U.S. Securities and Exchange Commission

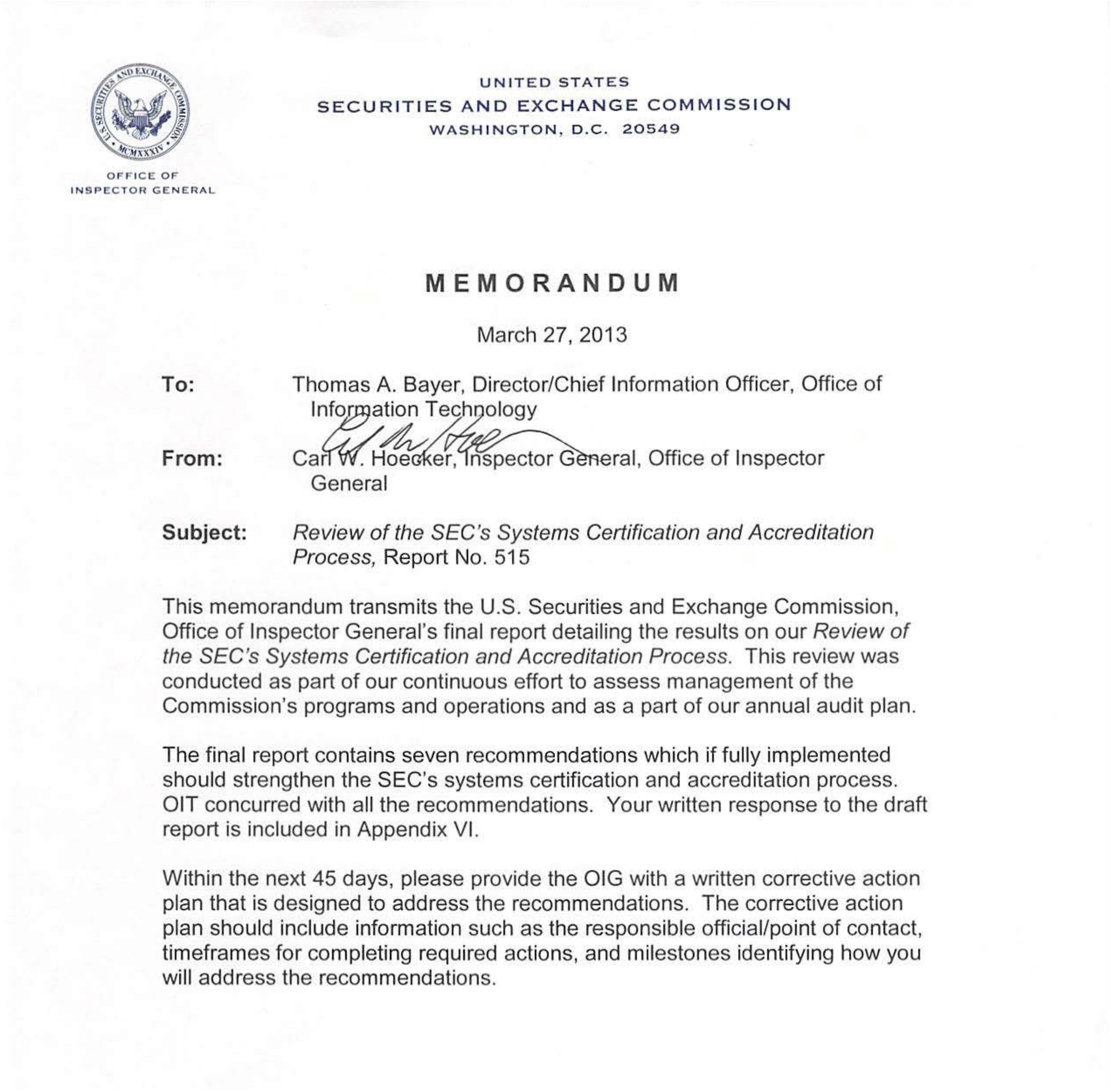
Office of Inspector General

Office of Audits

Review of the SEC's Systems Certification and Accreditation Process

March 27, 2013
Report No. 515

REDACTED PUBLIC VERSION



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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 27, 2013

To: Thomas A. Bayer, Director/Chief Information Officer, Office of Information Technology

From: Carl W. Hoecker, Inspector General, Office of Inspector General

Subject: *Review of the SEC's Systems Certification and Accreditation Process,* Report No. 515

This memorandum transmits the U.S. Securities and Exchange Commission, Office of Inspector General's final report detailing the results on our *Review of the SEC's Systems Certification and Accreditation Process*. This review was conducted as part of our continuous effort to assess management of the Commission's programs and operations and as a part of our annual audit plan.

The final report contains seven recommendations which if fully implemented should strengthen the SEC's systems certification and accreditation process. OIT concurred with all the recommendations. Your written response to the draft report is included in Appendix VI.

Within the next 45 days, please provide the OIG with a written corrective action plan that is designed to address the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframes for completing required actions, and milestones identifying how you will address the recommendations.

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

Attachment

cc: Elisse B. Walter, Chairman
Erica Y. Williams, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Daniel Gallagher, Commissioner
Jeff Heslop, Chief Operating Officer, Office of the Chief Operating Officer
Pamela C. Dyson, Deputy Director/Deputy CIO, Office of Information Technology
Todd K. Scharf, Associate Director, Chief Information Security Officer, Office of Information Technology

Review of the SEC's Systems Certification and Accreditation Process

Executive Summary

The U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted the services of Networking Institute of Technology, Inc. (NIT) to assess the certification and accreditation (C&A) process the Office of Information Technology (OIT) and information system owners use to test their systems and determine compliance with governing SEC policies and procedures, industry best practices, and applicable government laws, directives, regulations, and publications such as the Office of Management and Budget Circular A-130, *Management of Federal Information Resources,* November 28, 2000 (OMB A-130),[1] including Appendix III, *Security of Federal Automated Information Resources*. OMB's circulars provide guidance that can be used to ensure information systems are protected throughout the lifecycle process. The lifecycle process for an information system consists of phases covering planning, analysis, design, implementation, and retirement.

OIT supports the SEC's functions in all aspects of information technology (IT), to include IT security and conducting C&As. The Chief Information Officer (CIO), who is responsible for developing and maintaining an agency-wide information security program, heads OIT. The Chief Information Security Officer (CISO) carries out the CIO's information security responsibilities under federal law. OIT has developed C&A packages for the SEC's information systems that provide relevant information on the security state of systems. OIT conducts system-level risk assessments for the SEC's information systems and plans of action and milestones are developed to mitigate identified risks. In addition, as part of its continuous monitoring process, OIT conducts penetration testing and vulnerability scanning on a regular basis.

The C&A process is required by the Federal Information Security Management Act (FISMA).[2] The traditional C&A approach requires C&A's be performed on all information systems. A C&A stays in force for three years, unless significant changes are made to the system or the operating environment. The C&A process consists of "[a] comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls

[1] OMB Circular No. A-130 Revised, *Management of Federal Information Resources (*November 28, 2000*)*.
[2] Title II, Pub. L, No. 107-347 (December 17, 2002), §3545.

are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system." [3]

A security testing and evaluation (ST&E) is essential to the C&A process. A ST&E is used to determine a system's compliance with defined security requirements where the correctness and effectiveness of the security controls implementing the security requirements are tested. Organizations use the ST&E to document security controls that are effective, ineffective, or have not been fully implemented.

Objectives. NIT's overall objective was to conduct a review of the SEC's systems C&A process and determine if there are areas that need strengthening. Our specific review objectives included:

- Reviewing OIT's C&A process to ensure it is based on the six-step Risk Management Framework criteria identified in National Institute of Standards and Technology (NIST) SP 800-37, Rev. 1.
- Conducting a system assessment and determining if the SEC has appropriately certified and accredited all its systems in accordance with industry best practices and guidelines.
- Determining whether the C&A process for critical applications is effective in identifying and mitigating risks in a timely manner.
- Conducting an assessment to determine the adequacy of OIT's internal controls and compliance with internal information security policies and procedures and industry best practices, standards, and guidelines.

Results. OIT's documentation to support evaluating some systems security controls needs improvement. Specifically, OIT's evaluation of security controls for some SEC information systems needs to be better documented. We determined some elements used to conduct the assessments were not clearly identified. The review found that contractors did not provide enough evidence within the ST&E to demonstrate they had examined documentation, conducted interviews and tested the security controls for the ST&E evaluation. Consequently, it was determined the ST&E needed support to demonstrate the assessor's method for examining, interviewing, and testing security controls. The review further found a ST&E was not done for a contractor system and OIT does not require ST&Es are conducted for contractor systems.

The review also found that OIT's evaluation of some security controls should have been better documented. Specifically, all elements used to conduct the assessments should have been clearly identified. Without having sufficient

[3] NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006), pp. 31-32, Appendix B, Glossary.

documentation in the ST&E, OIT cannot validate that security controls are functioning as intended. We determined OIT should improve how it evaluated the SEC system's security controls.

Further, the review found the designated approving authority (DAA) did not review and verify the terms and conditions set forth in the system authorization on an annual basis, as described in the authorization to operate letter. Also, the DAA reviewed and verified the terms and conditions of the SEC's security controls on a three-year cycle, rather than on a continuous basis. Because security controls are not reviewed and a security status report is not developed at least annually, SEC's systems are operating at an elevated risk of exploitation level to its information systems.

The review of personally identifiable information (PII) is not consistently documented in some C&A packages. Moreover, PII related to some systems was inconsistent with the C&A documentation that was reviewed. As a result, PII is potentially not being properly protected.

Additionally, the SEC's information system owners did not fully understand their roles and responsibilities in the C&A process. As a result, they approved C&A packages without having any technical knowledge. We also found that system owners did not receive any formal role-based IT security training or guidance based on their roles and responsibilities as system owner. As a result, they are approving C&A packages without having technical knowledge. This could potentially result in data not being properly protected.

Finally, the DAA has not taken role-based training and is responsible for providing advice and assistance to senior management regarding SEC's systems; developing, maintaining, and facilitating the implementation of a sound information security program; and promoting the effective and efficient design and operation of all major information resources management processes. Having role-based training would enhance the DAA's understanding of federal IT security standards.

Summary of Recommendations. This report contains seven recommendations that were developed to strengthen the SEC's systems certification and accreditation process. Our most significant recommendations were that OIT implement a centralized repository for managing C&A activities including the security test and evaluation process, determine if the Commission has C&A files stored on its contractor's off-site servers, and require future contractors maintain Commission files only on SEC servers.

We further recommended OIT develop and provide security status reports to the designated approving authority annually as specified in the authorization to operate memorandums, work with system owners and the SEC privacy office to review all Commission's systems and conduct privacy analysis worksheets to determine if they contain PII.

Finally, we recommended OIT develop a formal C&A briefing for information systems and present it to the system owners for review; provide direction to staff properly evaluating security controls; identify the portion of the hybrid controls that are inherited by the general support system and the portion that is covered by system-specific controls; and include a list of common controls that is inherited from the general support system, in accordance with approved system security plan templates.

Management's Response to the Report's Recommendations. OIG provided SEC management with the formal draft report on March 14, 2013. SEC management concurred with all recommendations in this report. OIG considers the report recommendations resolved. However, the recommendations will remain open until documentation is provided to OIG that supports each recommendation has been fully implemented.

SEC management's response to each recommendation and OIG's analysis of their responses are presented after each recommendation in the body of this report.

The full version of this report includes information that the SEC considers to be sensitive or proprietary. To create this public version of the report, OIG redacted (blacked out) potentially sensitive, proprietary information from the report.

TABLE OF CONTENTS

Executive Summary iii

Table of Contents vii

Background and Objectives 1
- Background 1
- Objectives 4

Findings and Recommendations 5
- Finding 1: OIT's Documentation to Support Evaluation Security Controls for SEC's Information Systems Could be Improved 5
  - Recommendation 1 16
  - Recommendation 2 16
- Finding 2: OIT Did Not Develop Security Status Reports for SEC's Systems the DAA Could Review 17
  - Recommendation 3 18
- Finding 3: PII is Inconsistently Documented in Some C&A Packages 19
  - Recommendation 4 22
- Finding 4: SEC Information System Owners Did Not Fully Understand Their Roles and Responsibilities in the C&A Process 23
  - Recommendation 5 25
- Finding 5: DAA Has Not Had Formal Role-Based IT Security Training 25
- Finding 6: OIT Did Not Identify the Portion of Hybrid Controls GSS Inherited and the Portion Covered by System-Specific Controls 27
  - Recommendation 6 33
  - Recommendation 7 33

Appendices
- Appendix I: Abbreviations 34
- Appendix II: Definitions 35
- Appendix III: Scope and Methodology 36
- Appendix IV: Criteria 39
- Appendix V: List of Recommendations 41
- Appendix VI: Management Comments 43

Tables

Table1: Evaluation of AC-2.1 for NIT's Sample System Universe 7
Table 2: CA-2.2. Detail for the Systems NIT Evaluated 10
Table 3: Evidence and Artifacts for CA-7.1 for the Systems NIT Evaluated 13
Table 4: NIT's Privacy Analysis [redacted] 21
Table 5: Identification of Hybrid and System-Specific Controls for CA-7.1 for the Systems Evaluated 30

Figures

Figure 1: Risk Management Framework Process 4

REDACTED PUBLIC VERSION

Background and Objectives

Background

The U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted the services of Networking Institute of Technology, Inc. (NIT) to assess the certification and accreditation (C&A) process the Office of Information Technology (OIT) and information system owners use to test their systems and determine compliance with governing SEC policies and procedures, industry best practices, and applicable government laws, directives, regulations, and publications such as the Office of Management and Budget Circular A-130, *Management of Federal Information Resources,* November 28, 2000 (OMB A-130), including Appendix III, *Security of Federal Automated Information Resources*. [4]

OMB A-130 establishes policy for managing federal information resources and it includes procedural and analytic guidelines for implementing specific aspects of these policies in its appendices. Specifically, Appendix III, establishes a minimum set of controls to be included in federal automated information security programs; assigns federal agency responsibilities for the security of automated information; and links agency's automated information security programs and management control systems in accordance with OMB Circular A-123, *Management's Responsibility for Internal Controls, December 21, 2004*, which further defines management's responsibility for internal control in federal agencies. These circulars also provide guidance that can be used to ensure information systems are protected throughout the lifecycle process. The lifecycle process for an information system consists of phases covering planning, analysis, design, implementation, and retirement.

The Office of Information Technology

OIT supports the SEC's functions in all aspects of information technology (IT), to include IT security and conducting C&As. OIT is comprised of four branches and is led by the Chief Information Officer (CIO), who is responsible for developing and maintaining an agency-wide information security program. The Chief Information Security Officer (CISO) carries out the CIO's information security responsibilities under federal law. One of the CISO's primary duties includes the performance of information security.[5]

[4] OMB Circular No. A-130 Revised, *Management of Federal Information Resources* (November 28, 2000).
[5] OIT Security Policy Framework Handbook, No. CIO-PD-08-06 (August 7, 2012), pp. 7-8, Responsibilities.

OIT has developed C&A packages for the SEC's information systems that provide relevant information on the security state of the systems. Further, OIT conducts Federal Information Processing Standards (FIPS) 199 analysis to determine the categorization of each system and the security control selection is based on the system categorization level. In addition, system security plans (SSP) have been developed for each system and the SSPs are approved by a senior OIT official. Control implementation is documented in the SSP, to include a functional description of the control implementation. A system level risk assessment is conducted for each system and a plan of action and milestones (POA&M) are developed to mitigate the risks. Finally, as part of its continuous monitoring process, OIT conducts penetration testing and vulnerability scanning on a regular basis.

ST&E and Certification and Accreditation

A security testing and evaluation (ST&E) is essential to the C&A process. A ST&E is used to determine a system's compliance with defined security requirements where the correctness and effectiveness of the security controls implementing the security requirements are tested. Organizations use the ST&E to document security controls that are effective, ineffective, or have not been fully implemented. Ineffective security controls and controls that have not been fully implemented are documented in a risk assessment. The risk assessment defines the residual risk[6] for a system prior to mitigation and after appropriate risk mitigation has occurred.

OIT's designated approving authority (DAA) determines the acceptable level of risk based on the SEC's requirements, while using the risk assessment and certification package to issue an authorization to operate, or no accreditation of the system. The DAA is an organizational official who acts on behalf of an authorizing official to carry out and coordinate required activities associated with security authorization.[7] OIT's CIO is the SEC's designated DAA. The DAA's primary responsibilities include reviewing the SEC's security risks and making a final decision whether to authorize operations, delay operation to allow mitigation of risks prior to authorizing, or deny operation based on risk findings of the SEC's information systems.

The C&A process is required by the Federal Information Security Management Act (FISMA).[8] The traditional C&A approach requires that C&As be performed on all information systems. A C&A stays in force for three years, unless significant changes are made to the system or the operating environment. The

[6] The remaining potential risk after all IT security measures are applied.
[7] NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, (February 2010), p. B-2, Glossary.
[8] Title II, Pub. L, No. 107-347 (December 17, 2002), §3545.

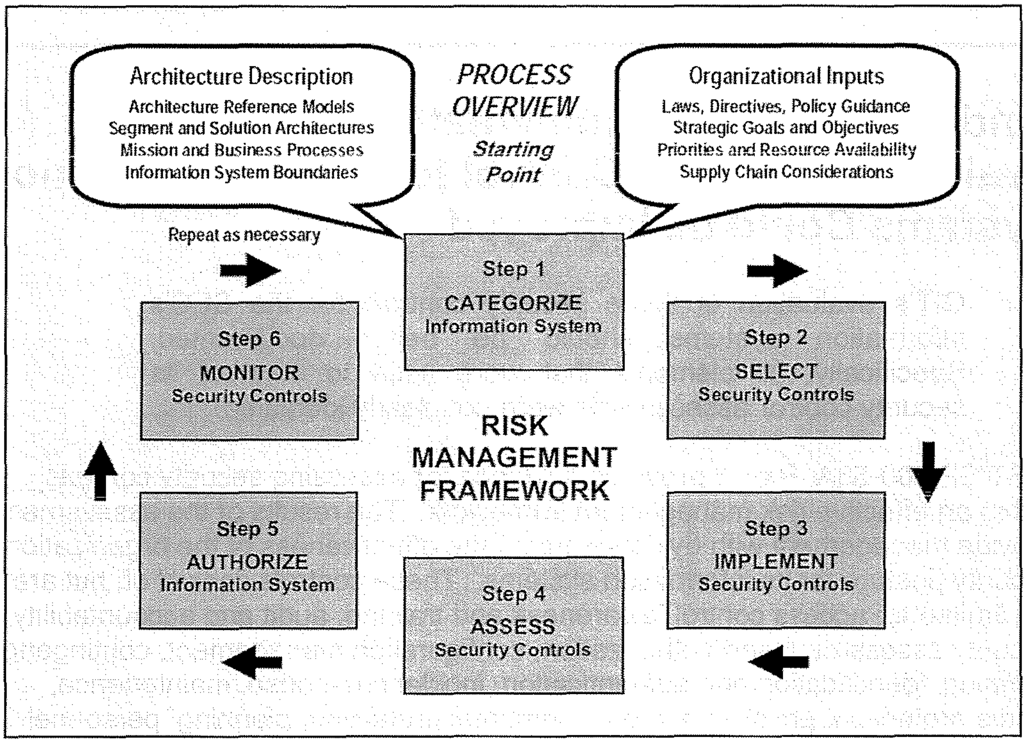
traditional C&A approach has transformed into a more robust approach that is related to managing security-related risks and is based on the six-step risk management framework (RMF) criteria that is identified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST SP 800-37, Rev. 1).[9]

The C&A process consists of "[a] comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system." [10] Based on the results of the assessment, a senior agency official authorizes an information system to operate and explicitly accepts the risk to agency operations. This process emphasizes: "(i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems."[11]

In accordance with SEC policy, OIT is responsible for overseeing the C&A team and ensuring security controls have been properly assessed using the assessment methods and procedures described in NIST publications and in accordance with industry best practices, and to ensure an accreditation package is prepared and maintained for each system.[12] We reviewed OIT's C&A process based on the RMF criteria identified in NIST SP 800-37, Rev. 1. Figure 1 below illustrates the RMF process.[13]

[9] NIST SP 800-37, Rev. 1, p. 1, Section 1.1.
[10] NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006), pp. 31-32, Appendix B, Glossary.
[11] NIST SP 800-37, Rev. 1, pp. 1-2, Section 1.1.
[12] Implementing Instruction, IT Security Certification and Accreditation, Policy No. 24-04-10-01 (June 29, 2005), pp. 6-8, Section 6, Roles and Responsibilities.
[13] NIST SP 800-37, Rev. 1, p. 8, Figure 2-2.

Figure 1: Risk Management Framework Process


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Source: NIST SP 800-37, Rev. 1.

Objectives

Objectives. NIT's overall objective was to conduct a review of the SEC's systems C&A process and determine if there are areas that need strengthening. Our specific review objectives included:

- Reviewing OIT's C&A process to ensure it is based on the six-step RMF criteria identified in NIST SP 800-37, Rev. 1.
- Conducting a system assessment and determining if the SEC has appropriately certified and accredited all its systems in accordance with industry best practices and guidelines.
- Determining whether the C&A process for critical applications is effective in identifying and mitigating risks in a timely manner.
- Conducting an assessment to determine the adequacy of OIT's internal controls and compliance with internal information security policies and procedures and industry best practices, standards, and guidelines.

Findings and Recommendations

Finding 1: OIT's Documentation to Support Evaluation Security Control for SEC's Information Systems Could be Improved

> OIT's evaluation of some security controls for the SEC's information systems should be better documented. Specifically, all elements that were used to conduct its security control assessments were not clearly identified.

NIST SP 800-53A, Rev. 1 provides guidance for assessing security controls within an effective risk management framework. The results of the assessment provide management with evidence about the effectiveness of the organization's security posture for its information systems. These controls consist of, but are not limited to: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.[14]

We used the aforementioned controls to evaluate and assess OIT's security posture by testing a judgmental sample of 15 percent (11 of 59) of the SEC's information systems. Our testing consisted of reviewing the C&A packages for 11 information systems the SEC certified and accredited from January 1, 2010 to March 31, 2012. The systems in our sample universe consisted of the [redacted] We also assessed the systems to determine if they were evaluated in accordance with industry best practices and guidelines. Further, we reviewed the ST&E for each system to determine if OIT examined, interviewed and tested security controls, provided detail for each security control evaluated,

[14] NIST SP 800-53A, Rev. 1, Appendix F.

and obtained evidence and artifacts to evaluate the security controls. The ST&E security document consisted of assessment criteria and assessment results for required security controls for information systems. We further conducted a detailed ST&E review based on a judgmental sampling of 12 percent (24 of 200) security controls from the ST&E documents.

Our review of the SEC's 11 systems found a ST&E was not done for a contractor system. We later learned OIT does not require ST&Es are conducted for contractor systems. OIT examines the ST&Es that are conducted by the contractor. Our review of the 10 remaining systems found that OIT's evaluation of some security controls should have been better documented and all elements used to conduct the assessments should have been clearly identified.

NIST Examine, Interview, and Test Requirements

NIST SP 800-53A, Rev. 1 describes the assessment methods used to conduct a security control evaluation as follows:

> Assessment methods define the nature of the assessor actions and include *examine*, *interview*, and *test*. The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence. The *interview* method is the process of holding discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence. The *test* method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.[15]

OIT's contractor provide the office with C&A support in general support systems (GSS) and reportable systems, in accordance with NIST SP 800-53A, Rev. 1. Our review of ST&E documents for the systems in our sample determined the contractor, in assessing the SEC's security posture, did not fully apply NIST SP 800-53A, Rev. 1. Our review of ST&E documents included reviewing OIT's assessment objectives for 24 security controls and their response to those objectives. We found the contractor did not provide sufficient documentation

[15] Ibid, p. 9, Section 2.4.

within the ST&E to demonstrate they had examined system documentation, conducted interviews and tested the security controls for the ST&E evaluation. We determined the ST&E lacked sufficient details and evidence to demonstrate the assessor's method for examining, interviewing, and testing security controls.

The contractor's evaluation of security controls relied heavily on penetration testing. However, the contractor did not provide support the assessments were conducted in accordance with NIST SP 800-53A, Rev. 1. We determined that although penetration testing is a good mechanism to use, it does not address all the security controls that are identified in NIST SP 800-53A, Rev. 1 that are needed when conducting a security control assessment.[16] Without having sufficient documentation in the ST&E, OIT cannot validate that security controls are functioning as intended. For example, for each security control the assessor determined was satisfied from a prior assessment of the same information system, the assessor can record the results in the control evaluation, which indicates the control is satisfied. However, if the assessor does not independently examine evidence, interview OIT stakeholders, or test the security controls, the assessment of the system's security controls is not thorough.

Table 1 illustrates our comparison between the security control outlined in NIST SP 800-53A, Rev. 1, AC-2.1, Account Management and the 11 systems in our sample universe.[17]

Table 1: Evaluation of AC-2.1 for NIT's Sample System Universe

OIT Modified Assessment Objective for Control AC-2.1	OIT's ST&E Response for Control AC-2.1.	System Evaluated	NIT's Evaluation Result
Does the organization manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts?	SEC policy prohibits use of temporary or guest accounts, and thus these are not used for [name of system].	[redacted]	No evidence of conducting interviews, examining documentation, or testing the security control.

[16] Penetration testing covers risk assessment, system and communications protection, and system and information integrity but does not address access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, system and services acquisition, and program management. Ibid, Appendix F.

[17] Ibid, p. F-5.

[18] We reviewed 6 of the 11 information systems in our sample and found the same response for this control.

OIT Modified Assessment Objective for Control AC-2.1	OIT's ST&E Response for Control AC-2.1.	System Evaluated	NIT's Evaluation Result
Examine organizational records to determine if establishing, activating, modifying, reviewing, disabling, and removing accounts are being performed in accordance with documented account management procedures.	See IA-4.1 and AC-2.1. The need for [redacted] access and for particular system roles are revalidated annually as part of the budget preparation cycle. (Partially covered by common controls provided by the GSS)[19]	[redacted]	No evidence of conducting interviews, examining documentation, or testing the security control.
Does the organization manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts?	SEC policy prohibits use of temporary or guest accounts except for security testing, and thus these are not normally used for [redacted]. Accounts established for test purposes (such as the security testing accompanying this certification) are appropriately authorized.	[redacted]	No evidence of conducting interviews, examining documentation, or testing the security control.
N/A	[redacted] is a contractor system, and ST&Es are not required for contractor systems.	[redacted]	N/A
Does the organization manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts?	[redacted] External is intentionally designed to allow use without login. SEC policy prohibits use of temporary or guest accounts, and thus these will not be used for [redacted] Internal.	[redacted]	No evidence of conducting interviews, examining documentation, or testing the security control.
Does the organization manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts?	SEC policy prohibits use of temporary or guest accounts, except as specified in OIT Security policy during vulnerability scanning or testing of applications.	[redacted]	No evidence of conducting interviews, examining documentation, or testing the security control.

Source: NIT Generated

Our review found no evidence that the assessors examined or tested system accounts even though AC-2.1, Account Management, requires examining and testing according to Appendix F of NIST SP 800-53A, Rev. 1.[20] Overall, while we did not find enough evidence to support the method the assessor used for their

[19] NIST SP 800-53, Rev. 3 states that organizations assign a hybrid status to a security control when one part of the control is common and another part is system-specific. NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations (August 2009)*, p. 11.

[20] NIST SP 800-53A, Rev. 1, p. F-5.

testing, of these occurrences, we found they properly documented their responses in the ST&E documents for the 11 systems in our sample.

ST&E's Security Control Assessments

Although OIT does not prepare security assessment reports, OIT informed us that the results of their security control assessments, which are usually included in a security assessment report, were documented in the ST&Es.
NIST SP 800-37, Rev 1 state:

> The assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings. …Security control assessment results are documented at a level of detail appropriate for the assessment…[21]

OIT's policy, *IT Security Certification and Accreditatio*n defines the sufficient level of detail for the assessment as follows:

> Each SEC major application and general support system shall undergo appropriate technical evaluations to ensure that it meets all Federal and SEC policies, and that all installed security safeguards appear to be adequate and appropriate for the protection requirements of the system. Certification of the system shall be based on the documented results of the formal risk assessment and the Security Test and Evaluation (ST&E), which are based on a specified set of security requirements derived from Federal laws and SEC policies. Certification also may be based on additional forms of evidence, including penetration testing, audit reports, business continuity and disaster recovery plans, monitoring, log reviews, and self-assessments.[22]

While OIT documents the results of security control assessment in their ST&Es, we found the documented results did not provide enough information that could be used to (1) assess the overall effectiveness of the controls for the 11 systems in our sample; and (2) determine if the controls were implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for each information system. We made this determination based on the lack of detail that was provided in the ST&Es. The ST&E results did not have details such as interviews, report references, and policies or procedures that were used to support conclusions. In addition, the

[21] NIST SP 800-37, Rev. 1, p. 32, Section 3.4, Task 4.3.
[22] OIT's Implementing Instruction (II), *IT Security Certification and Accreditation*, Policy No. II 24-04.10.01 (02.0), (June 29, 2005) p. 3.

results did not include the sites that were accessed or assessment date, which is required by NIST SP 800-53A, Rev. 1. NIST SP 800-53A, Rev. 1 requires assessor's document areas such as the assessment date, key elements for assessment reporting, sites assessed, and the assessor's identification.[23]

Table 2 illustrates the comparison between the security control outlined in NIST SP 800-53A, Rev. 1, CA-2.2, Security Assessments and the systems evaluated in our sample.[24]

Table 2: CA-2.2. Detail for the Systems NIT Evaluated

OIT Modified Assessment Objective for Control CA 2.2	OIT's ST&E Response for Control CA-2.2.	System Names	NIT's Evaluation Result
Control was not evaluated and an explanation why it was not evaluated was not provided.	No CA-2.2. Control was not evaluated and an explanation why it was not evaluated was not provided.	[redacted]	Control was not evaluated and an explanation why it was not evaluated was not provided.
Does the organization produce a security assessment report that documents the results of the assessment?	See CA-2.2. This ST&E is being published as part of the first assessment of [redacted] security controls. A Risk Assessment Summary report is being delivered concurrently with this ST&E Results Report and an updated POA&M.	[redacted] [redacted] [redacted]	Does not provide sufficient level of detail or identify the date of assessment
Does the organization produce a security assessment report that documents the results of the assessment?	See CA-2.2. This ST&E is being published as part of the third assessment of [redacted] security controls. A Revised Risk Assessment Summary report is being delivered concurrently with this ST&E Results Report and an updated POA&M.	[redacted]	Does not provide sufficient level of detail or identify the date of assessment
Does the organization produce a security assessment report that documents the results of the assessment?	See CA-2.2. This ST&E is being published as part of the second assessment of [redacted] security controls. A Revised Risk Assessment Summary report and an updated POA&M are being delivered concurrently with this ST&E Results Report.	[redacted] [redacted] [redacted] [redacted]	Does not provide sufficient level of detail or identify the date of assessment
N/A	[redacted] is a contractor system, and ST&Es are not required for contractor systems.	[redacted]	N/A

[23] NIST SP 800-53A, Rev. 1, p. G-1, Appendix G.
[24] NIST SP 800-53A, Rev. 1, p. F-81.
[25] We reviewed 3 of the 11 information systems in our sample and found the same response for this control.
[26] We reviewed 4 of the 11 information systems in our sample and found the same response for this control.

OIT Modified Assessment Objective for Control CA 2.2	OIT's ST&E Response for Control CA-2.2.	System Names	NIT's Evaluation Result
Does the organization produce a security assessment report that documents the results of the assessment?	See CA-2.2. This ST&E is being published as part of the first assessment of [redacted] security controls. A Risk Assessment Summary report is being delivered concurrently with this ST&E Results Report and an initial POA&M.		Does not provide sufficient level of detail or identify the date of assessment
Does the organization produce a security assessment report that documents the results of the assessment?	See CA-2.2. This ST&E is being published as part of the reassessment of [redacted] security controls. A Revised Risk Assessment Summary report and updated POA&M are being delivered concurrently with this ST&E Results Report.	[redacted]	Does not provide sufficient level of detail or identify the date of assessment

Source: NIT Generated

The 11 systems in our sample had no evidence the assessor provided a sufficient level of detail for the assessment. Accordingly, the ST&Es for the systems did not list the date the security control was evaluated.

The security control assessor is "[t]he individual, group, or organization responsible for conducting a security control assessment."[27] We were told OIT does not require the security control assessor to identify the evaluation date. OIT uses a manual process to conduct these assessments. However, automated C&A tools are available that could simplify this process by automatically recording the assessor's name, date of the assessment for each control, and require assessors to provide detail. OIT's manual ST&E process requires the assessor to type-in its results in evaluating security controls and managing the C&A process. OIT informed us they will implement an automated solution, which will become effective by 2014.

Evidence and Artifacts

NIST SP 800-53A, Rev. 1 states that the assessors obtain evidence and artifacts for the security control assessment:

> Assessors obtain the required evidence during the assessment process to allow the appropriate organizational officials to make objective determinations about the effectiveness of the security controls and the overall security state of the information system.
>
> Security control assessors/assessment teams begin preparing for the assessment by… [o[btaining artifacts needed for the security

[27] NIST SP 800-37, Rev. 1, p. B-9, Appendix B.

> control assessment (e.g., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, previous assessment results)… [28]

Our ST&E review found the evidence and artifacts the assessors provided to support their ST&Es results did not have enough evidence that could be used to make an objective determination regarding the effectiveness of the security controls and the overall security state of the system. In addition, the evidence and artifacts collected and used to support the security assessment results were not mapped to a specific security control. For example, the documentation for the [redacted] systems (2 of the 11 systems in our sample universe) were labeled by the assessor as evidence to support the ST&Es included the SSP and system categorization, which were insufficient evidence or artifacts. We also found the documentation did not map to specific security controls or allow appropriate organization officials to make objective determinations about the effectiveness of the security controls and the overall security state of the information system. An SSP is a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Table 3 shown below consists of a comparison between the security control outlined in NIST SP 800-53A, Rev 1, CA-7.1, Continuous Monitoring and the ST&Es. The responses found in the ST&Es do not reference any evidence or artifacts.[29]

[28] NIST SP 800-53A, Rev. 1, p. 8, section 2.3; p. 14, Section 3.1.

[29] Ibid, p. F-87. Continuous monitoring is the process of tracking the security state of an information system on an ongoing basis and maintaining the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and mission and business processes. Network vulnerability assessments, ongoing security control assessments, and C&A are all components of continuous monitoring programs.

Table 3: Evidence and Artifacts for CA-7.1 for the Systems NIT Evaluated

OIT Modified Assessment Objective for Control CA 7.1	OIT's ST&E Response for Control CA-7.1	System Names	NIT's Evaluation Result
Does the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components?	The SEC has mature continuous monitoring and configuration management programs. SEC systems are reaccredited when security-relevant changes are made. System changes are approved through a documented process that includes security review. Continuous monitoring is performed on [name of system] components residing on GSS devices. [name of system] has also been stable after being limited to a read-only archive in November 2009. (Partially covered by GSS common controls)[30]	[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]	No evidence or artifacts provided

[30] NIST SP 800-53, Rev. 3 states organizations assign a hybrid status to a security control when one part of the control is common and another part is system-specific. NIST SP 800-53, Rev. 3, p. 11.

[31] We reviewed 8 of the 11 information systems in our sample and found the same response for this control.

OIT Modified Assessment Objective for Control CA 7.1	OIT's ST&E Response for Control CA-7.1	System Names	NIT's Evaluation Result
Does the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components?	• The SEC has mature continuous monitoring and configuration management programs. SEC systems are reaccredited when security-relevant changes are made. System changes are approved through a documented process that includes security review. Continuous monitoring is performed on [redacted] components residing on GSS devices. No significant changes have been made to the [redacted] application code since it became operational, but minor changes have been tracked in the [redacted] Configuration Management tool. Following this initial C&A, [redacted] will receive additional continuous monitoring attention (e.g., annual review of user accounts, the SSP, and the DRP, and quarterly review of open POA&M findings). • (Partially covered by GSS common controls)[32]	[redacted]	No evidence or artifacts provided
N/A	[redacted] is a contractor system, and ST&Es are not required for contractor systems.	[redacted]	N/A

[32] Ibid.

OIT Modified Assessment Objective for Control CA 7.1	OIT’s ST&E Response for Control CA-7.1	System Names	NIT’s Evaluation Result
Does the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components?	• The SEC has mature continuous monitoring and configuration management programs. SEC systems are reaccredited when security-relevant changes are made. System changes are approved through a documented process that includes security review. Continuous monitoring is performed on [redacted] components residing on GSS devices. No significant changes have been made to the [redacted] application code since it became operational, but minor changes have been tracked in the [redacted] Configuration Management tool. [redacted] reviewed the [redacted] SCRs in [redacted] to verify CM was being used appropriately. Other forms of monitoring have also been conducted (e.g., annual review of user accounts, the SSP, and the DRP, and quarterly review of open POA&M findings). (Partially covered by GSS common controls)[33]	[redacted]	No evidence or artifacts provided

Source: NIT Generated

OIT informed us the information the assessor used to conduct and prepare the ST&Es is generated and supplied by OIT. However, OIT’s staff did not have direct access or control of the ST&E documentation the contractor collected. Also, we were informed this documentation is stored on the contractor’s off-site

[33] Ibid.

server that is owned by the assessor, and OIT approved the assessor storing the data at the off-site location.

Conclusion

We determined OIT needs to improve its evaluation of the SEC's security controls for its systems. Specifically, we determined OIT is not ensuring they examine, interview and test security controls; provide a sufficient level of detail for each security control evaluated; and obtain evidence and artifacts to ensure the information systems meet federal guidance and SEC policy. Further, we found that the ST&E responses in our sample universe did not reference any evidence or artifacts. Therefore, we concluded if evidence and artifacts was collected, stored on SEC servers, and referenced to the ST&E, the SEC would then be able to ensure NIST SP 800-53A, Rev. 1 requirements were achieved and the security controls were properly reviewed.

Finally, we determined to properly meet NIST's requirements, assessors should collect and document enough evidence within the ST&E, map the evidence to the specific security controls, and keep the information in a centralized repository for future reference only on an SEC server.

Recommendation 1:

The Office of Information Technology should implement a centralized repository for managing certification and accreditation activities including the security test and evaluation process (i.e., evidence, artifacts, assessor date, and sites assessed).

Management Comments. OIT concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Recommendation 2:

The Office of Information Technology should determine if the Commission has certification and accreditation files that are stored on its contractor's off-site servers and, in the future, require contractor to maintain all Commission files on servers the Commission owns and manages.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 2: OIT Did Not Develop Security Status Reports for SEC's Systems the DAA Could Review

> OIT did not develop security status reports for the information systems in our sample. As a result, we determined the SEC's systems are operating at an elevated risk level for information system exploitation.

NIST SP 800-37, Rev. 1, requires the DAA to verify the terms and conditions of the authorization on an ongoing basis, specifically, that "[t]he authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the information system owner or common control provider."[34]

An authorization to operate (ATO) letter is the official management decision to authorize the operation of an information system and to accept the risk to the organizational operations including mission, functions, or reputation.[35] The DAA issues an ATO after reviewing the results of the C&A package to determine risk to the SEC. An ATO is required for each SEC information system. Consistent with the NIST SP 800-37 requirements, the SEC's ATOs for the 11 systems in our sample state, specifically, that "[t]he security accreditation of the information system will remain in effect as long as (i) the required security status report for the system are submitted to this office every year…."[36]

Security status reports describe or summarize key changes to security plans, security assessment reports, and plans of action and milestones.[37] These documents identify information security vulnerabilities and the plans to address them.

[34] NIST SP 800-37, Rev. 1, p. 36, Chapter 3.
[35] Ibid, p. B-1, Glossary.
[36] This is the Office of the Chief Information Officer.
[37] NIST SP 800-37, Rev. 1, p. G-2, Appendix G, Footnote No. 86.

OIT did not develop security status reports for the systems in our judgmental sample and, therefore, did not comply with its ATO letter requirements. OIT's contractor evaluated its controls on a three-year cycle, rather than using a continuous monitoring approach and assessing a subset of controls on an annual basis, in accordance with NIST SP 800-37, Rev. 1. Continuous monitoring is the process of tracking the security state of an information system on an ongoing basis and maintaining the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and mission and business processes. Network vulnerability assessments, ongoing security control assessments, and C&As are all components of continuous monitoring programs. As a result, if security controls are not assessed annually, OIT is unable to fully generate an updated annual security status report that identifies vulnerabilities to the SEC's systems.

OIT did not provide evidence that status reports are developed annually in the past. Though we requested system security status reports and documentation from OIT, we only received C&A documentation for the three-year certification cycle.

Conclusion

We determined the DAA is not reviewing and verifying the terms and conditions set forth in the system authorization on an annual basis as described in the ATO. Consequently, all 11 systems in our sample are operating without the proper authority. Our review found that the DAA is reviewing and verifying the terms and conditions of the SEC's security controls on a three-year cycle and not on a continuous basis. We determined that because security controls were not reviewed and a security status report is not developed at least annually, SEC's systems are operating at an elevated risk of exploitation level to its information systems.

Recommendation 3:

The Office of Information Technology should develop and provide security status reports to the designated approving authority as specified in their authorization to operate memorandums.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 3: PII is Inconsistently Documented in Some C&A Packages

> Personally Identifiable Information (PII) for 3 of the 11 systems we reviewed was inconsistent with other C&A documentation obtained during our assessment. As a result, PII is potentially not being properly protected.

PII is information in an IT system or online collection system that directly identifies an individual by name, address, social security number or other identifying number or code, telephone number, email address, etc. In addition, PII may be comprised of information an agency intends to identify specific individuals in conjunction with other data elements such as indirect identification. These data elements may also include identifying factors such as gender, race, birth date, geographic indicator and other descriptors.[38]
NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories* (NIST SP 800-60, Rev. 1)*,* addresses the FISMA direction to develop guidelines recommending that agencies conduct privacy impact assessments to determine if their information systems contain PII. The guidance further states:

> Agencies are required to conduct Privacy Impact Assessments (PIA) before developing IT systems that contain personally identifiable information or before collecting personally identifiable information electronically….Categorizations should be reviewed to ensure that the adverse effects of a loss of PII confidentiality have been adequately factored into impact determinations. The confidentiality impact level should generally fall into the moderate range.[39]

The E-Government Act of 2002 establishes the requirement for agencies to conduct PIA for information systems and states the following:

> …This law mandates that each agency shall: —conduct a privacy impact assessment; ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and if practicable, after completion of the review under clause (ii), make the privacy impact

[38] U.S. Securities and Exchange Commission, Office of Information Technology, Privacy Impact Assessment Guide (Revised January 2007).

[39] NIST SP 800-60, Volume I, Rev. 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008), p. 30, Section 4.4.2.

> assessment publicly available through the website of the agency, publication in the Federal Register, or other means.[40]

To address PII requirements SEC's C&A packages include privacy analysis worksheets (PAW) and/or PIA. The PAW is completed to determine whether a full PIA is required. A PIA is an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy. It is used to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."[41]

We reviewed copies of the PAWs and PIAs that the SEC's Privacy Office used for the systems in our sample universe and found the PAWs/PIAs representations regarding PII for the [redacted] systems were inconsistent with other C&A documentation. Specifically, the system categorization documentation received during the assessment was inconsistent with the C&A documentation. "The [system categorization] process is carried out by the information system owner and information owner/steward in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business function and/or risk management responsibilities). The security categorization process is conducted as an organization-wide activity taking into consideration the enterprise architecture and the information security architecture….The results of the security categorization process influence the selection of appropriate security controls for the information system and also, where applicable, the minimum assurance requirements for that system."[43]

[redacted] The [redacted] system did not have a PAW disposition. Therefore, the system may contain PII. Based on our review of the EMTS system's C&A documentation, we were unable to determine if the system contained PII. The system owner informed us it did not contain PII. At the time of our review this system was in use.

[redacted] Based on our review of the PAW for the [redacted] system, we determined the system did not contain PII. However, the system categorization within the risk assessment and SSP identified the system as having PII. The system owner informed us that the system did not contain PII, which is consistent with its PAW disposition. At the time of our review this system was in use.

[40] Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, (September 2003), Attachment b, Section 208B.
[41] NIST SP 800-53, Rev. 3, p.B-9, Glossary.
[42] Represents 3 of the 11 systems in our sample.
[43] NIST SP 800-37, Rev. 1, p. 21, Section 3.1, Task 1-1.

[redacted] Our review of the [redacted] system included a PIA that identified the system as containing PII. However, the system categorization, risk assessment, and SSP did not identify the system as having PII. The system owner also informed us the system contained PII, which is consistent with the PIA's disposition. At the time of our review this system was in use.

NIT requested documentation on January 9, 2013 confirming if the [redacted] systems contained PII. However, we were not provided any evidence. SEC's Privacy Office and OIT were working to provide us with documentation to resolve this matter. Table 4, shown below, outlines the discrepancies between the PAW disposition/PIA disposition and the security categorization for the [redacted] systems.

Table 4: NIT's Privacy Analysis of [redacted]

System Name	PAW Disposition	PIA Disposition	Privacy Office's Notes	Project# 515 Analysis	Privacy Office / OIT's Responses
[redacted]	Pending	Pending	No determination from the privacy office	No determination from the privacy office. The system is in production without a disposition of the PAW. This system may possibly contain PII.	The Privacy Office previously worked with the DIO for the system to obtain a completed PAW and PIA. Our team will contact the system owner to complete the pending PAW and PIA for the system by February 15, 2013.
[redacted]	Completed, PIA Not Required	Not Completed	Approved 11/21/07 (PIA n/a)	The PAW states there is no PII. The system categorization in the 2011 risk assessment and 2011 SSP (dated June 27, 2007) states the existence of PII in the system, but there is no PIA.	The Privacy Office will work with the system owner to complete an updated PAW and PIA to reflect the current status of the system by February 15, 2013.
[redacted]	Not Completed	Completed	Approved 6/10/08	The PIA identifies PII. However, the system categorization in the 2011 risk assessment and 2011 SSP (dated November 30, 2007) does not identify the system as having PII.	(This response is not from the Privacy Office, but from OIT): The documents have been updated and we're awaiting signatures from all concerned.

Source: NIT Generated

Table Response Options

- Completed, PIA Required – The PAW was completed and a PIA is required.
- Completed, PIA Not Required – The PAW was completed and a PIA is not required.
- Not Completed – The documentation was not completed.
- Pending – There is no determination from the Privacy Office.

Table 4 further shows the missing documents, which we attributed to the lack of system owner involvement during the categorization process to provide direction on identifying PII within systems. Additionally, based on our review of the PAWs and PIAs for [redacted], we determined OIT did not effectively document the PII classification in the C&A documentation. As a result, there is a potential that PII is not being properly protected, which could result in improper release of PII to unauthorized individuals.

Conclusion

Overall, we found the PAWs/PIAs representations regarding the inclusion of PII for [redacted] was inconsistent with the C&A documentation that was provided for the assessments, in particular, the system categorization. Our interviews with system owners found many were able to identify whether PII was in their respective systems. Therefore, involving system owners in the categorization process would provide OIT with better direction to identify PII within the system and correctly document PII within C&A documents.

Recommendation 4:

The Office of Information Technology (OIT) should review the security documentation in the certification and accreditation packages, including system categorization documents, risk assessment documents, and system security plans to ensure that references to personally identifiable information, privacy impact assessments, and privacy analysis worksheets, are consistently providing the same disposition regarding Personally Identifiable Information.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 4: SEC Information System Owners Did Not Fully Understand Their Roles and Responsibilities in the C&A Process

> SEC information system owners did not fully understand their roles and responsibilities in the C&A process. As a result, they approved C&A packages without having any technical knowledge.

System Owner Roles and Responsibilities

NIST SP 800-37, Rev. 1, defines the information system owner as a person "responsible for addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements."[44] Further, NIST SP 800-37, Rev. 1 explains the RMF responsibilities/tasks of the system owner.

> The Risk Management Framework and associated RMF tasks apply to both *information system owners* and *common control providers*. In addition to supporting the authorization of information systems, the RMF tasks support the selection, development, implementation, assessment, authorization, and ongoing monitoring of common controls inherited by organizational information systems.[45]

Information system owners are also responsible for input into the certification and accreditation process for a system, including providing input into the supporting documentation package. A comprehensive C&A documentation package consists of the following documents.[46]

- FIPS 199 analysis
- Security assessment plan (include a tailored control list)
- ST&E report
- Risk assessment
- SSP
- POA&M report
- Security assessment report
- ATO

[44] NIST 800-37, Rev. 1, page D-5, Appendix D, Section D.9.
[45] Ibid, p. 20.
[46] Title II, Pub. L, No. 107-347 (December 17, 2002).

Information system owners are required to categorize information systems and document the results,[47] help select the security controls,[48] and assist with preparing POA&Ms and assembling the C&A package.[49] Our interviews with information system owners found they do not fully understand their roles and responsibilities in the C&A process, but sign-off on systems documentation that is presented to them for C&A packages.

We interviewed nine system owners and they informed us that they understood their roles as a system owner.[50] However, one system owner told us she was given a C&A package, but did not understand what the documents represented and signed the ATO as a formality. Overall, our evaluation found that 5 of 9 system owners are not familiar with system categorization; 6 of 9 system owners did not know the number of POA&Ms for their system; 3 of 9 system owners indicated they signed the ATO memo without fully understanding its significance; and 4 of 9 system owners did not attend any formal briefing.

Training

NIST SP 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model* (NIST SP 800-16), states that "prior to be granted access to IT applications and systems, all individuals must receive specialized training focusing on their IT security responsibilities and established system rules.[51]

We determined the system owners did not receive formal role-based IT security training or guidance based on their roles and responsibilities . As a result, the system owners are approving C&A packages without having technical knowledge. This results in data potentially not being properly protected.

Conclusion

We determined that system owners do not have an adequate understanding of their roles and responsibilities and have not been provided specialized training focusing on their IT security responsibilities.

[47] NIST 800-37, Rev. 1, p. 21, Section 3.1, Task 1.1.

[48] Ibid, p. 25, Section 3.2, Task 2.2.

[49] Ibid, p. 34, Section 3.5, Tasks 5.1 and 5.2.

[50] We were unable to obtain interviews with the [redacted] system owners. We interviewed both the former and current [redacted] system owners.

[51] NIST SP 800-16. *Information Technology Security Training Requirements: A Role and Performance Based Model* (April 1998), Chapter 1, p. 3. *See also* OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources.*

Recommendation 5:

The Office of Information Technology should provide a documented brief that management officials (system owners) can use as a resource reference.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 5: DAA Has Not Had Formal Role-Based IT Security Training

> The DAA has not had formal role-based IT security-related training. Having role-based training would enhance the DAA's understanding of federal IT security standards.

OIT's CIO is designated as the DAA. The DAA's primary responsibilities include reviewing the SEC's security risks and making a final decision whether to authorize operations, delay operation to allow mitigation of risks prior to authorizing, or deny operation based on findings of risk for the information systems. The DAA has an integral role and responsibility for authorizing systems, potentially including vulnerabilities, to operate in a production environment.

NIST 800-50, *Building an Information Technology and Security Awareness Training Program*, states that CIOs "are tasked by the FISMA to administer training and oversee personnel with significant responsibilities for information security."[52]

NIST SP 800-53, Rev. 3 requires "role-based security-related training based on assigned roles and responsibilities in which "the organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access."[53]

[52] NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003), p. 3, Section 1.5.2.

[53] NIST SP 800-53, Rev. 3, p. F-22.

Consistent with the NIST requirements, the SEC Implementing Instruction 24-04-03-01, IT Security Awareness Training states, "[R…[role-based] training is required of employees holding certain IT positions, specifically those that have access to or knowledge of SEC sensitive data or materials."[54]

According to the SEC's OIT Security Policy Framework Handbook, the roles and responsibilities of the DAA for the Commission include:

- Providing advice and assistance to senior management to ensure IT is acquired and information resources are managed in a manner consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency.
- Developing, maintaining, and facilitating the implementation of a sound information security program.
- Promoting the effective and efficient design and operation of all major information resources management processes.[55]

The DAA, who has worked at the SEC since October 2010, informed us that although he has knowledge of the SEC's sensitive data, he has not attended any formal, role-based IT security-related training. The DAA was unaware that such training was a NIST requirement or OIT policy. The DAA relies on OIT security staff to provide IT security and FISMA related expertise and guidance, including when the DAA should authorize a system to operate.

The DAA authorized the operations of 10 of the 11 information systems in our sample universe.[56] Thus, the DAA explicitly accepted the risk to the SEC's operations and organizational assets based on an agreed-upon set of security controls. Having formal training in NIST and FISMA's requirements, would enhance the DAA's understanding of risks to the SEC's operations in areas such as mission, functions, image, reputation, or assets.

Conclusion

The DAA has not taken role-based training and is responsible for providing advice and assistance to senior management regarding SEC's systems; developing, maintaining, and facilitating the implementation of a sound information security program; and promoting the effective and efficient design and operation of all major information resources management processes.

[54] Implementing Instruction, IT Security Awareness Training, Policy No. 24-04-03-01 (Dec. 29, 2005), p. 4, Section 5b(1).

[55] OIT Security Policy Framework Handbook, CIO-PD-08-06 (August 2012), p. 7.

[56] The DAA authorized the operation of [redacted] systems.

The DAA should consider attending role-based information technology security training to further enhance his understanding of the National Institute of Standards and Technology and Federal Information Security Management Act requirements.

Finding 6: OIT Did Not Identify the Portion of Hybrid Controls GSS Inherited and the Portion Covered by System-Specific Controls

> The ST&Es for the application specific SEC systems did not identify the portion of hybrid controls that were inherited by GSS, or the portion that is covered by the system-specific controls.[57] This could result in a portion of security controls not being properly evaluated and security vulnerabilities not being detected.

OIT did not identify the portion of the hybrid controls that were inherited by the GSS and the portion covered by the system-specific controls in accordance with NIST SP 800-37, Rev. 1,[58] which state there are "…three types of security controls for information systems that can be employed by an organization: (i) *system-specific controls* (i.e., controls that provide a security capability for a particular information system only); (ii) *common controls* (i.e., controls that provide a security capability for multiple information systems); or (iii) *hybrid controls* (i.e., controls that have both system-specific and common characteristics).[59] Further, the security controls are subsequently allocated to the information systems as system-specific, hybrid, or common controls.[60]

OIT documented security controls that were partially covered by GSS common controls in the ST&Es in our sample information system universe, but did not specify which portion of the hybrid controls is inherited by the GSS, or the portion that is covered by the system-specific controls.

Hybrid Controls

Hybrid controls are controls having both system-specific and common characteristics.[61] For example, contingency planning policy and procedures

[57] The GSS is "[a]n interconnected set of information resources under the same management control that shares common functionality." NIST SP 800-18, Rev. 1, p. 33, Glossary.
[58] Ibid.
[59] NIST SP 800-37, Rev. 1, p. 16, Section 2.4.
[60] Ibid, p. 7, Section 2.1.
[61] Ibid, p. 16, Section 2.4.

control may be implemented as a hybrid control.[62] The policy portion of the control may be common (shared). However, the procedures may differ for each system. Since the policy is common, but the procedures are specific to each system, this control is considered hybrid.

System-Specific Controls

Unlike common controls which are evaluated once and the evaluation results can be inherited by many systems, system-specific controls apply to each individual system and must be individually evaluated for each system. A system-specific control is "[a] security control for an information system that has not been designated as a common security control."[63] For example, the privacy impact assessment control may require testing on a limited number of information systems containing PII.[64] Since the application of this control does not apply to all systems within the GSS it cannot be inherited and is considered a system-specific control. Controls which are neither common nor hybrid are system-specific and pertain to a specific system.

Common Controls

"Common controls are security controls inherited by one or more organizational information systems."[65] They typically originate from the GSS and are accepted for use by major or minor applications. For example, the physical and environmental protection (PE) control family is typically evaluated for the GSS.[66] Major and minor applications associated with the GSS will not reevaluate the PE controls. Since the major or minor applications are hosted in the same computing environment as the GSS, the major and minor applications can inherit the PE security controls from the GSS. This reduces the need for repeat use of identical controls and reduces the resources required for implementing and evaluating security controls.

Identification of Hybrid and System-Specific Controls

NIST SP 800-53, Rev. 3 states that organizations assign a hybrid status to a security control when one part of the control is common and another part is system-specific. The guidance further states:

> Security controls not designated as common controls are considered *system-specific controls* or *hybrid controls*. System-

[62] NIST SP 800-53, Rev. 3, p. F-47.
[63] NIST SP 800-18, Rev. 1, p. 39, Glossary.
[64] NIST SP 800-53, Rev. 3, p. F-87.
[65] NIST SP 800-37, Rev. 1, p. 24, Section 3.2, Task 2.1.
[66] NIST SP 800-53, Rev. 3, pp. D-4-D-5.

> specific controls are the primary responsibility of information system owners and their respective authorizing officials. Organizations assign a *hybrid* status to a security control when one part of the control is deemed to be common and another part of the control is deemed to be system-specific.[67]

We reviewed the ST&Es for each information system in our sample universe to determine if OIT identifies the portion of the hybrid controls that are inherited by the GSS and the portion that is covered by system-specific controls. Our detailed ST&E review was based on a judgmental sample of approximately 12 percent (24 of 200) security controls from OIT's ST&E documents. Overall, our review found that application specific systems did not identify the hybrid controls portion that were inherited by the GSS, or the portion that was covered by the system-specific controls.

OIT's ST&E documented response to "Does the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components?" The ST&E stated, "Partially covered by common controls provided by the GSS." The response did not include the assessor's rationale for the hybrid controls. Further, we found OIT did not evaluate security controls based on the full evaluation criteria identified in NIST SP 800-53A, Rev 1.

We determined OIT's security staff has a general understanding of basic NIST concepts such as the identification of common and hybrid controls, but lacks the understanding needed to identify the portion of the hybrid controls that are inherited by the GSS, or the portion that is covered by system-specific controls. This occurred because OIT has not fully applied NIST guidance to identify the portion of the hybrid controls inherited by the GSS and the portion covered by the system-specific controls. We also found that OIT did not evaluate security controls based on the full evaluation criteria that is identified in NIST SP 800-53A, Rev 1.

Table 5 below, demonstrates the comparison between the security control outlined in NIST SP 800-53A, Rev 1, CA-7.1, Continuous Monitoring and the ST&Es in our sample universe.[68]

[67] Ibid, p. 11.
[68] NIST SP 800-53A, Rev. 1, p. F-87.

Table 5: Identification of Hybrid and System-Specific Controls for CA-7.1 for the Systems Evaluated

OIT Modified Assessment Objective for Control CA 7.1	OIT's ST&E Response for Control CA-7.1	System Names	NIT's Evaluation Result
Does the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components?	The SEC has mature continuous monitoring and configuration management programs. SEC systems are reaccredited when security-relevant changes are made. System changes are approved through a documented process that includes security review. Continuous monitoring is performed on [name of system] components residing on GSS devices.[name of system] has also been stable after being limited to a read-only archive in November 2009 **(Partially covered by GSS common controls)**[69]	[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]0	Does not identify the portion of the hybrid controls inherited by the GSS and the portion covered by the system-specific controls

[69] NIST SP 800-53, Rev. 3 states organizations assign a hybrid status to a security control when one part of the control is common and another part is system-specific. NIST SP 800-53, Rev. 3, p. 11.

[70] Our review of 8 of the 11 systems in our sample found the same response for this control.

			t
Does the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components?	The SEC has mature continuous monitoring and configuration management programs. SEC systems are reaccredited when security-relevant changes are made. System changes are approved through a documented process that includes security review. Continuous monitoring is performed on [redacted] components residing on GSS devices. No significant changes have been made to the [redacted] application code since it became operational, but minor changes have been tracked in the [redacted] Configuration Management tool. Following this initial C&A, [redacted] will receive additional continuous monitoring attention (e.g., annual review of user accounts, the SSP, and the DRP, and quarterly review of open POA&M findings). **(Partially covered by GSS common controls)**[71]	[redacted]	Does not identify the portion of the hybrid controls inherited by the GSS and the portion covered by the system-specific controls
N/A	[redacted] is a contractor system, and ST&Es are not required for contractor systems.	[redacted]	N/A

[71] NIST SP 800-53, Rev. 3 states organizations assign a hybrid status to a security control when one part of the control is common and another part is system-specific. NIST SP 800-53, Rev. 3, p. 11.

OIT Modified Assessment Objective for Control CA 7.1	OIT's ST&E Response for Control CA-7.1	System Names	NIT's Evaluation Result
Does the organization establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components?	The SEC has mature continuous monitoring and configuration management programs. SEC systems are reaccredited when security-relevant changes are made. System changes are approved through a documented process that includes security review. Continuous monitoring is performed on [redacted] components residing on GSS devices. No significant changes have been made to the [redacted] application code since it became operational, but minor changes have been tracked in the [redacted] Configuration Management tool. [redacted] reviewed the [redacted] SCRs in [redacted] to verify CM was being used appropriately. Other forms of monitoring have also been conducted (e.g., annual review of user accounts, the SSP, and the DRP, and quarterly review of open POA&M findings). (**Partially covered by GSS common controls**)[72]	[redacted]	Does not identify the portion of the hybrid controls inherited by the GSS and the portion covered by the system-specific controls

Source: NIT Generated

As demonstrated in Table 5, the responses found in the ST&E for the sample universe do not specifically identify the portion of the hybrid controls inherited by the GSS, or the portion that was covered by the system-specific controls. Not knowing which controls are inherited and which ones are system-specific could result in a portion of the security controls not being properly evaluated and security vulnerabilities going undetected.

[redacted]

Our review of the C&A package for the [redacted] found the package did not include a list of common controls derived from the GSS within the SSP. When creating the SSP for [redacted] application, OIT inadvertently did not include a list of common controls that were derived from the GSS within the SSP. OIT's

[72] NIST SP 800-53, Rev. 3 states organizations assign a hybrid status to a security control when one part of the control is common and another part is system-specific. NIST SP 800-53, Rev. 3, p. 11.

SSP template contains a table for listing common controls inherited from the GSS. As a result, the security controls for the [redacted] system may not have been allocated properly, which could result in security controls not being properly evaluated.

Conclusion

NIT determined OIT did not identify the portion of the hybrid controls that were inherited by GSS, or the portion that was covered by the system-specific controls for the information systems in our sample universe. We further determined that OIT is not evaluating the security controls based on the full evaluation criteria that is identified in NIST SP 800-53A, Rev. 1. Lastly, we found the C&A package for the [redacted] does not include a list of common controls. As a result, a portion of the security controls may not be properly evaluated and security vulnerabilities may go undetected.

Recommendation 6:

The Office of Information Technology should identify the portion of the hybrid controls that are inherited from the general support system and the portion that should be evaluated as a system-specific control.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Recommendation 7:

The Office of Information Technology should review and update the [redacted] security plan and include a list of common controls that was inherited from the general support system in accordance with the approved system security plan template.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

REDACTED PUBLIC VERSION

Abbreviations

[redacted]	[redacted]
ATO	Authorization to Operate
[redacted]	[redacted]
[redacted]	[redacted]
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSC	Continuity Support Center
DAA	Designated Approving Authority
[redacted]	[redacted]
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GSS	General Support System
IT	Information Technology
[redacted]	[redacted]
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
NIT	Networking Institute of Technology, Inc.
OCA	Office of the Chief Accountant
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PAW	Privacy Analysis Worksheet
PIA	Privacy Impact Analysis
PII	Personally Identifiable Information
POA&M	Plan of Actions and Milestones
RMF	Risk Management Framework
SEC or Commission	U.S. Securities and Exchange Commission
[redacted]	[redacted]
SSP	System Security Plan
ST&E	Security Test and Evaluation
[redacted]	[redacted]
[redacted]	[redacted]

Definitions

FIPS 199 Analysis - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Security Assessment Plan - Provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures.

ST&E Report - The security document that contains the assessment criteria and the assessment results for the required security controls for each system.

Risk Assessment - The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

SSP Formal Document - A document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

POA&M Report - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Security Assessment Report - The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls.

Authorization to Operate - The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Scope and Methodology

The full version of this report includes information that the SEC considers to be sensitive or proprietary. To create this public version of the report, OIG redacted (blacked out) potentially sensitive, proprietary information from the report.

NIT conducted its review in accordance with *SEC/OIG Office of Audit's Audit Manual and Standard Operating Procedures*.[73]

Scope. NIT conducted this review from June 2012 to December 2012. The scope of the review consisted of examining the OIT's C&A process to ensure it is based on the RMF criteria identified in NIST SP 800-37, Rev. 1. The six steps are listed below:

- *Step 1–Categorize Information System*: We examined the system documentation to determine if the OIT is categorizing the information system in accordance with FIPS 199, describing the information system (including system boundary), and registering the information system with appropriate organizational program/management offices.

- *Step 2–Select Security Controls:* We evaluated the security controls to establish whether an initial set of baseline security controls for the information system includes tailoring based on the security categorization, organizational assessment of risk, and local conditions.

- *Step 3–Implement Security Controls:* We evaluated the SSP and ST&E reports to identify whether the security controls are implemented and identified in the tailored control list.

- *Step 4–Assess Security Controls* - We assessed the SEC processes for evaluating security controls to determine if the SEC is using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- *Step 5–Authorize Information System*: We reviewed the C&A package for each system to determine if the SEC C&A process were in accordance with NIST SP 800-37, Rev. 1 guidance.

[73] *SEC/OIG Office of Audit's Audit Manual and Standard Operating Procedures, (*May 2012).

- *Step 6–Monitor Security Controls:* NIT reviewed the continuous monitoring program to establish whether or not there is an effective monitoring strategy for the systems. The continuous monitoring strategy for the information systems identifies the security controls monitored, the frequency of monitoring, and the control assessment approach.

We assessed the C&A process OIT and other information system owners use to test its systems and to determine compliance with governing SEC policies and procedures, industry best practices, and applicable government laws, directives, regulations, and publications such as the OMB A-130 in accordance with OMB A-123. We completed the review of the SEC's systems C&A process, performed the necessary evaluation procedures, and compiled this report for the SEC OIG.

Methodology. To meet the objective of reviewing OIT's C&A process to ensure it is based on the six-step RMF criteria identified in NIST SP 800-37, Rev. 1, and to determine if the SEC has appropriately certified and accredited its systems in accordance with appropriate guidelines, we interviewed key OIT personnel and examined policies, procedures, and other related documentation. The key personnel included system owners, OIT representatives, and OIG stakeholders. We conducted follow-up interviews to gather additional evidence, and reviewed relevant documentation (such as policies, procedures, and roles and responsibilities) to address the evaluation objective. We reviewed policies and procedures to include RFMs, and had discussions with SEC officials to discuss and confirm our analysis.

To meet the objective of determining if the C&A process for critical applications is effective in identifying and mitigating risks in a timely manner and assessing the adequacy of OIT's internal controls and compliance with internal information security policies and procedures and industry best practices, standards, and guidelines, we conducted a detailed ST&E review based on a judgmental sampling of approximately 12 percent (24 of 200) security controls from the OIT's ST&E documents for the 11 information systems in a sample universe. Also, we reviewed other documentation relating to the scope of the C&A review. Our analysis is based on information provided from various sources, interviews with key SEC OIT personnel, prior audit coverage, support documentation, and artifacts provided to our staff.

Management Controls. Consistent with the objectives of this review, we did not assess OIT's management control structure. We reviewed existing controls at the Commission considered specific to the C&A review. To thoroughly understand OIT's management controls pertaining to its policies and procedures and methods of operation, we relied on information requested from and supplied by OIT staff members and information from interviews held with various OIT personnel. In accordance with OMB A-123, we evaluated management's responsibility for establishing and maintaining internal control to achieve the objectives of effective and efficient operations and compliance with applicable laws and regulations.

Use of Computer-Processed Data. We did not assess the reliability of OIT's computers because it did not pertain to our objectives for this review. Further, NIT did not perform any tests on the general or application controls over OIT's automated systems because such tests were not within the scope of our work. The information retrieved from these systems as well as the requested documentation provided to us, was sufficient, reliable, and adequate to use in meeting our stated objectives.

Judgmental Sampling. We conducted a limited-scope review of the Commission's C&A process. We performed a review on the SEC's computer systems that were certified and accredited from January 1, 2010 to March 31, 2012. Our evaluation consisted of reviewing C&A packages for a judgmental sample of 15 percent (11 of 59) of the SEC's computer systems. The systems selected for testing in our sample universe consisted of the [redacted] We based the judgmental sample on a limited scope review of both internal and external systems found in the SEC's inventory compliance workbook. The ST&E review consisted of controls that were reviewed within the scope and were based on a random selection of critical controls from the SEC's ST&E reports.[74] We also interviewed nine of these system owners.

[74] The ST&E controls selected for our review were as follows: AC-2.6, AC-3.1, AC-6.1, AU-2.1, AU-5.1, AU-5.2, AU-6.1, CA-2.1, CA-2.3, CA-7.1, CM-2.1, CM-2e1.1, CM-2e.3.1, CM-6.1, CP-2.1, IA-2.1, IA-7.1, PL-2.1, PL-5.1, RA-2.1, RA-5.1, SA-8.1, SC-4.1, SC-8.1, and SI-7.1.

Criteria

Federal Information Security Management Act of 2002, **Title III, Pub. L. No. 107-347.** Requires federal agencies to develop, document, and implement an agency-wide program providing security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Office of Management and Budget Memorandum A-123, ***Management's Responsibility for Internal Controls****.* Provides guidance to agencies for ensuring information systems are protected throughout the lifecycle process.

Office of Management and Budget Memorandum A-130, *Management of Federal Information Resources*. Provides guidance to agencies for managing federal information resources.

Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. Establishes the requirement for agencies to conduct PIAs for information systems.

NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model*. Provides guidance for security training.

NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*. Provides guidance for security training and implementation.

NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations.* Provides guidance related to the steps in the RMF addressing security control selection.

NIST Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans* (companion guideline to NIST SP 800-53). Covers the security control assessment and continuous monitoring steps in the RMF and provides guidance on the security assessment process.

NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life*

Cycle Approach. Provides guidance for applying the RMF to federal information systems.

NIST Special Publication 800-60, Volume 1, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories.* Addresses the FISMA direction to develop guidelines recommending agencies conduct privacy impact assessments to determine if the information systems contain PII.

List of Recommendations

Recommendation 1:

The Office of Information Technology should implement a centralized repository for managing certification and accreditation activities including the security test and evaluation process (i.e., evidence, artifacts, assessor date, and sites assessed).

Recommendation 2:

The Office of Information Technology should determine if the Commission has certification and accreditation files that are stored on its contractor's off-site servers and, in the future, require contractor to maintain all Commission files on servers the Commission owns and manages.

Recommendation 3:

The Office of Information Technology should develop and provide security status reports to the designated approving authority as specified in their authorization to operate memorandums.

Recommendation 4:

The Office of Information Technology (OIT) should review the security documentation in the certification and accreditation packages, including system categorization documents, risk assessment documents, and system security plans to ensure that references to personally identifiable information, privacy impact assessments, and privacy analysis worksheets, are consistently providing the same disposition regarding Personally Identifiable Information.

Recommendation 5:

The Office of Information Technology should provide a documented brief that management officials (system owners) can use as a resource reference.

Recommendation 6:

The Office of Information Technology should identify the portion of the hybrid controls that are inherited from the general support system and the portion that should be evaluated as a system-specific control.

Recommendation 7:

The Office of Information Technology should review and update the [redacted] [redacted] security plan and include a list of common controls that was inherited from the general support system in accordance with the approved system security plan template.

REDACTED PUBLIC VERSION

Appendix VI

Management Comments

MEMORANDUM

March 25, 2013

To: Jacqueline Wilson, Assistant Inspector General for Audits, Office of Inspector General

Pamela Dyson for

From: Thomas A. Bayer[1], Chief Information Officer, Office of Information Technology

Subject: Management Response, *Review of the SEC's Systems Certification and Accreditation Process*, Report No. 515

Thank you for the opportunity to comment on the recommendations in the report annotated above, as we work together for the integrity and efficiency of the Commission. We appreciate the Office of Inspector General's insights and are providing the official response from the Office of Information Technology (OIT).

Recommendation 1: "The Office of Information Technology should implement a centralized repository for managing certification and accreditation activities including the security test and evaluation process (i.e. evidence, artifacts, assessor date, and sites assessed)."

Management Response: OIT concurs with the recommendation. OIT Security is working toward implementing a centralized repository that would maintain the deliverables that support the authorization to operate.

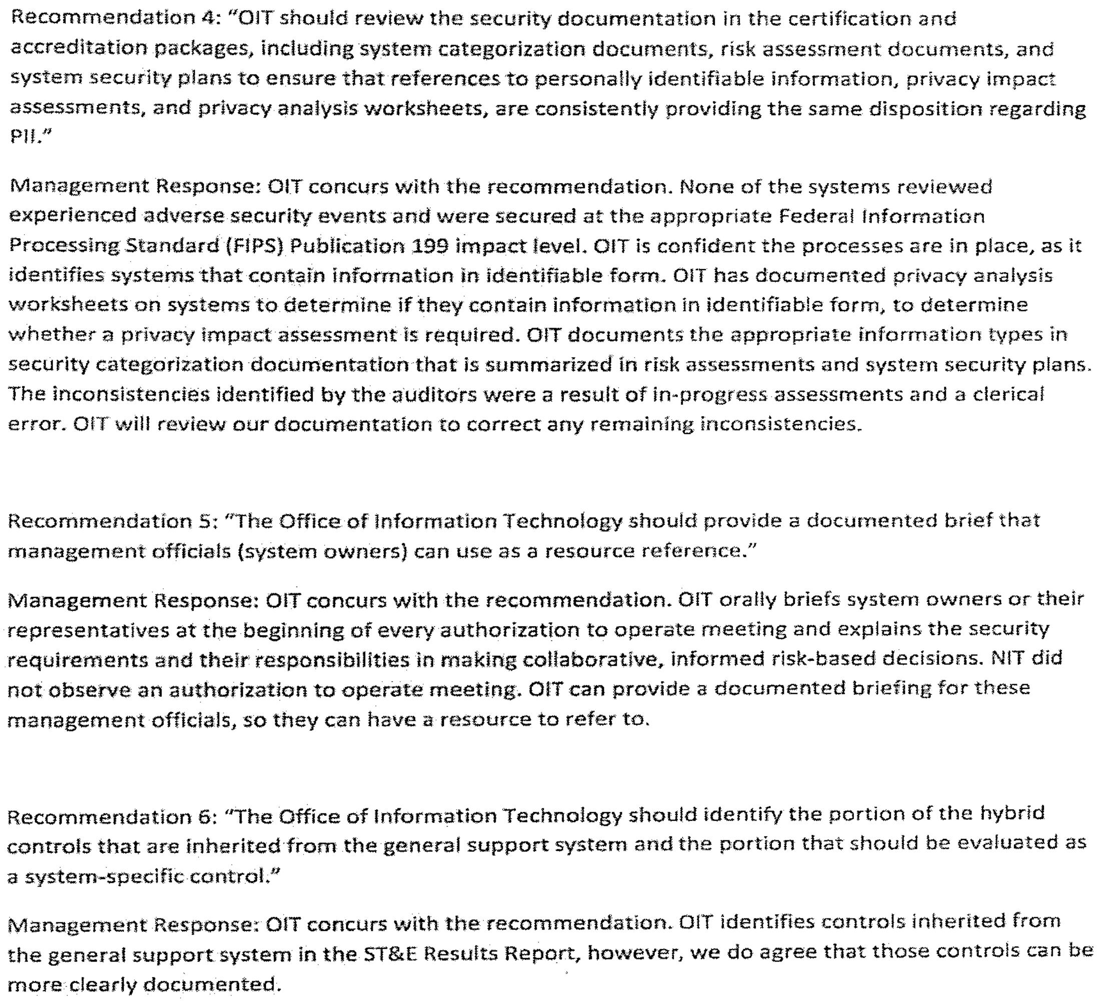
Recommendation 2: "The Office of Information Technology should determine if the Commission has certification and accreditation files that are stored on its contractor's off-site servers and, in the future, require contractor to maintain all Commission files on servers the Commission owns and manages."

Management Response: OIT concurs with the recommendation. OIT Security is aware of Commission files on contractors' servers and is working on rectifying the situation.

Recommendation 3: "The Office of Information Technology should develop and provide security status reports to the designated approving authority as specified in their authorization to operate memorandums."

Management Response: Concur with the recommendation. OIT will revise the language in the authorization to operate memorandums and report accordingly.

[1] Pamela C. Dyson, Deputy Chief Information Officer, Office of Information Technology



Recommendation 4: "OIT should review the security documentation in the certification and accreditation packages, including system categorization documents, risk assessment documents, and system security plans to ensure that references to personally identifiable information, privacy impact assessments, and privacy analysis worksheets, are consistently providing the same disposition regarding PII."

Management Response: OIT concurs with the recommendation. None of the systems reviewed experienced adverse security events and were secured at the appropriate Federal Information Processing Standard (FIPS) Publication 199 impact level. OIT is confident the processes are in place, as it identifies systems that contain information in identifiable form. OIT has documented privacy analysis worksheets on systems to determine if they contain information in identifiable form, to determine whether a privacy impact assessment is required. OIT documents the appropriate information types in security categorization documentation that is summarized in risk assessments and system security plans. The inconsistencies identified by the auditors were a result of in-progress assessments and a clerical error. OIT will review our documentation to correct any remaining inconsistencies.

Recommendation 5: "The Office of Information Technology should provide a documented brief that management officials (system owners) can use as a resource reference."

Management Response: OIT concurs with the recommendation. OIT orally briefs system owners or their representatives at the beginning of every authorization to operate meeting and explains the security requirements and their responsibilities in making collaborative, informed risk-based decisions. NIT did not observe an authorization to operate meeting. OIT can provide a documented briefing for these management officials, so they can have a resource to refer to.

Recommendation 6: "The Office of Information Technology should identify the portion of the hybrid controls that are inherited from the general support system and the portion that should be evaluated as a system-specific control."

Management Response: OIT concurs with the recommendation. OIT identifies controls inherited from the general support system in the ST&E Results Report, however, we do agree that those controls can be more clearly documented.

REDACTED PUBLIC VERSION

Recommendation 7: "The Office of Information Technology should review and update the [redacted] security plan and include a list of common controls that was inherited from the general support system in accordance with the approved system security plan template."

Management Response: OIT concurs with the recommendation. OIT will be updating the system security plan template for internally hosted applications to include a list of common controls inherited from the general support system.

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