilities in system POA&M.
- Perform and store results of Risk Assessments and Security Test and Evaluations (ST&E) on each system following the current NIST requirements (Special Publications 800-53 and 800-53A).

- Produce quarterly and annual FISMA reports for OMB using mostly automated CSAM functionality.
- Produce reports showing various aspects of security in the agency's systems, including management snapshots, upcoming and overdue C&A tasks, and detailed reports of open POA&M items.

CSAM was fully deployed at the SEC in March 2009. CSAM is externally hosted by the Department of Justice and contains the SEC's C&A information. CSAM tracks system inventory, including names, security categorization of each information system, status of C&A activities, weakness descriptions and remediation plans in the form of POA&M, NIST 800-53 control assessment results, as well as audit finding maintenance, monitoring, and tracking. The SEC used CSAM to generate FISMA quarterly reports for the past two quarters. In addition, OIT uses CSAM to track GAO and OIG audit findings. OIT Security administers CSAM and it is used by other OIT divisions to track audit findings. GAO's inventory of POA&Ms is shown in Figure 2, located in the Appendices of this report.

OIT expects use of CSAM will provide a consistent approach to C&A in the Commission, allowing documents and status to be located and maintained in a more efficient way than the present manual processes. CSAM is one of two OMB Security Line of Business initiatives.

In response to question 5(a), we found the SEC has developed and documented adequate policy for establishing a certification and accreditation process that follows the NIST framework. The policy[2] establishes uniform policies, responsibilities, and authorities for the C&A of major applications and general support systems at the SEC. The policy further implements higher level policies such as SEC Regulation (SECR) 24-04, *Information Technology Security Program,* Operating Directive (OD) 24-04.10 *IT Security Compliance*, FISMA, and OMB Circular A-130*, Appendix III, Security of Federal Automated Information Resources.*

In question 5(b), we found that the SEC is currently managing and operating a C&A process in compliance with its policies.

In questions 5(c)1, 2, 3, 4 and 5, we found the C&A process adequately provides appropriate risk categories, adequate risk assessments, selection of appropriate controls, adequate testing of controls, and regular monitoring of system risks and the adequacy of controls. The SEC C&A program was developed using guidance from NIST.[3] SEC Policy II 24-04.10.01 (02.0) *Implementing Instruction:*

[2] SEC II 24-04.10.01 (02.0) *IT Security Certification and Accreditation*, dated June 29, 2005.
[3] See 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems,* NIST 800-53 *Recommended Security Controls for Federal Information Systems and*

IT Security Certification and Accreditation (June 29, 2005) has established "the uniform policies, responsibility, and authorities for the C&A of major applications and general support systems at the SEC." We reviewed data provided by SEC (i.e., ST&E, POA&M, System Security Plan, and Risk Assessment) and all the data provided supports our conclusion that SEC clearly applies the guidance and best practices defined in the NIST and OMB guidance. The Commission's C&As are performed by an independent third-party, the Science Applications International Corporation (SAIC), which ensures an independent evaluation and assessment of the systems to be certified and accredited.

In question 5(d), we found the authorizing official is presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented. As referenced in the previous questions, the SEC has a very thorough C&A process that was developed using NIST and OMB guidance.

Examples of POA&M entry pages are shown in Figure 3 and 4, located in the Appendices of this report. Our response to question 5 is shown below in Table 5.

Table 5: OIG Response to Question 5

ID	Question from OMB Questionnaire	Recommended Response
5	Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February 2004), Standards for Security Categorization of Federal Information and Information Systems, to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.	See text below
5(a)	Has the Agency developed and documented an adequate policy for establishing a certification and accreditation process that follows the NIST framework?	Yes
5(b)	Is the Agency currently managing and operating a C&A process in compliance with its policies?	Yes
5(c)	For systems reviewed, does the C&A process adequately provide: (check all that apply)	
5(c)1	Appropriate risk categories	Check Box
5(c)2	Adequate risk assessments	Check Box
5(c)3	Selection of appropriate controls	Check Box
5(c)4	Adequate testing of controls	Check Box
5(c)5	Regular monitoring of system risks and the adequacy of controls	Check Box
5(d)	For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented?	Yes

Source: OMB FISMA Web Portal

We provided the following information in the comment box for Question 5:

> "C5i found the overall C&A program to be excellent. The SEC C&A program was developed using guidance from NIST 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems,* NIST 800-53 *Recommended Security Controls for Federal Information Systems and Organizations,* NIST 800-53A *Guide for Assessing the Security Controls in Federal Information Systems,* and OMB Circular A-130 *Security of Federal Automated Information Resources.* SEC Policy II 24-04.10.01 (02.0) *Implementing Instruction: IT Security*

Certification and Accreditation (June 29, 2005) has established "the uniform policies, responsibility, and authorities for the C&A of major applications and general support systems at the SEC". We reviewed artifacts provided by SEC (ST&E, POA&M, System Security Plan, and Risk Assessment) – specifically for GSS and APS - and all artifacts support our conclusion that SEC clearly applies the guidance and best practices defined in the NIST and OMB guidance. The C&As are performed by an independent third-party (SAIC) ensuring an independent evaluation and assessment of the systems to be certified and accredited."

Question 6: OIG Assessment of Privacy Program and PIA Process

- Provide a qualitative assessment of the agency's process, as discussed in Section D, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.

- Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information? Yes/No.

- Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies? Yes/No.

- Has the Agency developed and documented an adequate policy for Privacy Impact Assessments? Yes/No/NA.

- Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate privacy impact assessments? Yes/No/NA.

Response. During our assessment of the privacy program, we identified some significant problems with its policies, specifically the lack of approved and implemented policies. Currently, the SEC has only finalized one privacy policy for PII. The OIT Privacy Office has devoted a significant amount of time and money to drafting new policy documents and implementing guidance.

When the Privacy office transitioned to OIT, a contractor was brought in to review the existing draft SECR 31-1 and to draft other SEC privacy policies for review. Specifically, the contractor was to perform the tasks shown below.

- *C.3.4.8 Policy Review and Development*.

- *C.3.4.8.1 Current Policies. The contractor shall review current privacy policies, procedures, standards, and guidelines for conformance with current federal requirements and industry standards. The contractor shall address the content and effectiveness of SEC documents for adequacy and consistency with legislation, regulations, and guidelines considering the SEC mission.*

- *C.3.4.8.2 New Requirements Review. The contractor shall review and comment on new and proposed policies, legislation, standards, and guidance from federal policy authorities such as circulars and memoranda from OMB. The contractor shall keep the Privacy Office informed of all new privacy issues, topics, policy, and guidance in a timely manner. The contractor shall develop and deliver to the TM for review and approval any required guidance and memoranda on new privacy requirements, topics, and issues.*

- *C.3.4.8.3 Policy Changes. The contractor shall work with SEC personnel to develop or update internal and web-based privacy policies, procedures, standards, and guidelines based on new federal legislation, regulations, policies, standards, and guidelines to serve as the foundation of SEC privacy practices. The contractor shall update the documents as required by new guidelines. The contractor shall deliver these documents to the TM for review and approval.*

For clarity, below is OIT's Policy development/approval process:

1. [redacted]
   a) [redacted]
   b) [redacted]
   c) [redacted]
   d) [redacted]

2. [redacted]
   a) [redacted]

b) [redacted]
c) [redacted]
d) [redacted]
e) [redacted]

3. [redacted]

4. [redacted]

a) [redacted]
b) [redacted]
c) [redacted]
d) [redacted]

5. [redacted]

6. [redacted]

7. [redacted]

8. [redacted]

9. [redacted]

The following documents are posted on OIT's website to assist in preparing policy documents: "IT Policy Development Process," "Writing Tips and Tools and II 24-06.05.01," Preparing and Approving Information Technology-Related Policy."

The *Draft* SECR 31-1 policy was initially submitted to the IRM branch in March 2007, per OIT policy review process, and changed hands in IRM in September 2007 due to at that time, the OIT Policy Manager leaving the SEC. This resulted in several internal iterations of the draft SECR 31-1. Subsequently and pursuant to OMB Memo 07-16, additional draft policies were submitted to IRM for review. These included policies for breach notification (Privacy Incident Management); Reduction of SSNs; and Rules of Conduct for Safeguarding PII.

On the dates listed below, OIT issued the following policy documents for external reviews.

The OED provided comments to the SECR 24.08 Privacy Program on December 8, 2008, which resulted in restructuring the privacy tiered framework and essentially redrafting the SECR. As a result of the redrafted SECR, policy provisions for *Use and Reduction of SSNs and Rules of Conduct* were incorporated into the draft SECR. The Privacy Office met with the OED and discussed their comments and plans to revise policy at the agency. Based on that meeting and written comments, another draft SECR with attachments was provided to OED on March 31, 2009. The OED requested clarification, and in some instances, additional information such as sources of definitions. The OED then restructured the outline of the document and edited/added content, and

provide to OIT a rewrite of the SECR on November 17, 2009, including renaming the SECR to *Management and Protection of Privacy Act Records and other PII.*[4] The draft OD, Privacy Incident Management is still under OED review. Accordingly, these documents have not been formally approved, due to delays within the Commission. Therefore, we cannot state with assurance that the SEC is currently managing and operating its privacy program with the appropriate controls. Although the Privacy Office has made some progress with acquiring resources, performing outreach efforts within the Commission and Regional offices, as well as benchmarking with external agencies, the absence of formalized policies limit the Commission's ability to implement an effective privacy program.

In reviewing the *Draft* policies for Privacy Incident Management and the Privacy Program,[5] we found it thoroughly documents the roles, responsibilities, and procedures.[6] The *Draft* policies we reviewed were still under revision. Therefore, we cannot comment on whether the newly-drafted policy contains the same information as the *Draft* policies we reviewed for the 2009 FISMA reporting.

The Commission continues to make progress in their outreach to SEC Divisions, Offices and Regional Offices to increase compliance with privacy documentation – Privacy Analysis Worksheets, PIA, and Privacy Act System of Records Notices for programs and systems involving PII. Compliance efforts included updating and disseminating the *Privacy Impact Assessment Guide* (January 2007) and conducting training and seminars to apprise employees and contractors regarding the requirements. Additionally, the Privacy Office conducted a review of its existing inventory of System of Records Notice for the purpose of reducing the use of SSNs within the Commission.

In question 6(a) of the reporting template, we found the SEC Privacy Program and PIA processes will be implemented with the approval of the *Draft* SEC Regulation (SECR) 24-08 *Management and Protection of Privacy Act Records*

[4] Since the submission of the responses to the FISMA questionnaires, a draft policy was submitted on December 17, 2009 for external and internal OIT management review with a January 18, 2010 comment due date.
[5] SECR 24-08 (01.0) *SEC Regulation: Privacy Program* and OD 24-08.07 (01.0) *Operating Directive: Privacy Incident Management)*.
[6] The guidance was based on *The Privacy Act of 1974*, Title 5 U.S. C. §552a; *Federal Information Security Management Act (FISMA) of 2002*, *E-Government Act of 2002* Public Law 107-347, Title III; OMB Memorandum 05-08 (M-05-08), *Designation of Senior Agency Officials for Privacy*; OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*; *Regulations Pertaining to the Privacy of Individuals and Systems of Records Maintained by the Commission*, Title 17 C.F.R § 200.301 – 200.313, and OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

and Other PII. The Commission has identified appropriate responsible personnel, including a SAOP/CIO and Chief Privacy Officer (CPO).

In question 6(b), we found the SEC is currently developing a privacy program with appropriate controls. Though *draft* policy has been developed, it has not been implemented.

Regarding question 6(c), we found OIT developed a *Privacy Impact Assessment Guide* (January 2007) and intends to formally document its PIA process with the approval of the SECR 24-08, *Management and Protection of Privacy Act Records and other PII*, which consists of governing policy.

In question 6(d), we found that the SEC is drafting policies that are consistent with guidance provided by the applicable federal laws and regulations.[7] However, these policies (SECR 24-08 Management and Protection of Privacy Act Records and other PII and OD 24-08.07 Operating Directive: Privacy Incident Management) are still in DRAFT and have not been approved and implemented throughout the Commission. We must note that OIT developed a Privacy Impact Assessment Guide (January 2007) and intends to formally document its PIA process once the SECR is approved.

We provided our response to question 6 as shown in Table 6.

Table 6: OIG Response to Question 6

ID	Question from OMB Questionnaire	Recommended Response
6	Provide a qualitative assessment of the agency's process, as discussed in Section D, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.	See text below
6(a)	Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information?	No
6(b)	Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies?	No

[7] For example The Privacy Act of 1974, Title 5 U.S. C. §552a; Federal Information Security Management Act (FISMA) of 2002, E-Government Act of 2002 Public Law 107-347, Title III; OMB Memorandum 05-08 (M-05-08), Designation of Senior Agency Officials for Privacy; OMB Circular A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals; Regulations Pertaining to the Privacy of Individuals and Systems of Records Maintained by the Commission, Title 17 C.F.R § 200.301 – 200.313).

ID	Question from OMB Questionnaire	Recommended Response
6(c)	Has the Agency developed and documented an adequate policy for Privacy Impact Assessments?	No
6(d)	Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate privacy impact assessments?	No

Source: OMB FISMA Web Portal

Question 7: Configuration Management

- Is there an agency-wide security configuration policy? Yes/No.
- What tools, techniques is your agency using for monitoring compliance?
- Indicate the status of the implementation of Federal Desktop Core Configuration (FDCC) at your agency:

    - Agency has documented deviations from FDCC standard configuration. Yes/No.

    - New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes/No.

Response. C5i noted that the Commission has developed and disseminated formal, documented, configuration management policies and implementing guidance that addresses project configuration management. The policy is set forth in II 24-03.01.02(01.0) *Implementing Instruction Process and Product Assurance Management Configuration Management*, dated December 21, 2005 and II 24-04.04.02 (01.1), *Implementing Instruction for IT Security Configuration Management.*

These Implementing Instructions establish uniform policies, authorities, responsibilities, and procedures for IT security configuration management as directed in Operating Directive (OD) 24-04.04*, IT Security Operations and Communications Security Management Program*. All policies, authorities, responsibilities, and procedures listed are guided by requirements listed in SEC Regulation (SECR) 24-04, *Information Technology Security Program*.

This instruction identifies configuration management planning as a process managed by OIT's CM/QA branch and other OIT organizations engaged in project IT activities and provides a Project CM Plan template that describes configuration management activities in terms of configuration identification,

baseline management, configuration control, status accounting, audits, and configuration management tools.

While not specifically addressed in the configuration management questions, we found some areas of concern in the SEC Encryption Program and policies which are further detailed in a separate SEC Encryption Program report.

In question 7(a), the [redacted] is used to monitor real-time compliance with an established configuration baseline. The [redacted], in conjunction with administrative procedures already in place through formal SEC change management policies and procedures, effectively manages configuration compliance.

Any changes related to IT security follow the formal change management procedures established by the CM/QA branch, documented in OP 24-03.01.02.07 *Configuration Control: Change Management* and other related policies.

The SEC has implemented appropriate policies 24-1.2 *Introduction of New Technology Into the Agency, 24-1.6 Enterprise Architecture,* OD 24-03.01 *Process and Product Assurance Management,* OD 24-03.01.01 *Process and Product Assurance Management: Quality Management* to perform oversight and evaluation of contractor information systems. The Quality Management (QM) policy "identifies the use of QM for the systematic implementation and use of planning, control, assurance, and improvement activities to align the business goals, quality objectives, and process measures. Effective QM designs, develops, and implements guidance processes that assure accuracy and integrity. QM may involve providing information on standards, facilitating a team, or identifying and analyzing a process. Another expectation of QM is to collect measurement data and lessons learned as input to other process and product assurance management activities. QM resources act as consultants in continuous process improvement activities." QM has specific objectives, i.e., quality planning, quality control, quality assurance, and quality improvement, and helping to ensure successful implementation. OIT's CM/QA branch is responsible for conducting the review, control, and enforcement of the process and product assurance for IT products within OIT and the SEC, as well as ensuring that quality planning and quality control are addressed.
Some of the key components of the change management process are highlighted below, focusing on specific considerations related to IT security. A change request is prepared and initiated by a requester using the enterprise change control tool. The enterprise change control tool is administered by OIT's CM/QA branch within the Office of Enterprise Architecture. The information that a requester inputs into the change control tool generates a System Change Request. The OIT Security Group's Operational Change Control Board (O-CCB)

members review system change requests to evaluate and assess whether there are IT security implications. Information system components (hardware, operating system, utility, and applications) with IT security features require testing prior to the implementation of the change into the production environment, preventing unwarranted downtime of the production environment.[8]

When a change to an existing information system is proposed, the OIT Security Group O-CCB member conducts an impact analysis to determine the effects, if any, on the integrity and availability of the information and information system. This analysis ensures changes do not introduce new vulnerabilities or diminish existing IT security controls. In addition to the impact analysis, IT security testing and evaluation are conducted for proposed changes that have IT security implications and features. Once testing is completed and IT security implications are evaluated and assessed, O-CCB either approves or disapproves the proposed changes. The results of the analysis and any IT security testing and evaluation are documented within the enterprise change control tool.

Question 7(b). The FDCC is an OMB mandate that requires all Federal agencies to standardize the configuration of approximately 300 settings on Windows computers, agency-wide. The reason for this standardization is to strengthen Federal IT security by reducing the opportunity for hackers to access and exploit government computer systems. On September 18, 2009, the SEC OIT/End User Technology branch pushed the FDCC settings to all workstations and laptops by Active Directory Group Policy Object (GPO).

Question 7(c). The SEC had no documented deviations from FDCC standard configuration. The FDCC standard configuration was fully implemented in accordance with SEC OIT Memorandum, September 29, 2009.

Question 7(d). Federal Acquisition Regulation 2007-004 language, which modified *Part 39—Acquisition of Information Technology*, is included in all contracts related to common security settings. These requirements were promulgated in an SEC OIT Memorandum dated September 29, 2009.

Our response to question 7 is shown as follows in Table 7.

[8] See OD 24-03.01-C01*Operations Configuration Control Board (O-CCB) Charter.*

Table 7: OIG Response to Question 7

ID	Question from OMB Questionnaire	Recommended Response
7	Is there an agency-wide security configuration policy?	Yes – See text below
7(a)	What tools, techniques is your agency using for monitoring compliance?	See text below
7(a)1	For each OS/platform/system for which your agency has a configuration policy, please indicate the status of implementation for that policy.	See table below
7(b)	Indicate the status of the implementation of FDCC at your agency:	Yes
7(c)	Agency has documented deviations from FDCC standard configuration.	Yes
7(d)	New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings.	Yes

Source: OMB FISMA Web Portal

Question 7. The [redacted] is used to monitor real-time compliance with an established configuration baseline. This tool, in conjunction with administrative procedures already in place, i.e., Implementation Instructions for Configuration Management within the formal SEC change management policies and procedures, effectively enforces configuration compliance. All system changes follow the formal change management procedures established by OIT's CM/QA branch and are documented in the configuration control operations plan and other related policies.

Although encryption is not a specific FISMA question, our FISMA review included an assessment of the SEC's encryption policies and procedures. During our evaluation, we discovered some areas of concern with encryption implementation. We performed a full evaluation of the SEC's Encryption Program and provided recommendation for improvement in a separate report.

Question 7(a). Changes related to IT security follow the formal change management procedures established by the CM/QA branch, documented in OP 24-03.01.02.07 *Configuration Control: Change Management* and related policies. Some of the key components of the change management process are highlighted below, focusing on specific considerations related to IT security. A change request is prepared and initiated by a requester using the enterprise change control tool. The enterprise change control tool is administered by OIT's CM/QA branch within the Office of Enterprise Architecture. Information the requester puts into the change control tool generates a system change request. Members of OIT's Security Group, O-CCB, review system change requests to evaluate and assess IT security implications. Information system components

(i.e., hardware, operating system, utility, and applications) with IT security features require testing prior to implementing the change into the production environment. This prevents unwarranted production downtime.

When a change to an existing information system is proposed, O-CCB members conduct an impact analysis to determine the effects, if any, on the integrity and availability of the information and information system. This analysis ensures changes do not introduce new vulnerabilities or diminish existing IT security controls. In addition to the impact analysis, IT security testing and evaluation is conducted for all proposed changes that have IT security implications and features. Upon completion of testing and when all IT security implications are evaluated and assessed, the O-CCB approves or disapproves the proposed changes. The results of the analysis and any IT security testing and evaluation are documented in the change control tool. Configuration Policy for OS/Platform/System is illustrated below in Table 8.

Table 8: Configuration Policy for Each OS/Platform/System

OS/Platform/System	Tool/Technique Name	Tool Category	Implementation Status
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]			In Process
[redacted]	[redacted]	Configuration Scanner	Fully Implemented
[redacted]	[redacted]	Configuration Scanner	Fully Implemented
[redacted]	[redacted]	Configuration Scanner	Fully Implemented
[redacted]			Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
Microsoft Office SharePoint Server 2007			In Process
Microsoft Office 2007			In Process
Microsoft Outlook 2007			In Process

OS/Platform/System	Tool/Technique Name	Tool Category	Implementation Status
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
Microsoft Word 2007			In Process
Mysql5			Fully Implemented
[redacted]	[redacted]	Vulnerability Scanners	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanner	Fully Implemented
[redacted]			Fully Implemented
[redacted]	[redacted]	Vulnerability Scanner	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanner	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanner	Fully Implemented
[redacted]	[redacted]	Vulnerability Scanner	Fully Implemented

Source: OMB FISMA Web Portal

Question 8: Incident Reporting

- How often does the agency comply (with) documented policies and procedures for identifying and reporting incidents internally? Answer will be a percentage range.

- How often does the agency comply with documented policies and procedures for timely reporting of incidents to US CERT? Answer will be a percentage range.

- How often does the agency comply documented policy and procedures for reporting to law enforcements? Answer will be a percentage range.

Response. C5i found that the Commission does follow its documented policies and procedures for reporting incidents internally, to the United States Computer Emergency Response Team (US-CERT), and to law enforcement. The SEC has a very robust Incident Response program using guidance and best practices from NIST, OMB, and FISMA.

The SEC has implemented the following policies to address Incident Response processes (details on these processes are provided below): OD 24-04.07 *Information Security Incident Management,* II 24-04.07.01 *Computer Security Incident Response Capability,* OP 24-04.07.01.02 *Handling Inappropriate Usage Incidents,* OP 24-04.07.01.03 *Handling of Denial of Service Incidents,* OP24-04.07.01.04 *Handling Unauthorized Access Incidents,* OP 24-04.07.01.05 *Handling Laptop Theft and Tampering Incidents,* OP 24-04.07.01.05.A01 *Laptop Theft and Tampering Incident Materials, SEC Incident Response Capability Handbook*, and II 24-04.07.01.A01 *SEC Incident Response Capability Handbook.*

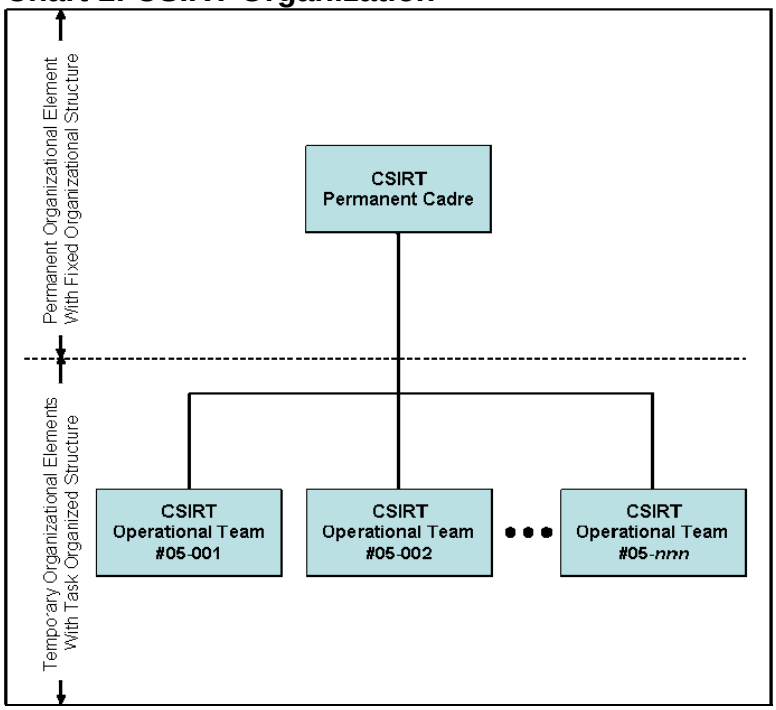
Incident Response Capability Handbook

The Incident Response Capability (IRC) handbook was developed by the SEC to assist in the mission of the SEC Computer Security Incident Response Team (CSIRT). The handbook clearly and fully defines processes and procedures, roles and responsibilities, types of incidents, reporting criteria and timeframes, evidence collection and handling, event categories and incident severity, etc., as well as post-mortem procedures, i.e., lessons learned.

The following excerpt was taken from the IRC handbook:

> "The CSIRT consists of both a permanent cadre and temporary task organized teams. Whereas the permanent cadre is responsible for ensuring the mission readiness of the CSIRT and controlling the operational teams, it is the operational teams that actually perform the hands-on response to security incidents. This organizational construct is depicted in Chart 1 shown below.

Chart 1: CSIRT Organization



Source: Incident Response Capability Handbook

The CSIRT's permanent cadre consists of a manager, senior staff, and supporting staff. Senior staff members of the permanent cadre are selected because they have specific expertise needed in the CSIRT; that is, they have management authority over SEC Federal resources and/or contractor employees that are likely to become members of CSIRT operational teams. Supporting staff are chosen based on their ability to assist with activities in the CSIRT that continue regardless of whether any incident response operations are underway. CSIRT members are responsible for accomplishing much of the administrative, logistical, and training needs of the CSIRT.

CSIRT operational teams are transient. They are chartered by the CSIRT permanent cadre, charged with restoring a safe computing environment when an incident occurs, and task organized to meet the challenges of that individual mission. The CSIRT permanent cadre disbands each operational team once it has accomplished its mission. II 24-04.07.01 documents command and control of the operational teams by the CSIRT permanent cadre. This handbook documents procedures used for hands-on response by the CSIRT operational teams."

The handbook also defines which types of incidents are required to be reported to the US-CERT (based on OMB A-130 and FISMA) and which do not. The types of incidents that are not required to be reported are incidents that are self-

inflicted, did not result in unauthorized access, or were not a result of an attacker's actions. All other incidents require reporting to US-CERT.

Examples of the CSIRT procedures for incident handling from the IRC handbook are illustrated in Tables 9 and 10 below and in Figure 2, located in this report's Appendices.

Table 9: Laptop Theft Response Procedures

Detection and Analysis Stage	Team Member	Status
1. Interview the person the laptop is assigned to using CSIRT-FRM-IH003 to collect the required information. Within one hour file a report with US CERT if there is any possibility that PII has been compromised, per OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information."	CSIRT Manager or Op Team Lead	
2. Alert CISO, OOD, and Chief Privacy Officer that USCERT report has been filed.	CSIRT Manager or Op Team Lead	
3. Determine whether there exists substantial risk to any Government network or mission as a result of the theft.	CSIRT Manager or Op Team Lead	
4. Determine whether any PII has been compromised.	CSIRT Manager or Op Team Lead	
Containment, Eradication, and Recovery Stage		
5. If it is determined that there is substantial risk to any Government network as a result of the theft take appropriate precautions to mitigate the risk, such as revoking the credentials of any user whose credentials were available on, in, or nearby the stolen laptop.	CSIRT Manager or Op Team Lead	
6. If it is determined that any PII may have been compromised, notify the Privacy Officer.	CSIRT Manager or Op Team Lead	
Post-Incident Activity Stage		
7. Create a follow-up report.	Op Team Lead	
8. Hold a lessons learned meeting.	CSIRT Manager	

Source: Incident Response Capability Handbook

Table 10: Unauthorized Access Response Procedure

Detection and Analysis Stage	Team Member	Status
1. Prioritize handling the incident based on its business impact:	CSIRT Manager	
• Identify which resources have been affected and forecast which resources will be affected.	Op Team Lead Op Team SSB Rep Op Team Network Rep	
• Estimate the current technical effect of the incident.	Op Team Lead Op Team SSB Rep Op Team Network Rep	
• Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources.	Op Team Lead Op Team SSB Rep Op Team Network Rep	
• If the incident is ongoing, determine what additional logging may be required to capture evidence of wrongdoing. Affect the logging changes.	Op Team Lead Op Team SSB Rep Op Team Network Rep	
2. Report the incident to the appropriate internal personnel and external organizations.	Op Team Lead	
Containment, Eradication, and Recovery Stage		
3. Perform an initial containment of the incident.	Op Team Lead Op Team SSB Rep Op Team Network Rep	
4. Acquire, preserve, secure, and document evidence.	Forensics Specialist	
5. Confirm the containment of the incident:	Op Team Lead	
• Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion).	Op Team Lead Op Team SSB Rep Op Team Network Rep	
• Implement additional containment measures if necessary.	Op Team Lead Op Team SSB Rep Op Team Network Rep	
6. Eradicate the Vulnerability:		
• Identify and mitigate all vulnerabilities that were exploited.	Op Team SSB Rep Op Team Network Rep	

7. Recover from the incident:		
• Return affected systems to an operationally ready state.	Op Team SSB Rep Op Team Network Rep	
• Confirm that the affected systems are functioning normally.	Op Team SSB Rep Op Team Network Rep	
• If necessary, implement additional monitoring to look for future related activity.	Op Team SSB Rep Op Team Network Rep	
Post-Incident Activity Stage		
8. Create a follow-up report.	Op Team Lead	
9. Hold a lessons learned meeting.	CSIRT Manager	

Source: IRC Handbook

We found that the Commission has robust incident prevention, detection, response, and reporting capabilities. This capability features a number of tools, such as:

[redacted]. The SEC has implemented the [redacted]. The [redacted] is an in-line device that is inserted seamlessly and transparently into the network. As packets pass through the Intrusion Protection System, they are fully inspected to determine whether they are legitimate or malicious. This instantaneous form of protection is the most effective means of preventing attacks from ever reaching their targets. [redacted] provide Application Protection, Performance Protection and Infrastructure Protection at gigabit speeds through total packet inspection. Application Protection capabilities provide fast, accurate, reliable protection from internal and external cyber attacks. Through its Infrastructure Protection capabilities, the [redacted] protects VoIP infrastructure, routers, switches, DNS and other critical infrastructure from targeted attacks and traffic anomalies. [redacted] capabilities enable customers to throttle non-mission critical applications that hijack valuable bandwidth and IT resources, thereby aligning network resources and business-critical application performance.

[redacted] delivers real-time event management with [redacted] As a key component of the [redacted] delivers "forensics on the fly," the ability to drill down from an alert to the source events that triggered the alert. The advanced real-time correlation capability of

[redacted] identifies the relevance of any given event by placing it within context of who, what, where, when and why that event occurred and its impact on business risk. [redacted] correlates incoming events with asset prioritization and vulnerability, user activity, and threat history to deliver accurate and automated prioritization of security risks and compliance violations. The powerful correlation engine of [redacted] processes many millions of log entries down to the few critical events that matter. These incidents are then presented through real-time dashboards, notifications, or reports to the security administrator. Once risks are identified, [redacted] provides a built-in workflow engine that guides risk containment activities including case management and handing off the threat information to [redacted] for threat isolation and remediation options. The [redacted] implementation at the SEC is currently being upgraded to the most recent software version.

[redacted] The [redacted] product offers a rich list of features. The application effectively scans desktops in real-time, and at preprogrammed scheduled times. The program also scans for spyware and adware. [redacted] has an Antivirus Emergency Response Team that continually monitors the worldwide virus activities. The always-on protection guards against viruses, spyware and other Internet threats that may enter Commission systems via e-mail, instant message attachments, Internet downloads, and web browsing.

*Project Einstein II***.** The US-CERT Einstein Program is an initiative that builds cyber-related situational awareness across the Federal government. The program monitors government agencies' networks to facilitate the identification and response to cyber threats and attacks, improve network security, increase the resiliency of critical electronically delivered government services, and enhance the survivability of the Internet. Einstein leverages information technology so that the US-CERT can automate the sharing of critical information across the entire Federal government. Enhanced data sharing between Federal government agencies and the US-CERT provides an advanced cyber view and analysis of the Federal government's critical cyber networks.

[redacted] is the premier computer forensic application available. It gives investigators the ability to image a drive and preserve it in a forensic manner using the [redacted] evidence file format [redacted] a digital evidence container

validated and approved by courts worldwide. [redacted] also contains a full suite of analysis, bookmarking and reporting features. [redacted] and third-party vendors provide support for expanded capabilities to ensure that forensic examiners have the most comprehensive set of utilities.

[redacted] centralizes and streamlines the complete case management lifecycle for cyber and physical incidents and ethics violations. [redacted] web-based solution allows the SEC to capture organizational events that may escalate into incidents, evaluate incident criticality, and assign response team members based on business impact and regulatory requirements. You can also consolidate response procedures, manage investigations end-to-end, and report on trends, losses, recovery efforts and related incidents. Powered by the [redacted], the Incident Management software solution allows you to effectively handle incidents that occur anywhere you do business from detection through analysis and resolution. The SEC's [redacted] implementation is currently being upgraded to the latest software version.

[redacted]. The SEC uses [redacted] test receivers and [redacted] for wireless scanning. [redacted] is a wireless test receiver system that demodulates, sweeps, analyzes, and optimizes all popular 802.11 Wi-Fi network standards including 802.11b/g (2.4 GHz), 802.11n, and even 802.11a (5 GHz). [redacted] is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. [redacted] will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. [redacted]t identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, de-cloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic.

We found local processes and procedure based on NIST SP 800-61, *Computer Security Incident Handling Guide* as well as the following publications:

- NIST SP 800-72, *Guidelines on PDA Forensics*
- NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-101, *Guidelines on Cell Phone Forensics*

- CMU/SEI-2003-HB-001, *Organizational Models For Computer Security Incident Response Teams (CSIRTs)*
- CMU/SEI-20030TR-001, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*
- CMU/SEI-20030HB-002, *Handbook for Computer Security Incident Response Teams (CSIRTs)*
- CMU/SEI-2004-TR-015, *Defining Incident Management Processes for CSIRTs*
- CMU/SEI-20050HB-001, *First Responders Guide to Computer Forensics*
- SAND98-8667, *A Common Language for Computer Security Incidents*, Howard and Longstaff, Sandia National Laboratories

The incident reporting procedures are widely used and fully integrated into the SEC's IT management processes. We assess that the incident response procedures are complied with between 90 and 100 percent of the time.

In question 8(a), we found that the SEC has a robust collaborative relationship with the US-CERT. The SEC complies with documented policies and procedures for timely reporting of incidents to US- CERT between 90 and 100 percent of the time.

In question 8(b), we found that the SEC does comply with the documented policies and procedures for reporting to law enforcement at least 90 percent of the time.

Based on our review and analysis, we answered OMB question 8 as shown in Table 11.

Table 11: OIG Response to Question 8

ID	Question from OMB Questionnaire	Recommended Response
8	How often does the agency comply (with) documented policies and procedures for identifying and reporting incidents internally?	90% to 100%
8(a)	How often does the agency comply with documented policies and procedures for timely reporting of incidents to US CERT?	90% to 100%
8(b)	How often does the agency comply documented policy and procedures for reporting to law enforcement?	90% to 100%

Source: OMB FISMA Web Portal

Question 9: Security Awareness Training

- Has the agency ensured IT security awareness training of all users with log in privileges, including contractors and those employees with significant IT security responsibilities? Provide explanatory detail in the space provided.

- Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log in privileges, and providing them with suitable IT security awareness training? Yes/No/NA.

- Report the following for your agency:

    - Total number of people with log in privileges to agency systems.

    - Number of people with log in privileges to agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003).

    - (The) total number of employees with significant information security responsibilities.
    - Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role-and Performance-Based Model," (April 1998).

Response. OIT Security entered into a second OMB Security line-of-business initiative in 2007 with the Department of State to purchase the Cyber Security Awareness Course known as JSAS. JSAS is an automated computer-based-training that provides standard cyber security training across the Federal Government, and allows for instant reporting and password resets. Users are required to read and review the content, as well as pass a test to complete the training. In addition to the standard cyber security training offered by the Department of State SEC paid for an additional module to support compliance with the SEC Rules of the Road. In 2009, the Rules of the Road went through a major update through the SEC policy review process.

The SEC takes Cyber Security Awareness training very seriously. Individuals who do not successfully complete the training by October 31, 2009 risk having their access credentials frozen until they successfully complete the training.

The screenshot below demonstrates the reporting and tracking capability of the JSAS tool showing that as of November 3, 2009 3,788 of 4,400 users (86 percent) have successfully completed the Cyber Security Awareness Course. As of November 14, 2009, the final numbers reported to OMB are 4,101 of 4,383 users (94 percent completed the Security Awareness Training.

The *SEC Cyber Security Awareness Training Certificate Summary* is illustrated in Figure 3, located in this report's Appendices. Based on our review, we answered question 9 as shown in Table 12 below.

Table 12: **OIG Response to Question 9**

ID	Question from OMB Questionnaire	Recommended Response
9	Has the agency ensured IT security awareness training of all users with log in privileges, including contractors and those employees with significant IT security responsibilities? Provide explanatory detail in the space provided.	Yes
9(a)	Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log in privileges, and providing them with suitable IT security awareness training?	Yes
9(b)	Report the following for your agency:	
9(b)1	Total number of people with log in privileges to agency systems	4383
9(b)2	Number of people with log in privileges to agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003).	4104
9(b)3	Total number of employees with significant information security responsibilities.	453

Source: OMB FISMA Web Portal

Question 10: Peer-To-Peer File Sharing

Does the agency explain policies regarding the use peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training?

Response. The Commission has monitoring systems and policies (SECR 24-04 *Information Technology Security Program* and SECR 24-04.04.02 *IT Security Configuration Management)* covering the use of collaborative web technologies

and peer-to-peer file sharing in IT security awareness, ethics, or other agency-wide training courses. For example, the SEC Rules of the Road (SECR 24-04-A01) user behavior policy prohibits the access or use of peer-to-peer software/systems within the SEC network. Additionally, the prohibited use of peer-to-peer software is addressed as a module in the Commission's annual cyber security training course.

Acronyms

APS	Automated Procurement System
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM/QA	Configuration Management/Quality Assurance
CPO	Chief Privacy Officer
CSAM	Cyber Security Assessment and Management
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Management Act
GAO	Government Accountability Office
GPO	Group Policy Objective
GSS	General Support System
HIDS	Host-Based Intrusion Detection Systems
IDS	Intrusion Detection System
IRC	Incident Response Capability
JSAS	Cyber-Security Awareness Course
NIST	National Institute of Standards and Technology
O-CCB	Operational Change Control Board
OED	Office of the Executive Director
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget

PIA	Privacy Impact Assessment
PII	Personally Identifying Information
PIRT	Privacy Incident Response Team
POA&M	Plan of Action and Milestone
QM	Quality Management
SAOP	Senior Agency Official for Privacy
SEC	The U.S. Securities and Exchange Commission
SSN	Social Security Number
ST&E	Security Test and Evaluation
US-CERT	United States Computer Emergency Readiness Team

Scope and Methodology

This review was not conducted in accordance with government auditing standards.

Scope. The scope of this effort included all systems owned or operated by the Commission or its contractors on behalf of the Commission.

Methodology. To meet the evaluation objective to assess the FISMA and report on how the Commission implemented its mandated information security requirements, C5i completed the OIG portion of the 2009 FISMA reporting template and based its responses on interviews with key personnel, independent observations, and the examination of supporting documentation.

Interviews with key personnel included systems owners, business-line managers, OIT representatives, and OIG personnel. Personnel were interviewed regarding the issues germane to completing the OIG portion of the 2009 FISMA reporting template. Areas discussed included:

- Processes and procedures for maintaining and inventory of information systems and tangible equipment (including portable devices).
- Certification and accreditation processes and procedures.
- Implementation and testing of security controls.
- Contingency planning and testing.
- Commission oversight of contractor systems.
- POA&M processes and procedures.
- Privacy program and privacy impact assessments.
- Configuration management.
- Incident reporting.
- Security awareness training.
- Collaborative web technologies and peer to peer file sharing.
- E-authentication risk assessments.

C5i also reviewed an extensive collection of system artifacts, policies, and other documentation relating to the systems and issues that were identified.

Management Controls. We reviewed the existing controls that were considered significant for FISMA and within the context of the evaluation objectives.

Prior Audit Coverage. We conducted an assessment of the Commission's FISMA program in 2008. The review looked at the FISMA major security areas as well as performed an assessment of two of the Agencies information systems; the Complaints/Tips/Referrals, and the Office of Compliance Inspections and Examinations Adviser Surveillance Intelligence System applications. The report contained three recommendations and revealed that while there were no significant issues with the systems, there were some problems with the overall security program. Not all the report recommendations have been closed. Specifically we recommended that:

- OIT complete the security controls and contingency plan testing for the remaining systems.
- OIT address the requirements for FDCC to include:
    - Adopting and implementing the FDCC standard configurations and documenting any deviations.
    - Modifying all contracts related to common security settings to include the New Federal Acquisition Regulation 2007-004 language.
    - Implementing the FDCC security settings for all Windows XP and VISTA computing systems.

Criteria

OMB Memorandum M-09-29, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* This memorandum provides instructions for meeting agency FY 2009 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). It also includes reporting instructions for agency privacy management programs.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* May 22, 2007*.* This memorandum requires agencies to develop and implement a breach5 notification policy. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974.

OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* July 12, 2006. This memorandum provides updated guidance on the reporting of security incidents involving personally identifiable information and to remind you of existing requirements, and explain new requirements your agency will need to provide addressing security and privacy in your fiscal year 2009 budget submissions for information technology.

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006). This memorandum recommends a number of actions necessary to protect sensitive information.

OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006). This memorandum reemphasizes agency responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and to train employees on their responsibilities.

OMB Memorandum M-03-22, *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002,* September 30, 2003. This memorandum provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

NIST SP 800-72, *Guidelines on PDA Forensics*. This guide provides an in-depth look into PDAs and explaining the technologies involved and their relationship to

forensic procedures. It covers three families of devices – Pocket PC, Palm OS, and Linux-based PDAs – and the characteristics of their associated operating system.

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*. This publication provides recommendations for improving an organizations malware incident prevention measures. It also gives extensive recommendations for enhancing an organizations existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. The recommendations address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools such as backdoors and rootkits. The recommendations encompass various transmission mechanisms, including network services (e.g., e-mail, Web browsing, file sharing) and removable media.

NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response.* This guide provides detailed information on establishing a forensic capability, including the development of policies and procedures. Its focus is primarily on using forensic techniques to assist with computer security incident response, but much of the material is also applicable to other situations.

NIST SP 800-101, *Guidelines on Cell Phone Forensics.* The objective of the guide is twofold: (1) To help organizations evolve appropriate policies and procedures for dealing with cell phones; and (2) To prepare forensic specialists to contend with new circumstances involving cell phones when they arise.

CMU/SEI-2003-HB-001, *Organizational Models For Computer Security Incident Response Teams (CSIRTs).* This handbook describes different organizational models for implementing incident handling capabilities, including each model's advantages and disadvantages and the kinds of incident management services that best fit with it. An earlier SEI publication, the Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-HB-002), provided the baselines for establishing incident response capabilities.

CMU/SEI-20030TR-001, *State of the Practice of Computer Security Incident Response Teams (CSIRTs).* This report provides an objective study of the state of the practice of incident response, based on information about how CSIRTs around the world are operating. It covers CSIRT services, projects, processes, structures, and literature, as well as training, legal, and operational issues.

CMU/SEI-2003-HB-002, *Handbook for Computer Security Incident Response Teams (CSIRTs).* This report proposes an intrusion-aware design model called trustworthy refinement through intrusion-aware design (TRIAD). TRIAD helps information system decision makers formulate and maintain a coherent,

justifiable, and affordable survivability strategy that addresses mission-compromising threats for their organization.

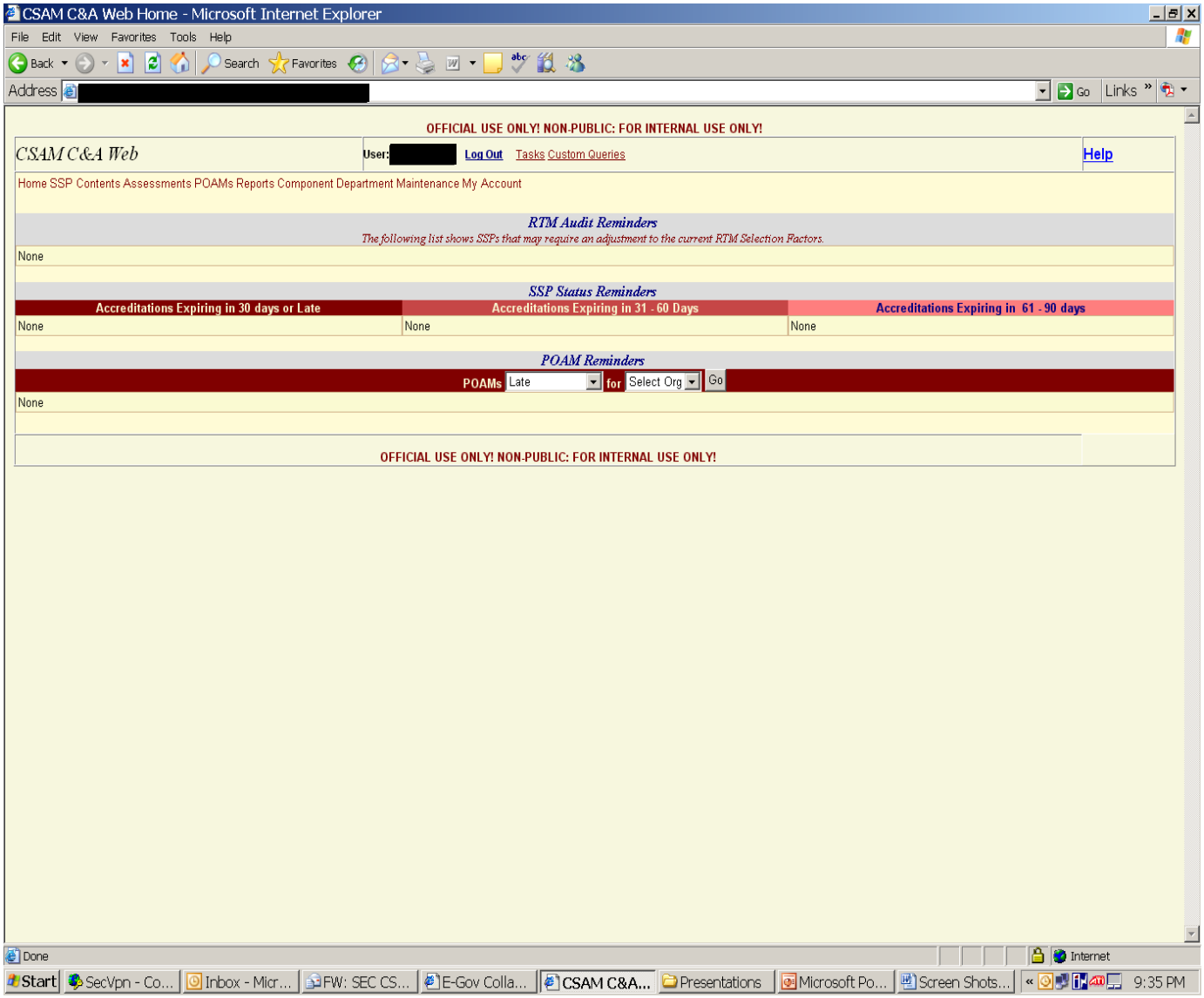
CMU/SEI-2004-TR-015, *Defining Incident Management Processes for CSIRTs.* This report presents a prototype best practice model for performing incident management processes and functions. It defines the model through five high-level incident management processes: Prepare/Sustain/Improve, Protect Infrastructure, Detect Events, Triage Events, and Respond. Workflow diagrams and descriptions are provided for each of these processes.

CMU/SEI-2005-HB-001, *First Responders Guide to Computer Forensics.* This handbook is for technical staff members charged with administering and securing information systems and networks. It targets a critical training gap in the fields of information security, computer forensics, and incident response: performing basic forensic data collection.

SAND98-8667, *A Common Language for Computer Security Incidents*. This paper presents the results of a project to develop a common language for computer security incidents. This project results from cooperation between the Security and Networking Research Group at the Sandia National Laboratories, Livermore, CA, and the CERT® Coordination Center at Carnegie Mellon University, Pittsburgh, PA.

CSAM Screenshots

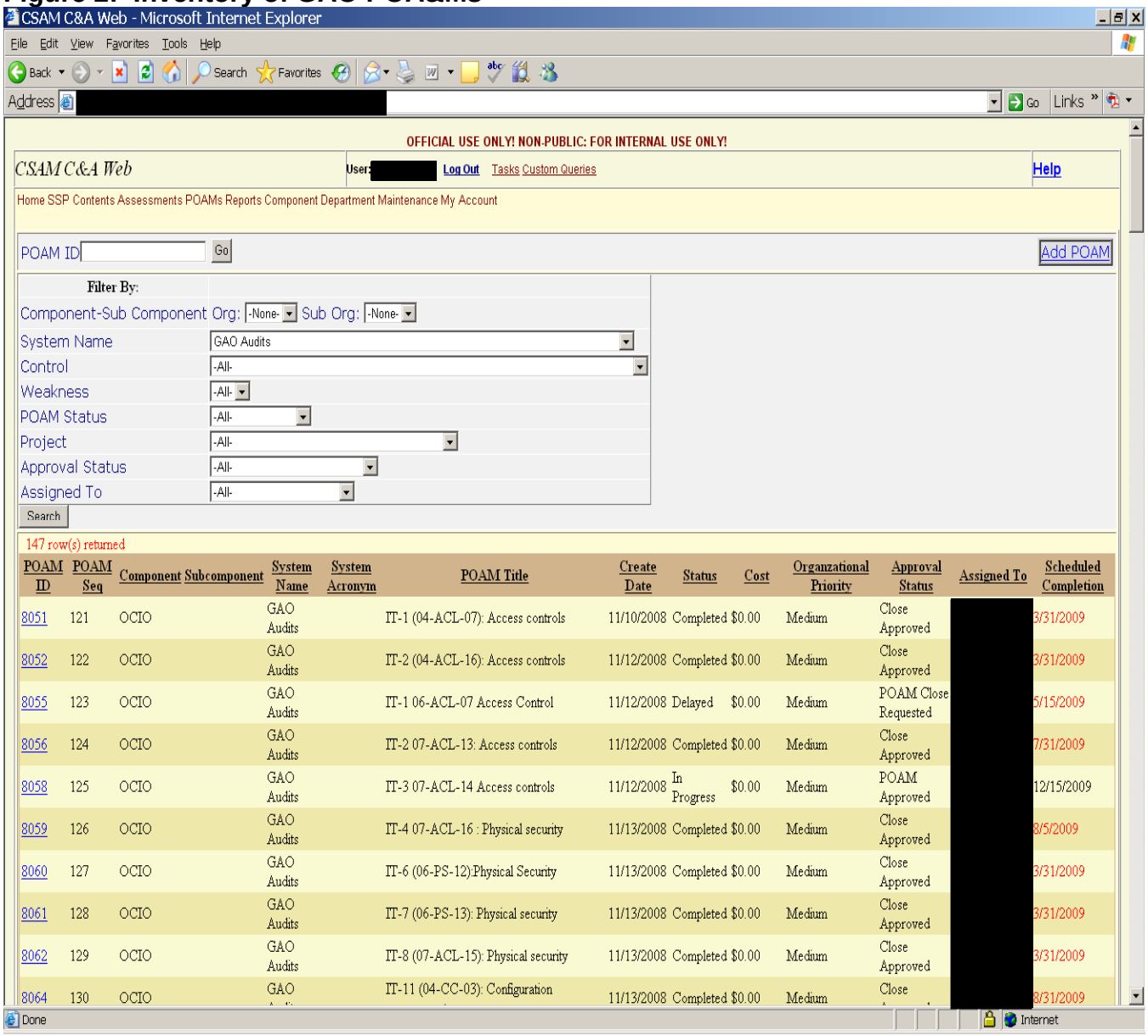
Figure 1: CSAM Screenshots



Source: CSAM Home Page

Inventory of GAO POA&Ms

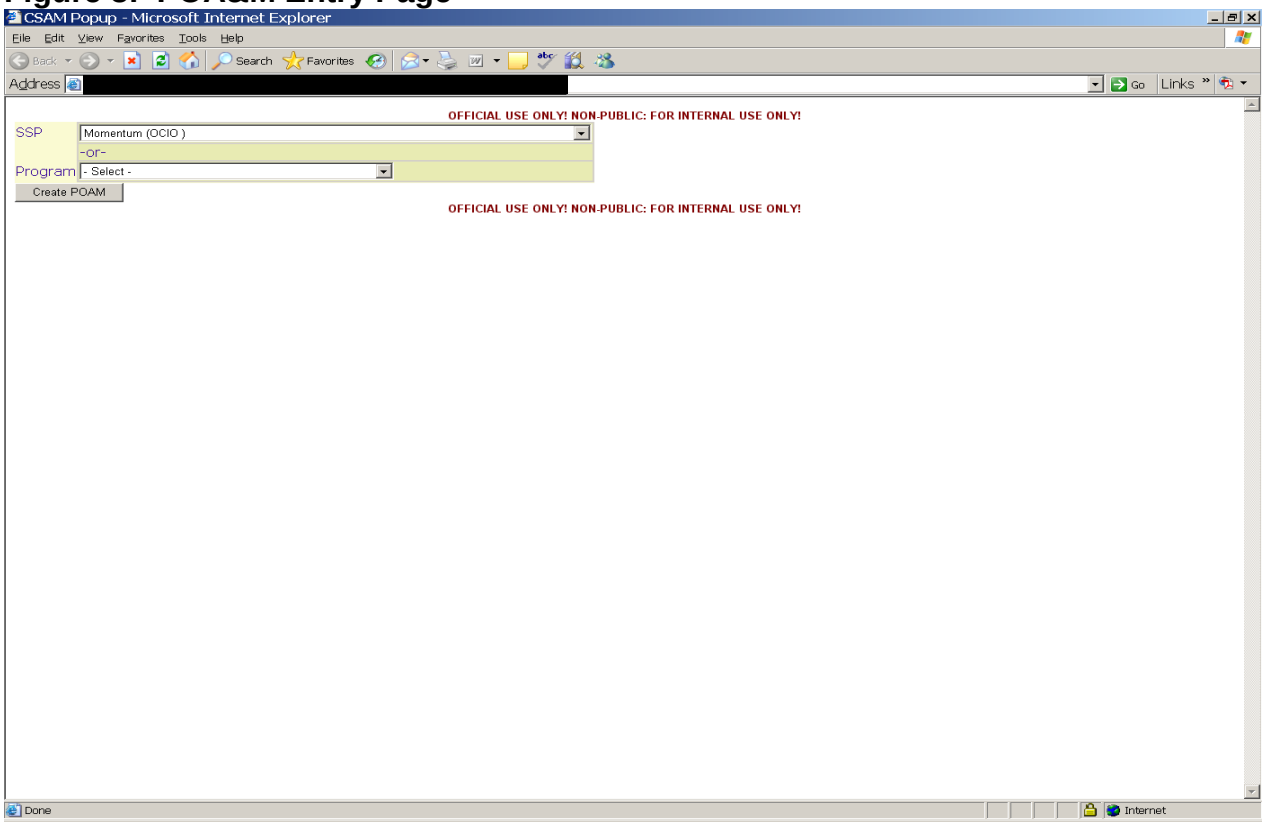
Figure 2: Inventory of GAO POA&Ms



Source: CSAM Home Page

POA&M Entry Page

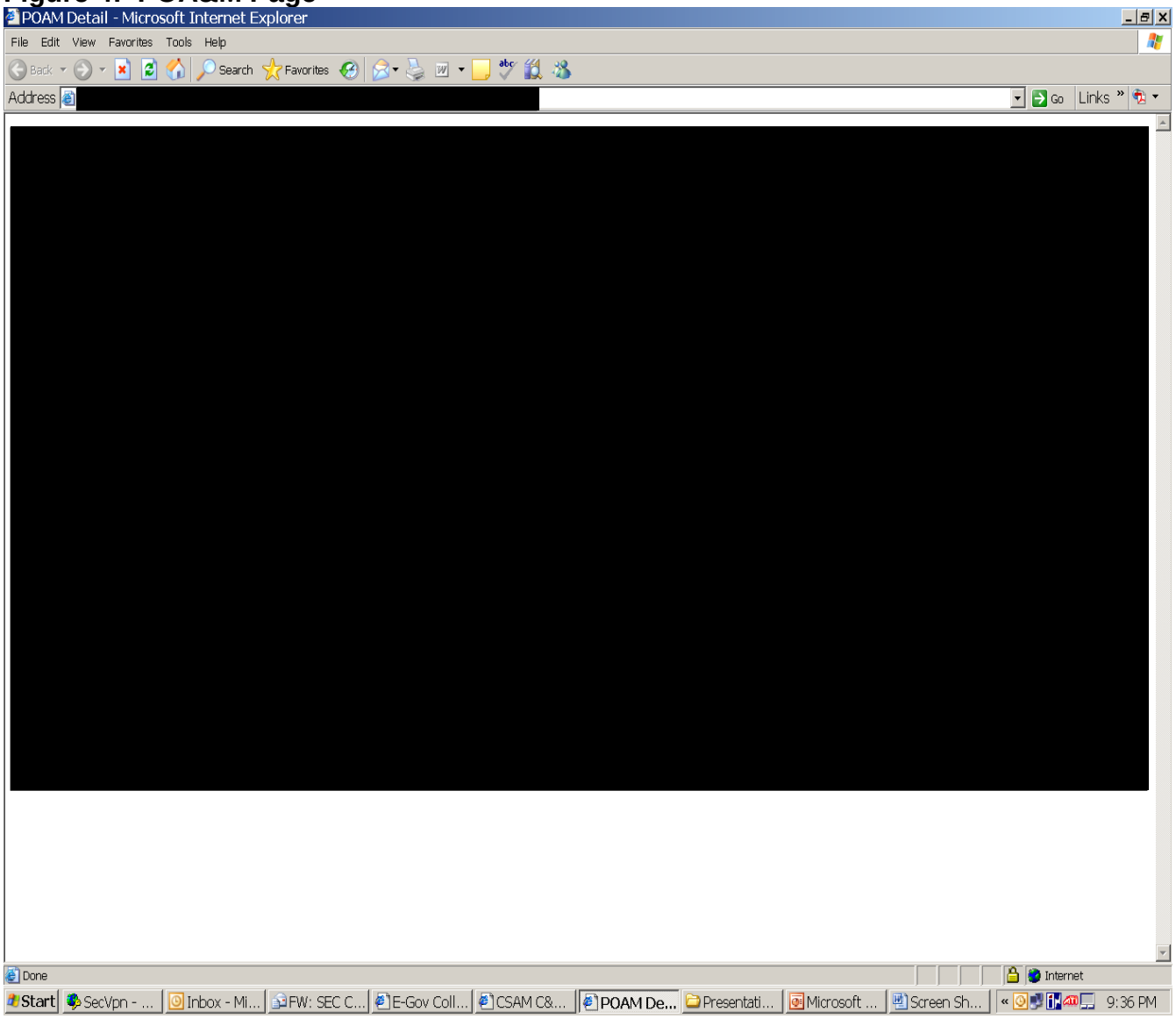
Figure 3: POA&M Entry Page



Source: CSAM Home Page

POA&M Page

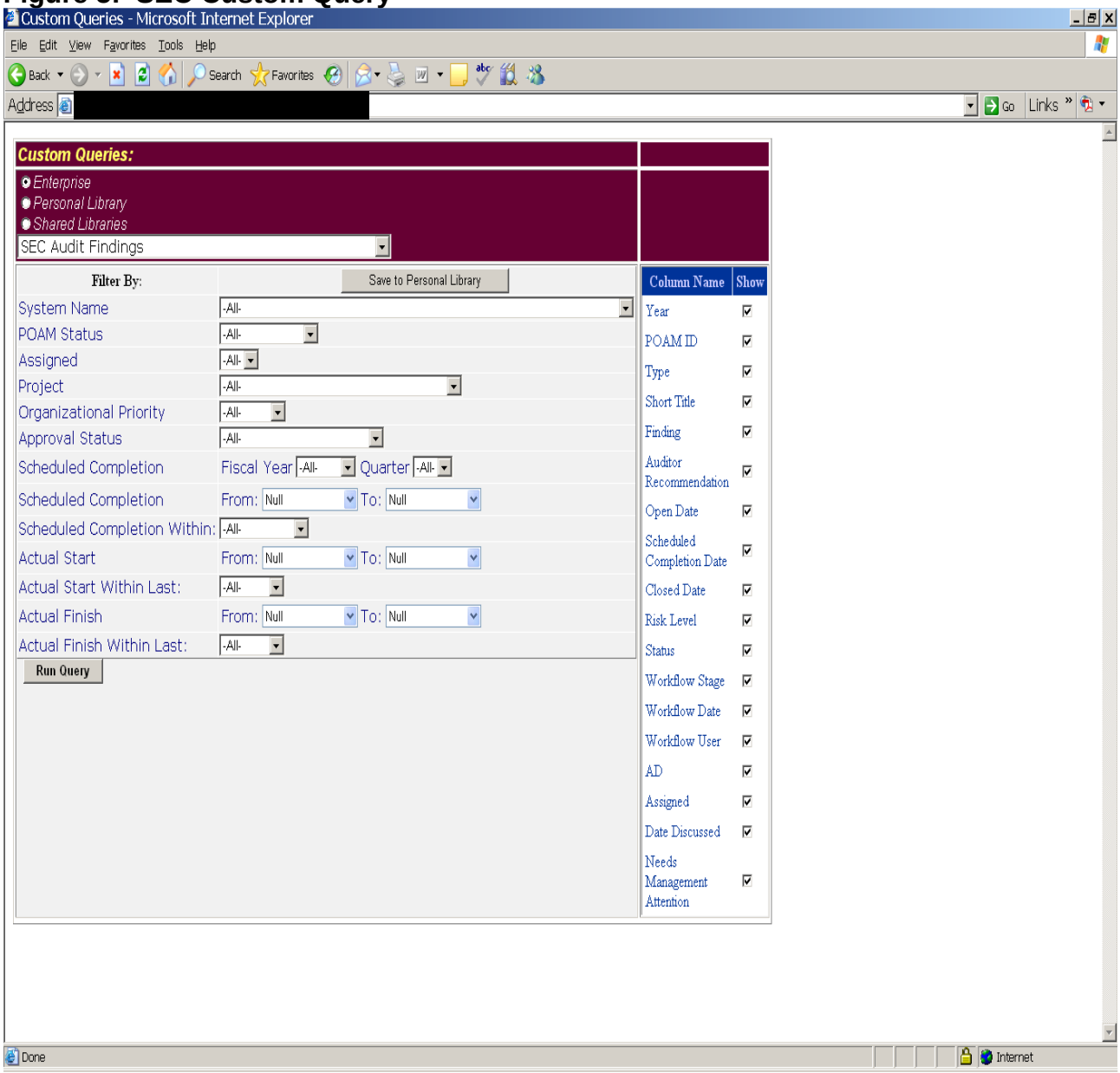
Figure 4: POA&M Page



Source: CSAM Home Page

SEC Custom Query

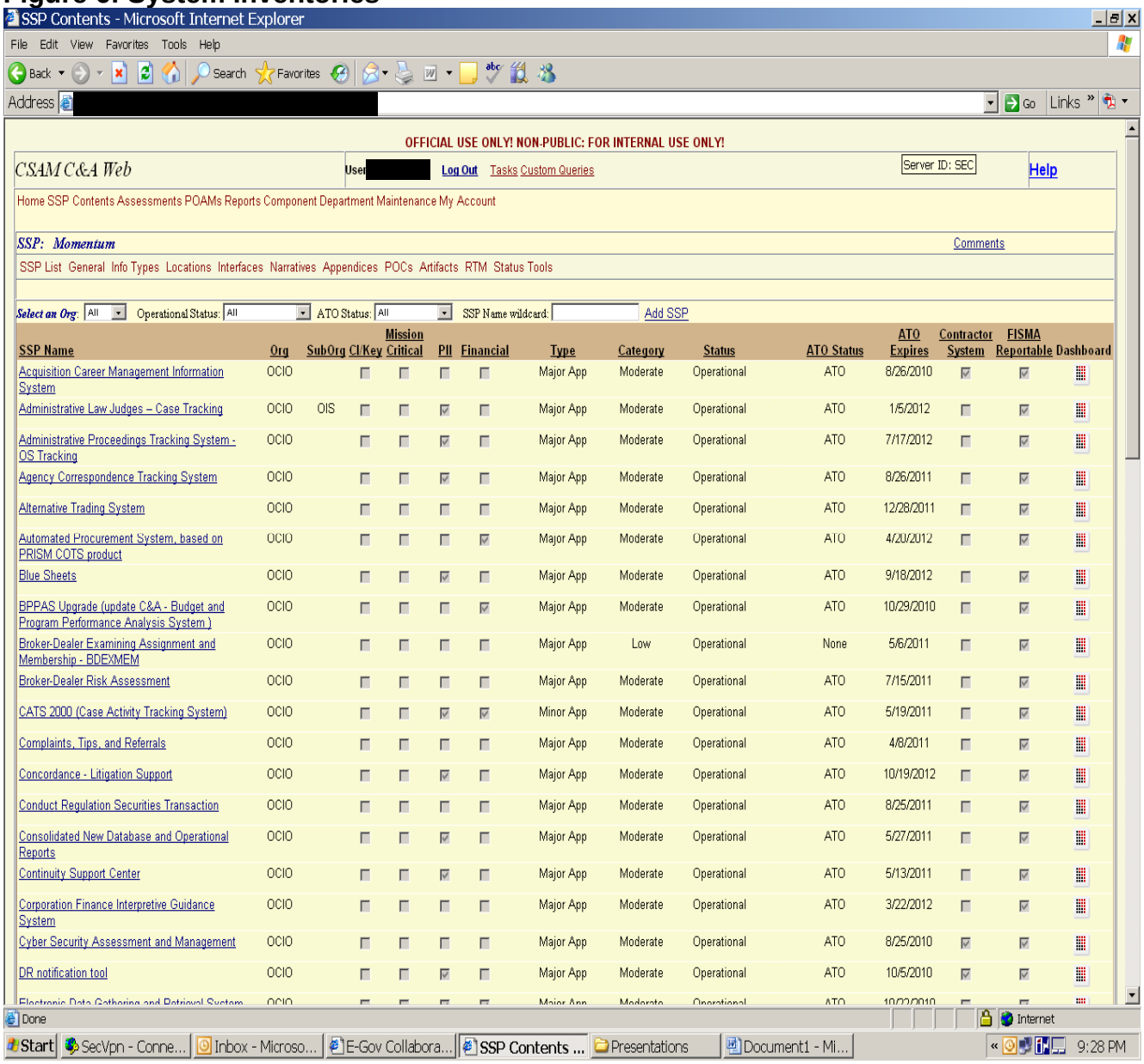
Figure 5: SEC Custom Query



Source: CSAM Home Page

System Inventories

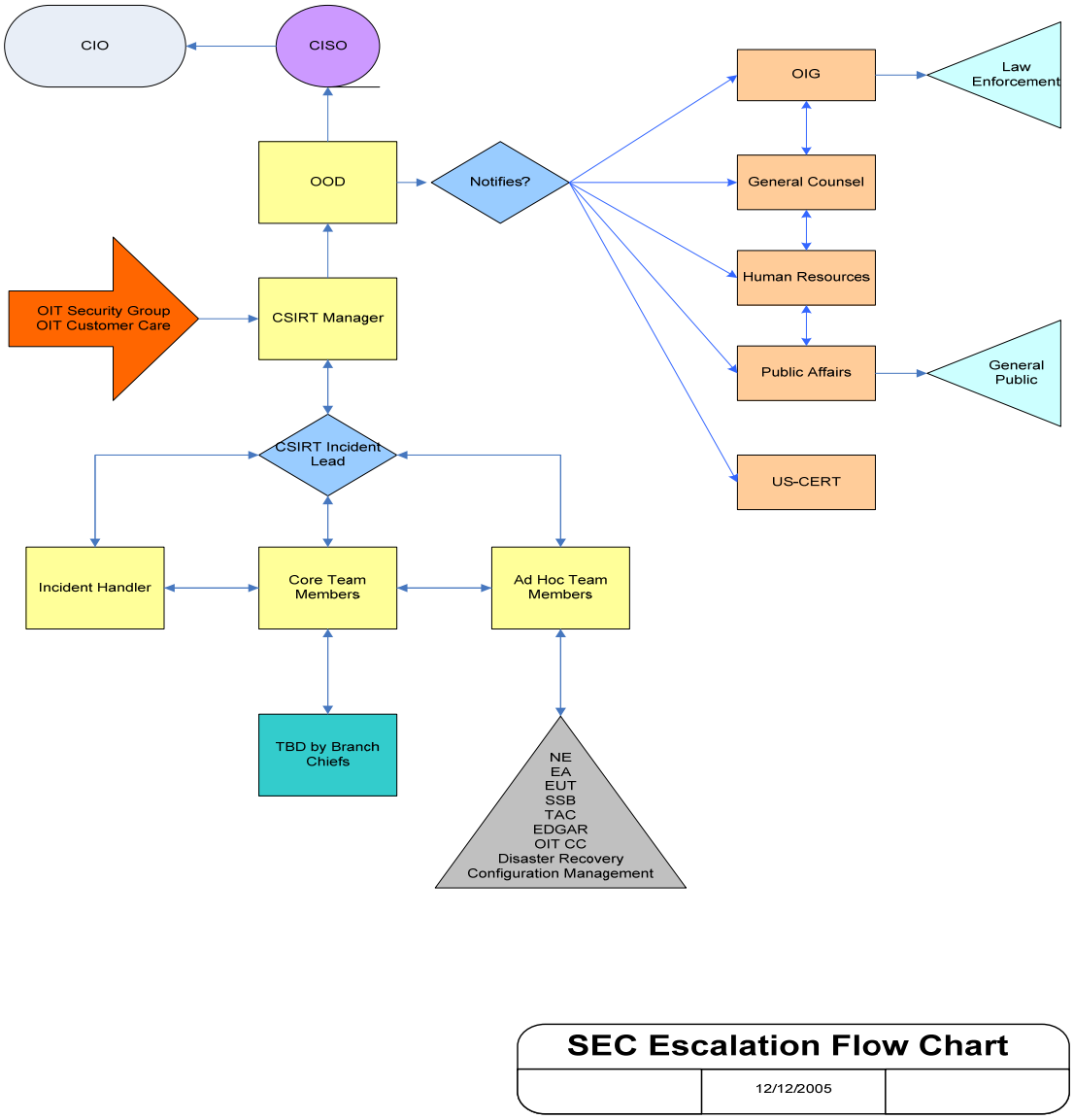
Figure 6: System Inventories



Source: CSAM Home Page

Incident Escalation Flow Chart

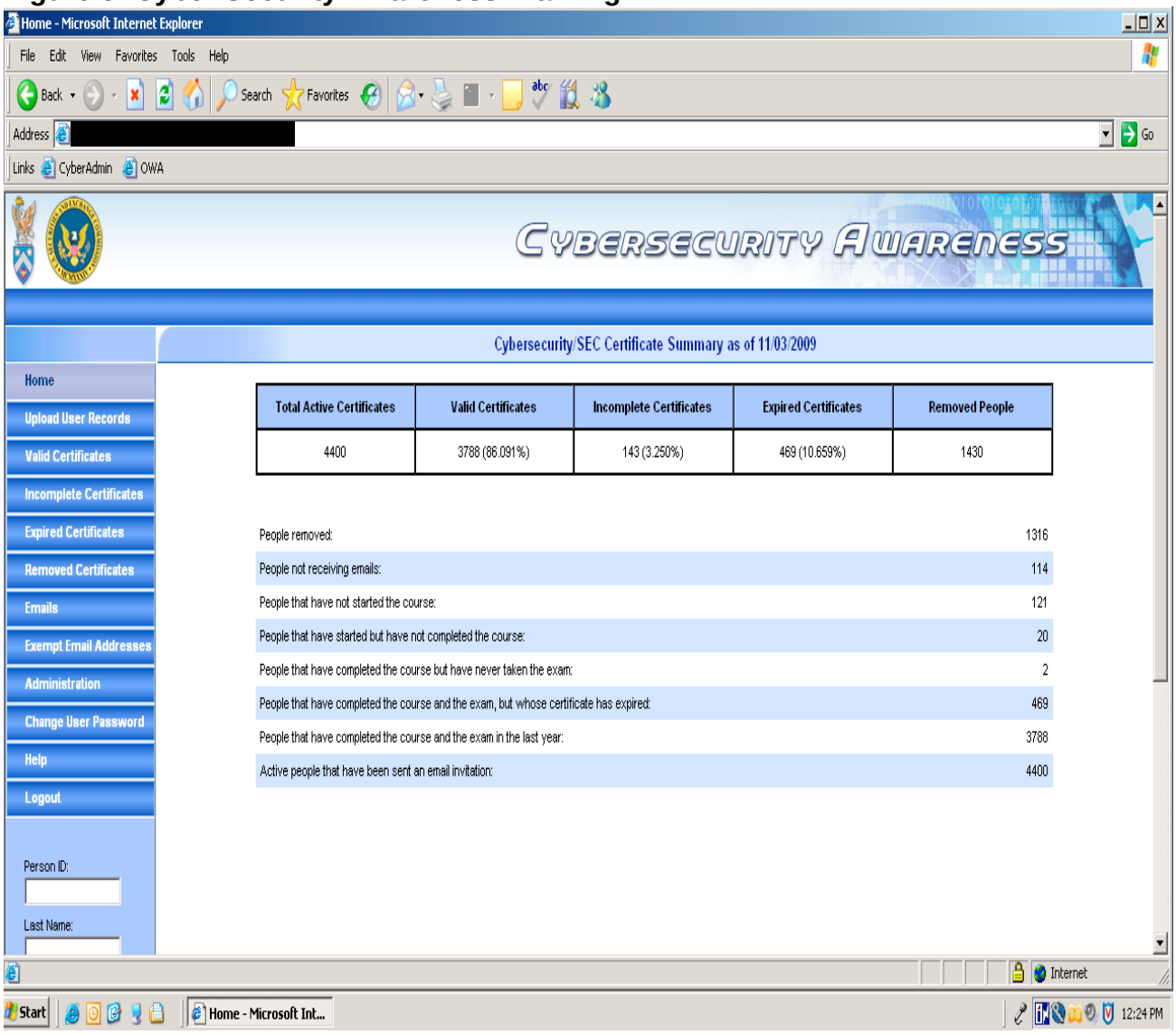
Figure 7: Incident Escalation Flow Chart



Source: OIT Security Group

Cyber Security Awareness Training

Figure 8: Cyber Security Awareness Training



Source: Department of Justice

Management Comments

Memorandum

Date: March 9, 2010

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

From : Charles Boucher, Chief Information Officer, OIT

Subject: Management Response to OIG Report 472, *2009 FISMA Executive Summary Report*

The Office of Information Technology appreciates the opportunity to comment on the subject report. We are pleased that the OIG found no need for recommendations on "how the Commission has implemented its mandated information security requirements."

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 Request/Idea)
100 F Street, N.E.
Washington D.C. 20549-2736

Tel. #: 202-551-6061
Fax #: 202-772-9265
Email: oig@sec.gov

Hotline

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

Phone: 877.442.0854

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