U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016

March 7, 2017
Report No. 539

REDACTED FOR PUBLIC RELEASE

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 7, 2017

TO: Kenneth Johnson, Acting Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016*, Report No. 539

Attached is the Office of Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC or the agency) compliance with the Federal Information Security Modernization Act for Fiscal Year 2016. To improve the SEC's information security program, we urge management to take action to address areas of potential risk identified in this report. The report contains 21 recommendations for corrective action that, if fully implemented, should strengthen the SEC's information security posture.

On February 8, 2017, we provided management with a draft of our report for review and comment. In its February 23, 2017, response, management concurred with our recommendations. We have included management's response as Appendix II in the final report.

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

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits Evaluations, and Special Projects.

Attachment

cc: Michael S. Piwowar, Acting Chairman
Jaime Klima, Co-Chief of Staff, Office of the Chairman
Richard Grant, Co-Chief of Staff, Office of the Chairman
Peter Uhlmann, Managing Executive, Office of the Chairman
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Sanket J. Bulsara, Acting General Counsel
Keith Cassidy, Director, Office of Legislative and Intergovernmental Affairs

REDACTED FOR PUBLIC RELEASE

Rick A. Fleming, Investor Advocate
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Andrew Krug, Chief Information Security Officer, Office of Information Technology
Lacey Dingman, Chief Human Capital Officer, Office of Human Resources
Vance Cathell, Director, Office of Acquisitions
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

U.S. SECURITIES AND EXCHANGE COMMISSION OFFICE OF INSPECTOR GENERAL

Executive Summary

Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016

Report No. 539
March 7, 2017

Why We Did This Audit

The U.S. Securities and Exchange Commission's (SEC or agency) information systems process and store significant amounts of sensitive, nonpublic information, including information that is personally identifiable, commercially valuable, and market-sensitive. The SEC's information security program protects the agency from the risk of unauthorized disclosure, modification, use, and disruption of this sensitive, nonpublic information. Without these controls, the agency's ability to accomplish its mission could be inhibited, and privacy laws and regulations that protect such information could be violated. To comply with the Federal Information Security Modernization Act of 2014 (FISMA), the SEC Office of Inspector General assessed the SEC's implementation of FISMA information security requirements based on fiscal year (FY) 2016 guidance issued to Inspectors General (IGs) by the U.S. Department of Homeland Security.

What We Recommended

To improve the SEC's information security program, we made 21 recommendations related to the 8 FY 2016 IG FISMA Reporting Metrics assessment domains. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. The full version of this report contains sensitive information about the SEC's information security program. We redacted the sensitive information in this public version.

What We Found

The SEC's Office of Information Technology (OIT) has overall management responsibility for the SEC's information technology program, including information security. Since the last fiscal year, OIT improved in key information security program areas, in part by updating policies and procedures, enhancing the functionality of the OIT Risk Committee, and strengthening the system authorization process. OIT also implemented procedures to more efficiently address plan of action and milestones items. Furthermore, OIT continues to enhance capabilities and develop tools in areas such as risk analytics, vulnerability management, and configuration management.

However, we found that the SEC information security program does not meet the FY 2016 IG FISMA Reporting Metrics' definition of "effective." Specifically, as shown in the following table, we determined that the SEC's maturity level for the five Cybersecurity Framework security functions was either Level 2 ("Defined") or Level 3 ("Consistently Implemented"). None of the functions reached Level 4 ("Managed and Measurable"), which the FY 2016 IG FISMA Reporting Metrics identifies as the level reflective of an effective information security program.

Cybersecurity Framework Security Functions	Maturity Level
Identify	Level 2: Defined
Protect	Level 2: Defined
Detect	Level 2: Defined
Respond	Level 3: Consistently Implemented
Recover	Level 3: Consistently Implemented

Furthermore, we identified opportunities for improvement in each of the eight FY 2016 IG FISMA Reporting Metrics assessment domains aligned with the Cybersecurity Framework security functions listed above. These opportunities for improvement pertain to critical security areas such as access and identity management, configuration management, and continuous monitoring. Implementing our recommended corrective actions will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, nonpublic information.

For additional information, contact the Office of Inspector General at (202) 551-6061 or http://www.sec.gov/oig.

TABLE OF CONTENTS

Figure and Tables

Appendices

ABBREVIATIONS

ATO	authorization to operate
DHS	U.S. Department of Homeland Security
FISMA	Federal Information Security Modernization Act
FY	fiscal year
IG	Inspector General
ISCM	Information System Continuous Monitoring
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
REV.	Revision
RMF	risk management framework
SEC or agency	U.S. Securities and Exchange Commission
SP	Special Publication
SSP	system security plan
US-CERT	United States Computer Emergency Readiness Team

Background and Objective

Background

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law 113-283), which amended the Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002 (Public Law 107-347). FISMA provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets, and a mechanism for oversight of Federal information security programs. FISMA also requires agencies to develop, document, and implement an agency-wide information security program to provide information security for the data and information systems that support the operations and assets of the agency.

In addition, FISMA requires Inspectors General (IGs) to annually assess the effectiveness of agency information security programs and practices and to report the results to the Office of Management and Budget (OMB) and Department of Homeland Security (DHS). This assessment includes testing and assessing the effectiveness of agency information security policies, procedures, and practices and a subset of agency information systems. In support of FISMA's independent evaluation requirements, DHS issued to IGs guidance on FISMA reporting for fiscal year (FY) 2016.[1]

The FY 2016 IG FISMA Reporting Metrics include eight assessment domains, which are aligned with the five information security functions outlined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework"),[2] as Table 1 illustrates.

Table 1. Cybersecurity Framework Security Functions Mapped to FY 2016 IG FISMA Reporting Metrics Assessment Domains

Cybersecurity Framework Security Functions	FY 2016 IG FISMA Assessment Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response
Recover	Contingency Planning

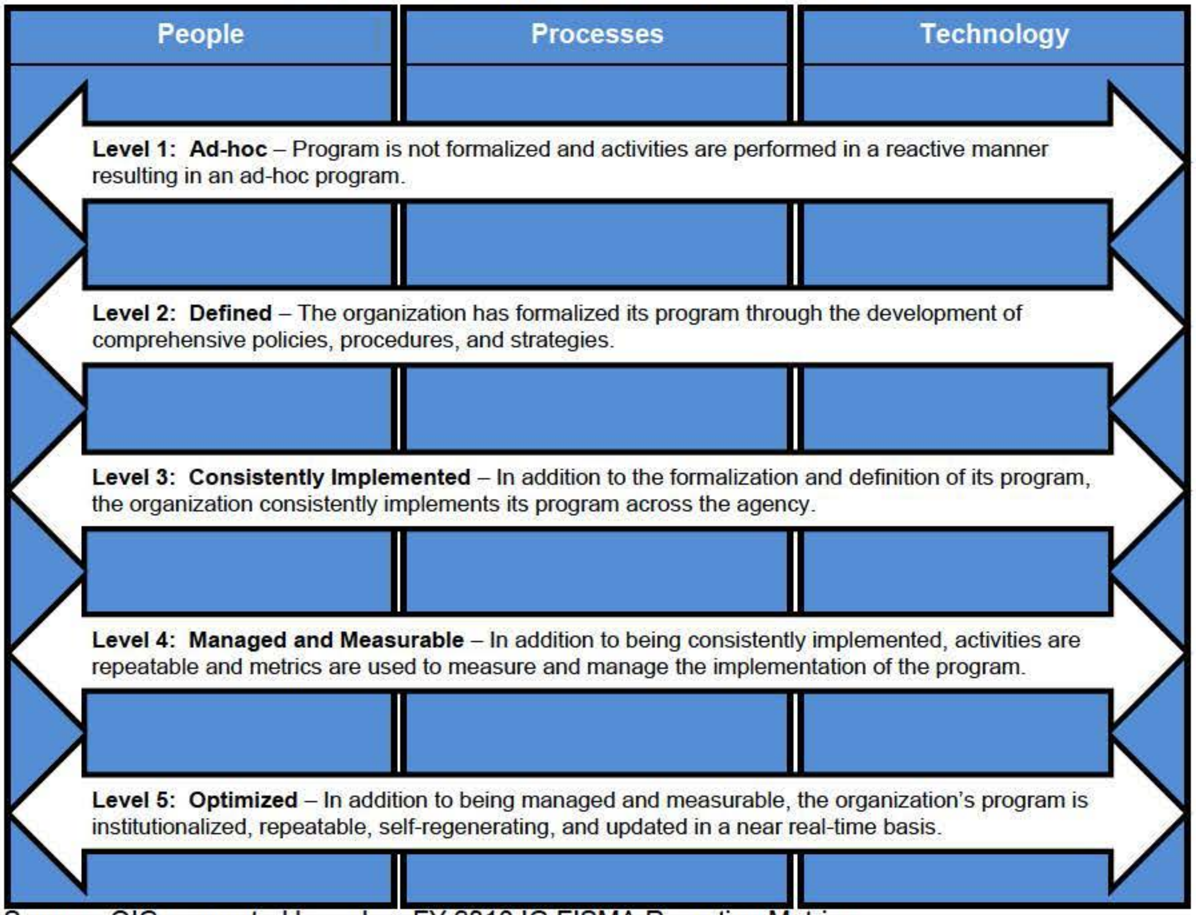
Source: Office of Inspector General (OIG)-generated from FY 2016 IG FISMA Reporting Metrics.

[1] *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics,* Version 1.1.3; September 26, 2016 (hereafter referred to as "FY 2016 IG FISMA Reporting Metrics").

[2] The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, and provides IGs with the guidance for assessing the maturity of controls to address those risks.

In FY 2015, the IG FISMA Reporting Metrics incorporated a maturity model to summarize the status of agencies' ISCM programs and their maturity on a 5-level scale. The FY 2016 IG FISMA Reporting Metrics continued this effort by establishing a maturity model for the incident response domain. The purpose of the maturity models is to (1) summarize the status of agencies' information security programs and their maturity; (2) provide transparency to agency Chief Information Officers, top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) help ensure consistency in IGs' annual FISMA reviews. The maturity model includes steps to assess an agency's program through an analysis of three domains: people, processes, and technology. The maturity levels of each of these domains dictate the overall maturity of an organization's program. A maturity ranking of level 4 or higher represents an effective level of security within an area. The figure below includes definitions of each maturity model level.

Figure. Maturity Model Level Definitions



Level 1: Ad-hoc – Program is not formalized and activities are performed in a reactive manner resulting in an ad-hoc program.

Level 2: Defined – The organization has formalized its program through the development of comprehensive policies, procedures, and strategies.

Level 3: Consistently Implemented – In addition to the formalization and definition of its program, the organization consistently implements its program across the agency.

Level 4: Managed and Measurable – In addition to being consistently implemented, activities are repeatable and metrics are used to measure and manage the implementation of the program.

Level 5: Optimized – In addition to being managed and measurable, the organization's program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis.

Source: OIG-generated based on FY 2016 IG FISMA Reporting Metrics.

Furthermore, in conjunction with the expansion of the maturity model concept, the FY 2016 IG FISMA Reporting Metrics incorporated a new methodology to score agencies' maturity across each Cybersecurity Framework security function. This is the first year this scoring methodology was used; therefore, scores are not comparable to prior years.

To comply with FISMA, we assessed the U.S. Securities and Exchange Commission's (SEC or agency) implementation of FISMA information security requirements in accordance with the FY 2016 IG Reporting Metrics. The results of these efforts supported the OIG's FY 2016 Cyberscope submission to OMB and DHS.[3]

Responsible Office. The SEC's Office of the Chief Operating Officer develops, coordinates, and provides strategic leadership and operational oversight of the agency's core mission support and compliance to include the Office of Information Technology (OIT). OIT has overall management responsibility for the SEC's information technology (IT) program, including information security. The Chief Information Officer directs OIT and is responsible for the development and maintenance of the agency-wide information security program. The Chief Information Officer designated the Chief Information Security Officer to carry out information security responsibilities. The Chief Information Security Officer is responsible, in part, for developing, maintaining, centralizing, and monitoring ongoing adherence to the SEC's Information Security Program Plan and supporting the Chief Information Officer in annual reporting on the effectiveness of the Information Security Program.

Prior Audits and Evaluations. Since last fiscal year, we closed the remaining two recommendations from our FY 2014 Federal Information Security Management Act evaluation report[4] and the four recommendations from our FY 2015 FISMA audit[5] because OIT took steps to improve key information security program areas. These steps included: (1) defining and documenting access methods for externally-hosted systems; (2) re-authorizing systems with expired authorizations to operate; (3) updating the OIT Risk Committee charter to address vacancies; (4) conducting OIT Risk Committee meetings in accordance with the updated charter; (5) implementing capabilities to more efficiently address plans of action and milestones; and (6) updating configuration management policies and procedures in support of rollback to previous versions of baseline configurations.

[3] Cyberscope is the platform Chief Information Officers, Privacy Officers, and IGs use to meet FISMA reporting requirements. The SEC OIG completed its FY 2016 Cyberscope submission to DHS and OMB on November 10, 2016.

[4] U.S. Securities and Exchange Commission, Office of Inspector General, *Federal Information Security Management Act: Fiscal Year 2014 Evaluation*, Report No. 529; February 5, 2015.

[5] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015*, Report No. 535; June 2, 2016.

Objective

Our overall objective was to assess the SEC's compliance with FISMA for FY 2016 based on guidance issued by OMB, DHS, and NIST. Specifically, we assessed the status of the following eight domains of the SEC's IT security program in accordance with the FY 2016 IG FISMA Reporting Metrics:

1. Risk Management
2. Contractor Systems
3. Configuration Management
4. Identity and Access Management
5. Security and Privacy Training
6. ISCM
7. Incident Response
8. Contingency Planning

To assess the SEC's compliance with FISMA, we judgmentally selected and reviewed a sample of 8 out of 18 FISMA-reportable information systems (or about 44 percent).[6] We also reviewed 10 contractor-operated systems added to the SEC's FISMA-reportable information systems inventory in September 2016. Appendix I includes additional information on our scope and methodology (including sampled systems); review of management controls; prior coverage; applicable Federal laws and guidance; and SEC regulations, policies, and procedures.

[6] We selected systems from the SEC's FISMA-reportable systems inventory as of June 28, 2016, which included 18 systems.

Results

Domain #1: Risk Management

Risk management encompasses the program and supporting processes used to manage information security risk to organizational operations, organizational assets, individuals, and other organizations. Risk management practices include establishing the context for risk-related activities, assessing risk, responding to risk, and monitoring risk over time. NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (dated March 2011), states to integrate the risk management process throughout the organization, a three-tiered approach is employed that addresses risk at the following levels: organizational (tier 1), mission/business processes (tier 2), and information systems (tier 3).

According to NIST SP 800-39, “The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization’s risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization.”

Tiers 1 and 2 Risk Management. NIST SP 800-39 tier 1 guidelines state, in part, agencies should establish and implement governance structures that provide oversight for the risk management activities conducted by organizations and include the establishment of the organization’s risk management strategy and the determination of risk tolerance.

According to NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (dated February 2010), tier 2 activities include, in part:
(i) defining the core missions and business processes for the organization;
(ii) prioritizing missions and business processes with respect to the goals and objectives of the organization; (iii) defining the types of information that the organization needs to successfully execute the stated missions and business processes and the information flows both internal and external to the organization; and (iv) developing an organization-wide information protection strategy and incorporating high-level information security requirements into the core missions and business processes.

We determined that the SEC developed capabilities to incorporate mission and business process-related risks into risk-based decisions at the organizational perspective. Specifically, the Office of the Chief Operating Officer established an Operational Risk Management program and Operational Risk Management Oversight Committee to improve operational risk awareness. However, the SEC has not developed an organizational risk management strategy as described in NIST SP 800-39 and the SEC's *Information Technology Security Program*.[7] Furthermore, the *Operational Risk Management Oversight Committee Charter*,[8] which according to the SEC also covers tier 2 mission and business-related risks, does not include responsibilities identified by NIST SP 800-37 as tier 2 activities.

Additionally, the charter does not include tier 2 responsibilities identified in OIT's *Information Security Risk Management Strategy*.[9] For example, OIT's *Information Security Risk Management Strategy* states that the tier 1 and 2 Risk Committee focus, in part, will include "ensuring security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from a Commission-wide perspective." The Committee's focus will also ensure that management of individual information system risk is consistent across the SEC. However, the *Operational Risk Management Oversight Committee Charter* does not identify responsibilities related to these specific information security risk objectives.

***Tier 3 Risk Management*.** The Risk Management Framework (RMF), described in NIST SP 800-37, provides a structured process that integrates risk management activities into the system development life cycle. The RMF operates primarily at tier 3 but also interacts with tiers 1 and 2.

NIST SP 800-37 describes the tasks required to apply the RMF at the information system level, which include: "(i) the categorization of information and information systems; (ii) the selection of security controls; (iii) the implementation of security controls; (iv) the assessment of security control effectiveness; (v) the authorization of the information system; and (vi) the ongoing monitoring of security controls and the security state of the information system."

We determined that the SEC has incorporated the six-step RMF into its tier 3 risk management activities through its *Information Security Compliance Program*.[10] However, we identified the following areas for improvement in the SEC's information systems-level risk management processes:

- The SEC's *Information Security Compliance Program* states assessments of risk help to maintain an ongoing situational awareness of the security state of the SEC's information systems and the environments in which the SEC's information systems operate. Furthermore, the policy states each information system undergoes a risk analysis at the beginning of its lifecycle and at least every 3 years thereafter. However, three of the eight systems we reviewed did not have a security risk assessment within the required 3-year interval.

[7] SEC Administrative Regulation 24-04, Rev. 2, *Information Technology Security Program*; August 12, 2015.

[8] *SEC Operational Risk Management Oversight Committee Charter*; May 17, 2016.

[9] *SEC OIT Information Security Risk Management Strategy*, Version 18; March 2013.

[10] SEC OIT 24-04.10, *Information Security Compliance Program*; September 8, 2016.

- The SEC's authorization processes did not fully ensure the implementation of the tailored set of baseline security controls. Specifically, a moderate impact baseline control was missing from all eight system security plans (SSPs) that we reviewed without documented tailoring rationale.[11] In addition, two of the eight systems we reviewed were missing additional controls without documented tailoring rationale. Furthermore, at the end of FY 2016, OIT approved three of the SSPs we reviewed but system owners did not update the SSPs to reflect revised templates (which included the missing baseline controls) in accordance with OIT instructions.[12]

- The SEC has not consistently implemented its processes to identify and manage risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics, and security requirements. Specifically, we reviewed agreements supporting three of the interconnections used by SEC systems. According to NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* (dated August 2002), an Interconnection Security Agreement (or equivalent document) details the technical requirements of the interconnection. One of the agreements we reviewed was more than 20-years old, included extensive amounts of outdated information, had not been updated in accordance with the agreement, and did not include security attributes identified in NIST SP 800-47. Recently, OIT took efforts to update this agreement; however, this activity was not fully completed in FY 2016. Another Interconnection Security Agreement we examined was not reviewed or updated by the SEC annually as required by the agreement.

- The SEC has not fully implemented procedures to continuously and consistently assess security controls, including hybrid and shared controls, 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. Specifically, the SEC's continuous monitoring policy lists two subparts of ISCM: (1) ongoing authorization, and (2) continuous diagnostics and mitigation.[13] However, OIT did not fully implement either of these activities. Additional information on this appears in the "Domain 6: ISCM" section of this audit report.

[11] NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; April 2013, states every security control from the applicable security control baseline is accounted for by the organization or by the information system owner. If certain security controls are tailored out, then the associated rationale is recorded in security plans for the information systems and approved by the responsible organizational officials as part of the security plan approval process.

[12] SEC OIT *System Security Plan Instructions for Information Systems Owners*; May 19, 2016, states, "all SSP information must be transferred to the appropriate new template before the system's initial authorization or re-authorization can commence."

[13] SEC OIT 24-04.09, *Continuous Monitoring*; September 14, 2016.

- The SEC has not fully implemented an ongoing information system authorization process in accordance with NIST guidance.[14] NIST guidance states, "to support ongoing authorization, security-related information for all implemented security controls, including inherited common controls, is generated and collected at the frequency specified in the organizational ISCM strategy." However, (1) the SEC has not defined the frequency for assessing each security control or control element for effectiveness, or the frequencies with which each metric is monitored; (2) the SEC's ISCM program is not mature; and (3) four of the eight systems we reviewed were operating on expired authorizations to operate (ATOs) for some duration of FY 2016.

- The SEC security authorization packages generally contain SSPs, risk assessments, and plans of action and milestones. However, four of the eight systems we reviewed had SSPs that had not been maintained (that is, reviewed and updated annually). Furthermore, we reviewed 10 additional contractor-operated systems and found that OIT and system owners did not consistently prepare and maintain authorization packages as required by the SEC's *Information Security Compliance Program*. Moreover, SEC authorizing officials granted contractor systems ATOs without complete authorization packages. Additional information on this topic is included in the "Domain 2: Contractor Systems" section of this audit report.

The SEC is taking steps to improve its risk management program, including developing a risk analytics program that will feed tier 3 information to the Operational Risk Management Oversight Committee. Furthermore, the SEC is updating Interconnection Security Agreement memorandums. However, these activities were not fully implemented in FY 2016, as described above. If not timely and properly addressed, the opportunities for improvement we identified may limit the SEC's ability to effectively manage information security risk to organizational operations, organizational assets, individuals, and other organizations.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the agency's risk management program, we recommend that:

Recommendation 1: The Office of the Chief Operating Officer, in coordination with the Office of Information Technology, should develop a comprehensive risk management strategy in accordance with National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, and document information security risk analytics to be measured and reported.

[14] *NIST Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management*; June 2014.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will work with the Office of the Chief Operating Officer to update the agency's Operational Risk Management Oversight Committee Charter in accordance with National Institute of Standards and Technology Special Publications 800-37 and 800-39. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, management should also develop a comprehensive risk management strategy. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 2: For the systems we reviewed and all other applicable agency systems, the Office of Information Technology should work with information system owners to develop and review system security plans in accordance with National Institute of Standards and Technology guidance and agency policies.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology has taken action to update all identified system security plans in accordance with National Institute of Standards and Technology guidance and agency policies. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 3: The Office of Information Technology should ensure that the agency documents and updates Interconnection Security Agreements in accordance with National Institute of Standards and Technology guidance and agency policy.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will take action to review and update all applicable Interconnection Security Agreements in accordance with National Institute of Standards and Technology guidance and agency policies. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #2: Contractor Systems

The SEC's *Information Security Compliance Program* establishes uniform policies, authorities, responsibilities, and procedures for the agency's IT security compliance.

This compliance program applies to all SEC IT systems and components and pertains to all SEC employees, contractors, and others who process, store, transmit, or have access to SEC computing resources. Similarly, OIT's *Assessment Program*[15] applies to both SEC and contractor systems. However, we identified the following areas for improvement related to the SEC's contractor system program:

- The contract for a cloud system in our sample hosted by a cloud provider did not include Federal Risk and Authorization Management Program standard contract clauses related to network log ownership, continuous monitoring, and the Government's right to perform audits. Furthermore, the SEC did not adequately specify within the contract how information security performance is measured, reported, and monitored. In addition, the contract included numerous references to outdated security policies.

- On September 1, 2016, SEC management added 10 contractor-operated systems to the agency's FISMA-reportable system inventory. We reviewed the authorization packages and ATOs for these 10 systems and determined that: (1) 3 of the 10 ATOs (or 30 percent) were not current for some duration of FY 2016, (2) OIT and system owners did not develop or properly update SSPs for 9 of the 10 systems (or 90 percent) in accordance with the SEC's *Information Security Compliance Program*, and (3) authorizing officials granted systems ATOs without complete authorization packages for 2 of 10 systems (or 20 percent).

The SEC is taking steps to improve its contractor systems program, including an ongoing project to develop a "menu" capability to provide suggested security contract clauses for different types of contracts. However, if not timely and properly addressed, the opportunities for improvement we identified could expose systems to unmitigated vulnerabilities and may foster a false sense of security that invites service interruptions, jeopardizes the availability and reliability of agency data, and exposes sensitive information.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the agency's contractor systems program, we recommend that:

Recommendation 4: The Office of Information Technology work with the Office of Acquisitions to review the cloud service provider contract for the cloud system we reviewed, and modify the contract to incorporate the appropriate Federal Risk and Authorization Management Program security clauses and requirements related to FISMA, National Institute of Standards and Technology, and agency requirements and guidelines.

[15] SEC OIT 24-04.10, *Assessment Program*; September 8, 2016.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will work the Office of Acquisitions to ensure all appropriate Federal Risk and Authorization Management Program security clauses are included in cloud service provider contracts. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 5: The Office of Information Technology work with information system owners to complete proper authorization documentation for the 10 contractor operated systems added to the agency's FISMA-reportable system inventory in September 2016.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology has taken action and is working to update authorization documentation for the 10 contractor systems identified by the OIG. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #3: Configuration Management

Configuration management is a collection of activities focused on establishing and maintaining the integrity of IT products and information systems through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. The SEC has developed a configuration management program that includes comprehensive agency policies and procedures. However, we identified the following areas for improvement related to the SEC's configuration management program:

- The SEC's *Information Security Controls Manual*[16] requires system owners to develop, document, and maintain an inventory of information system components. However, the authoritative hardware inventory required to be documented by system owners in the SSPs was not consistently updated or reviewed annually. In addition, the General Support System SSP (dated August 16, 2016) states that this control is only partially implemented. The SSP also refers to an updated inventory that is attached to the SSP. However, we determined that an updated inventory did not exist.

[16] SEC OIT 24-04A, Rev. 2.1, *Information Security Controls Manual*; November 10, 2015.

- The SEC does not fully (b) (7)(E) [redacted]

- The SEC has implemented baseline configurations for IT systems; however, these baselines are not consistently maintained as required. Specifically, SEC policy requires review and update of baseline configurations at least annually.[17] However, for five of the eight systems we reviewed, there was no evidence of review or update within the past year. For these systems, OIT had last made updates between FY 2013 and FY 2015.

- The SEC has implemented standard security settings for IT systems; however, these security settings are not consistently maintained in accordance with documented policy.[18] Specifically, the SEC's repository of security settings included and identified a number of operating system, application, and database security baselines that had not been approved by the Chief Information Security Officer, in accordance with SEC policy. Finally, the updated General Support System SSP identified additional issues related to security settings on machines and network devices.

- The SEC identifies and documents deviations from configuration settings. The SEC's *Information Security Controls Manual* states "exceptions/deviations from the mandatory configuration settings must be identified and documented by the Information System Owner, and approved by the Chief Information Security Officer [or designee]." However, the repository used by OIT to maintain documentation of deviations was incomplete and did not contain approval for all deviations. Therefore, we determined that OIT did not consistently approve deviations based on documented business justification and risk acceptance.

The SEC is taking steps to strengthen its configuration management program, including leveraging the results of its participation in DHS's Cyber Hygiene Initiative, which aims to assist agencies in identifying critical vulnerabilities associated with public-facing assets. However, the SEC's configuration management program is not fully effective as described above. If not timely and properly addressed, the opportunities for improvement we identified may expose SEC systems to configuration management vulnerabilities and exploitation.

[17] SEC OIT 24-04A, Rev. 2.1, CM-2 Baseline Configuration.

[18] SEC OIT 24-04.05, Security Baseline Configuration Management Policy; April 25, 2016.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the agency's configuration management program, we recommend that:

Recommendation 6: The Office of Information Technology ensure that system security plans reflect current hardware inventories for the systems we reviewed, in accordance with agency policy.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will take action to ensure the identified system security plans reference the most current hardware inventories in accordance with agency policy and asset management procedures. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 7: The Office of Information Technology ensure that information system owners review and update system baseline configurations annually.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will take action to ensure that all information system owners review and update system baseline configurations at least annually. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 8: The Office of Information Technology ensure the Chief Information Security Officer approves operating system, application, and database security baselines in accordance with agency policy.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will take action to update applicable policies and procedures to ensure that the Chief Information Security Officer or designee has signed all operating system, application, and database security baselines. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 9: The Office of Information Technology ensure the Chief Information Security Officer (or designee) approves deviations from configuration settings and documents appropriate business justification and risk acceptance.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will take action to update applicable policies and procedures to ensure that the Chief Information Security Officer (or designee) approves deviations from established security configuration settings. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, management should also ensure the Chief Information Security Officer (or designee) documents appropriate business justification and risk acceptance. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Domain #4: Identity and Access Management

The SEC's *Information Security Controls Manual* establishes policy for identity and access management. Specifically, the SEC employs an access management program to ensure that only authorized individuals have access to SEC information systems; users are restricted to authorized transactions, functions, and information; access is assigned according to the principles of separation of duties and least privilege; and users are individually accountable for their actions. Furthermore, an identification and authentication process confirms the identity of a user before granting access to SEC information and information systems. Although the SEC has established an identity and access management program, including policies and procedures, we identified the following areas for improvement:

- Access management processes did not ensure that 28 of 200 (or about 14 percent) judgmentally sampled users requiring access to SEC information and information systems signed appropriate access agreements and participated in required training before gaining access. Furthermore, SEC policy does not require users to recertify access agreements.

- The SEC did not meet the Administration Cybersecurity cross-agency priority goal of 100 percent strong authentication for all privileged users.[19] (b) (7)(E) [redacted]

[19] OMB M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (dated October 30, 2015), states in FY 2016 Federal agencies should continue to target the Administration Cybersecurity cross-agency priority goal of 100 percent strong authentication for all privileged users and for first quarter FY 2016, 85 percent strong authentication for unprivileged users. OMB M-16-04 initiates a protection activity directing agencies to complete PIV implementation for all employees and contractors required to obtain a PIV.

(b) (7)(E) [redacted]

- The SEC developed and executed a strategy in FY 2016 to require PIV for all users. However, at the end of FY 2016, the SEC had implemented PIV for 2,269 of 6,705 (or about 34 percent) of non-privileged users. Therefore, the SEC did not meet the cross-agency priority goal of 85 percent implementation.

- OIT's *Information Security Controls Manual* requires OIT to disable accounts after (b) (7) [redacted] days of inactivity. However, we determined that OIT performs only quarterly reviews of accounts that have been inactive for more than (b) (7) [redacted] days.

- Certain SEC issued (b) (7)(E) [redacted] do not enforce the SEC's unsuccessful login attempts policy. We noted that the SEC is switching to (b) (7)(E) [redacted] which, according to SEC management, will comply with the login policy.

If not timely and properly addressed, the opportunities for improvement we identified may increase the risk of unauthorized access to the SEC's network, information systems, and data.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the agency's identity and access management program, we recommend that:

Recommendation 10: The Office of Information Technology, in coordination with the Office of Human Resources, develop a process to document and track all users' initial access agreements and training before granting personnel access to agency information systems.

> **Management's Response.** The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will work with the Office of Human Resources to require personnel to complete initial network agreements and training prior to granting access to agency information systems. Management's complete response is reprinted in Appendix II.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 11: The Office of Information Technology, in coordination with the Office of Human Resources, develop a policy requiring access agreements to be recertified at a predetermined interval.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will work with the Office of Human Resources to update the applicable agency policies and procedures to ensure network access agreements are recertified on a periodic basis. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 12: The Office of Information Technology fully implement Personal Identity Verification or National Institute of Standards and Technology Level of Assurance 4 credentials for privileged and non-privileged users in accordance with cross-agency priority goals.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology has made significant progress in implementing Personal Identity Verification across the agency and continues to work towards achieving all cross-agency priorities associated with Personal Identity Verification compliance during fiscal year 2017. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 13: The Office of Information Technology update the *Information Security Controls Manual* to reflect the practice of performing quarterly reviews of accounts that have been inactive for more than [redacted] days.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will update the *Information Security Controls Manual* to reflect current practices relating to periodic account reviews. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #5: Security and Privacy Training

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (dated October 2003), states the following:

> Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked

> systems environment without ensuring that all people involved in using and managing IT understand their roles and responsibilities related to the organizational mission; understand the organization's IT security policy, procedures, and practices; and have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

The SEC has developed a security and privacy awareness and training program that includes comprehensive agency policies and procedures. However, we identified the following areas for improvement:

- OIT's current practices do not ensure that SEC employees receive privacy and information security awareness training annually as required by 5 Code of Federal Regulations §930.301, *Information Systems Security Awareness Training Program*. Specifically, OIT tracks privacy and information security training by fiscal year. So, a user who took privacy and information security training at the beginning of FY 2016 would not be required to take the training again until more than a year later, before the end of FY 2017.

- OIT has not fully implemented a process to evaluate the skills of users with significant security and privacy responsibilities, and then provide those users with additional security and privacy training content or implement strategies to close any identified skills gaps as required by NIST SP 800-50. Specifically, as of the end of FY 2016, only 5 of 509 users with significant security and privacy responsibilities participated in a skills inventory conducted by the Office of Human Resources.

- OIT measures the effectiveness of its privacy incident response program but does not (b) (7)(E)

Users who are unaware of their security responsibilities and/or have not received adequate security training may not effectively protect sensitive information. As a result, such users increase the SEC's risk of a computer security incident and loss, destruction, or misuse of sensitive Federal data assets.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the agency's security and privacy training program, we recommend that:

Recommendation 14: The Office of Information Technology, in coordination with the Office of Human Resources, update procedures to ensure users receive privacy and information security training annually (every 12 months).

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will work with the Office of Human Resources to assess the feasibility of ensuring that all personnel complete annual security and privacy awareness training at least once every 12 months as opposed to once per fiscal year. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is responsive to the recommendation.

Recommendation 15: The Office of Information Technology, in coordination with the Office of Human Resources, fully implement a process to evaluate the skills of users with significant security and privacy responsibilities and provide additional security and privacy training content, or implement strategies to close identified skills gaps.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology worked with the Office of Human Resources to complete a baseline cybersecurity workforce assessment in accordance with the Cybersecurity Workforce Assessment Act contained within the Consolidated Appropriations Act of 2016. As part of this effort, the Office of Human Resources, Office of Information Technology, and other agency stakeholders developed a strategy for mitigating identified gaps with appropriate training and certifications for staff. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 16: The Office of Information Technology consider (b) (7)(E) [redacted]

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will consider (b) (7)(E) [redacted] Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #6: Information Security Continuous Monitoring

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[20] An ISCM program allows an organization to maintain the security authorization of an information system over time in a dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions and business processes. The implementation of an ISCM program results in ongoing updates to the security plan, security assessment report, and plans of action and milestones, which are the three principal documents in a system's security authorization package.

Beginning in FY 2015, the IG FISMA Reporting Metrics incorporated a maturity model to measure the effectiveness of agency ISCM programs. We used this maturity model to review the SEC's ISCM program. Based on our review and input from OIT, we determined that the SEC's ISCM is operating at level 2 ("Defined") across the areas of "people," "processes," and "technology." Furthermore, we identified opportunities to mature the agency's ISCM program as follows:

> ***People.*** The SEC has made efforts to assess the skills, knowledge, and resources needed to effectively implement an ISCM program and defined how information will be shared. However, the SEC has not fully defined and communicated ISCM stakeholders and their responsibilities across the agency. Furthermore, the agency has not fully defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.
>
> ***Processes.*** The SEC has made efforts to define ISCM processes, identify performance measures and requirements to assess effectiveness, and capture lessons learned for making necessary improvements. However, OIT has not consistently implemented ISCM processes such as those pertaining to ongoing assessments and hardware, software, and configuration management.
>
> ***Technology.*** The SEC has made efforts to define how the agency will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the SEC has not fully identified and defined the ISCM technologies that the agency plans to use for continuous monitoring in all the FISMA-identified automation areas. Furthermore, the SEC has not fully and consistently implemented these technologies.

The SEC is obtaining additional continuous monitoring tools and assistance as part of a DHS Continuous Diagnostics and Mitigation contract. However, without a mature and consistently implemented ISCM program, the SEC is at greater risk of threats not being

[20] NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*; September 2011.

detected, which may result in unauthorized access or changes to information systems and lead to misuse, compromise, or loss of sensitive data/resources.

Recommendation, Management's Response, and Evaluation of Management's Response

To improve the agency's information security continuous monitoring program, we recommend that:

Recommendation 17: The Office of Information Technology finalize its Continuous Diagnostics and Mitigation Strategy to further mature its information security continuous monitoring activities across the areas of people, processes, and technology.

> **Management's Response.** The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will continue to develop its Continuous Diagnostics and Mitigation strategy. The current strategy involves maturing the Office of Information Technology's use of enterprise FISMA compliance capability for implementing continuous monitoring, creating an agency dashboard with technology inputs, and leveraging the U.S. Department of Homeland Security's Continuous Diagnostics and Mitigation program to implement new technologies. Management's complete response is reprinted in Appendix II.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #7: Incident Response

FISMA requires agencies to develop and implement procedures for detecting, reporting, and responding to security incidents, including mitigating the risks of such incidents before substantial damage is done. In addition, FISMA requires agencies to notify and consult with the United States Computer Emergency Readiness Team (US-CERT). Specifically, agencies are required within 1 hour to notify US-CERT of all computer security incidents involving a Federal Government information system with a confirmed impact to confidentiality, integrity, or availability. Furthermore, NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide* (dated August 2012) states establishing clear procedures for prioritizing the handling of incidents is critical. According to NIST, it is also vital to build relationships and establish suitable means of communication with other internal groups and with external groups.

In FY 2016, the IG FISMA Reporting Metrics incorporated a maturity model to measure the effectiveness of agency incident response programs. We used this maturity model to review the SEC's incident response program. Based on our review and input from OIT, we determined that the SEC's incident response program is operating at level 3 ("Consistently Implemented") across the areas of "people," "processes," and "technology." Furthermore, we identified opportunities to improve the agency's incident response program as follows:

People. The SEC met all the attributes within this domain at maturity level 3, which include processes related to defining roles and responsibilities, closing skills and knowledge gaps, using defined threat vector taxonomy, and integrating incident response activities with organizational risk management.

Processes. The SEC implemented processes to collaborate with DHS and other appropriate parties, captured qualitative and quantitative performance metrics, captured lessons learned, and conducted incident response activities comparably and predictably across the organization. However, the agency did not consistently report incidents within the 1-hour timeframe established by US-CERT. For example, we reviewed incident tickets that indicated the SEC's Security Operations Center notified US-CERT up to 14 days after the SEC had identified the incidents.

Technology. The SEC implemented Trusted Internet Connections security controls, used DHS' EINSTEIN program,[21] and implemented technologies to develop and maintain a baseline of network operations and expected data flows. However, the agency has not (b) (7)(E) [redacted]

To further mature the agency's incident response program and reach maturity level 4 ("Managed and Measurable"), the SEC must ensure incident response activities are repeatable and metrics are used to measure and manage the implementation of the program, achieve situational awareness, and control ongoing risk.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the agency's incident response program, we recommend that:

Recommendation 18: The Office of Information Technology develop metrics to track United States Computer Emergency Readiness Team response time, and review these metrics on a defined basis to verify compliance.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will review current incident reporting metrics to ensure United States Computer Emergency Readiness Team

[21] DHS developed the EINSTEIN system under the department's mission to provide a common baseline of security across the Federal civilian executive branch and to help agencies manage their cyber risk. EINSTEIN serves two key roles in Federal Government cybersecurity. The system detects and blocks cyber-attacks from compromising Federal agencies. Also, EINSTEIN provides DHS with the situational awareness to use threat information detected in one agency to protect the rest of the Government and to help the private sector protect itself.

response times are captured, evaluated, and reviewed with applicable operational teams. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 19: The Office of Information Technology update agency Security Operation Center Incident Management policies to include Office of Inspector General incident notification requirements developed in coordination with the Office of Inspector General.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will take action to review agency Security Operations Center Incident Response policies and procedures and work with the OIG to ensure notification requirements are properly documented. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 20: The Office of Information Technology (b) (7)(E) [redacted]

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. The Office of Information Technology will continue ongoing efforts to (b) (7)(E) [redacted] Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Domain #8: Contingency Planning

NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems* (dated May 2010), states that information systems are vital elements in most mission/business processes. Because information system resources are essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Furthermore, contingency planning is unique to each system and provides preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

The SEC has established a business continuity and disaster recovery policy that provides the authority and guidance necessary to reduce the impact of a disruptive event or disaster. However, we determined that the SEC did not annually test its system-specific contingency plans and disaster recovery plan, in accordance with agency policy, to determine the effectiveness of the plans as well as the readiness to execute the plans if necessary. The SEC did not complete a comprehensive annual exercise of the Enterprise Disaster Recovery Plan in FY 2016 or test the system-specific plans as required because (b) (7)(E) [redacted]

Without annual testing, reviews, and updates, the contingency plan might not provide adequate coverage of all system components, incorporate lessons learned from plan testing exercises, or address all potentially mission/business critical processes and their interdependencies.

Recommendation, Management's Response, and Evaluation of Management's Response

To improve the agency's contingency planning program, we recommend that:

Recommendation 21: The Office of Information Technology ensure that the Enterprise Disaster Recovery Plan and system-specific contingency plans are tested in fiscal year 2017 and updated as needed, in accordance with agency policies.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation. Due to unforeseen circumstances, the Office of Information Technology was unable to conduct a full disaster recovery exercise in September 2016 as previously scheduled. However, the Office of Information Technology successfully completed an annual enterprise disaster recovery exercise in February 2017 and will update associated contingency plans, as needed, in accordance with after-action reports. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

[redacted] (b)(7)(E) [redacted]

Overall Conclusion

Since last year, the SEC demonstrated improvements in key information security program areas, in part by updating policies and procedures, enhancing the functionality of the OIT Risk Committee, strengthening the system authorization process, and more efficiently addressing plan of action and milestones items. Furthermore, OIT continues to enhance capabilities and develop tools in areas such as risk analytics, vulnerability management, and configuration management. However, if not timely and properly addressed, the opportunities for improvement we identified could result in unauthorized access to, and disclosure of, the SEC's sensitive information and disruption of critical SEC operations. Implementing our recommended corrective actions will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, nonpublic information, and improve compliance with FISMA requirements.

Appendix I. Scope and Methodology

We conducted this performance audit from June 2016 through January 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope. Our overall objective was to assess the SEC's information security and privacy programs and respond to the FY 2016 IG FISMA Reporting Metrics. As required by FISMA, we assessed the SEC's information security posture based on guidance issued by OMB, DHS, and NIST.

The audit covered the period between October 1, 2015, and September 30, 2016, and addressed the following eight areas specified in the DHS's reporting instructions for FY 2016:

1. Risk Management
2. Contractor Systems
3. Configuration Management
4. Identity and Access Management
5. Security and Privacy Training
6. Information Security Continuous Monitoring
7. Incident Response
8. Contingency Planning

Methodology. We conducted a limited-scope review of the SEC's information security posture. Specifically, to assess system security controls, we reviewed the security assessment packages for a non-statistical, judgmentally selected sample of 8 of the SEC's 18 FISMA-reportable information systems (or about 44 percent). The sample consisted of the internally- and externally-hosted systems shown in Table 2.[23]

[23] We selected the information systems based on the SEC's system of record. The inventory included 18 information systems that were FISMA-reportable (as of June 28, 2016). We selected samples factoring in: (1) the time since we last selected the system as a FISMA sample item, (2) the system risk categorization, (3) the system's authorization to operate status, and (4) whether the system is hosted internally or externally.

Table 2. SEC Systems Sampled

[redacted]	[redacted]	(b) (7)(E) [redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Source: OIG-generated based on sampled systems' SSPs.

We interviewed key personnel, including personnel from the OIT Policy and Compliance Branch and system owner representatives for each system we reviewed. We also examined documents and records applicable to the SEC's information security processes, including memos, authorization packages, and applicable reports.

On September 1, 2016, OIT revised its FISMA-reportable information systems inventory to include 10 additional contractor-operated systems. These systems are as follows: (b) (7)(E) [redacted] As a result, we reviewed the ATOs and supporting documentation for each of these additional systems.

In addition, while reviewing the SEC's identity and access program and information security training program, we judgmentally selected a non-statistical sample of SEC personnel with network accounts to assess controls related to these programs. Because sampled items were non-statistical, we did not project our results and conclusions to the total user population or measure overall prevalence.

Federal Laws and Guidance: We reviewed applicable Federal laws and guidance, including the following:

- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.
- E-Government Act of 2002, Pub. L. No. 107-347.
- 5 Code of Federal Regulations §930.301, *Information Systems Security Awareness Training Program*.
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*; October 30, 2015.
- NIST *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*; February 12, 2014.
- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, Rev. 1; May 2010.
- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Rev. 1; February 2010.
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; March 2011.
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*; August 2002.

- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*; October 2003.
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Rev. 4; April 2013.
- NIST SP 800-61, *Computer Security Incident Handling Guide*, Rev. 2; August 2012.
- NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*; September 2011.
- *NIST Supplemental Guidance on Ongoing Authorization*, June 2014.

SEC Regulations, Policies, and Procedures: We reviewed applicable SEC regulations, policies, and procedures, including the following:

- SECR 24-04, *SEC OIT Information Technology Security Program*, Rev. 2; August 12, 2015.
- SEC OIT 24-04A, *SEC OIT Information Security Control Manual*, Version 2.1; November 10, 2015.
- SEC OIT 24-04.05, *Security Baseline Configuration Management Policy*, April 25, 2016.
- SEC OIT 24-04.09, *Continuous Monitoring*; September 14, 2016.
- SEC OIT 24-04.10, *Assessment Program*; September 8, 2016.
- SEC OIT 24-04.10, *Information Security Compliance Program*; September 8, 2016.

Internal Controls. Consistent with our audit objectives, we did not assess OIT's overall management control structure. Instead, we reviewed the SEC's controls specific to the FY 2016 IG FISMA Reporting Metrics. To understand thoroughly OIT's management controls pertaining to its policies, procedures, methods of operation, we relied on information requested from and supplied by OIT staff and information from interviews with OIT personnel. We found that the SEC generally complied with applicable FISMA and agency policies and procedures, except as identified in the report. Our recommendations, if implemented, should address the areas of improvement we identified.

Computer-processed Data. The U.S. Government Accountability Office's *Assessing the Reliability of Computer-Processed Data* (GAO-09-680G, July 2009) states, "data reliability refers to the accuracy and completeness of computer-processed data, given the uses they are intended for. Computer-processed data may be data (1) entered into a computer system or (2) resulting from computer processing." Furthermore, GAO-09-680G defines "reliability," "completeness," and "accuracy" as follows:

- "Reliability" means that data are reasonably complete and accurate, meet your intended purposes, and are not subject to inappropriate alteration.
- "Completeness" refers to the extent that relevant records are present and the fields in each record are appropriately populated.
- "Accuracy" refers to the extent that recorded data reflect the actual underlying information.

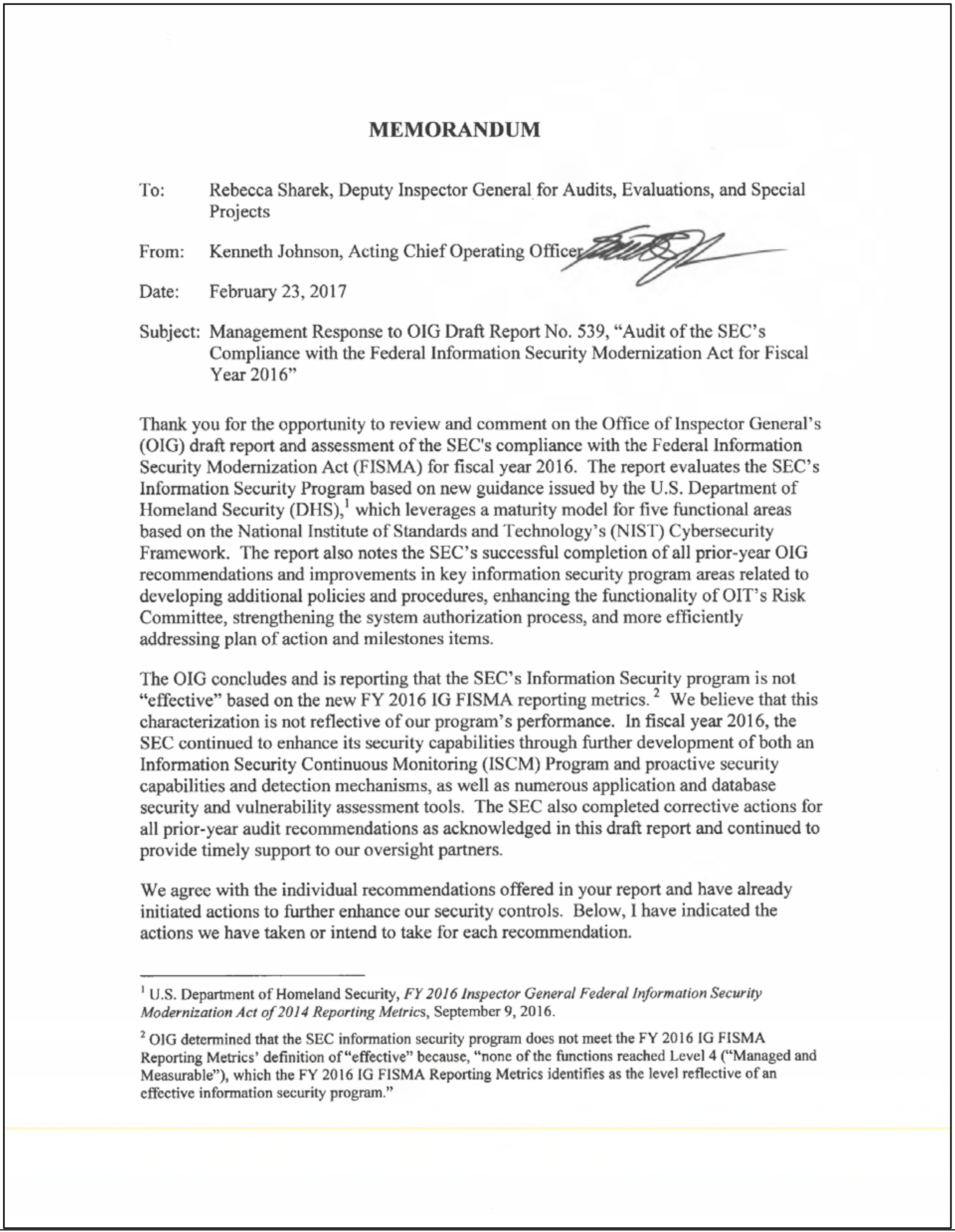
We used the SEC's governance, risk, and compliance tool, as a data source for obtaining documentation and reports related to the sampled systems and FISMA-reportable information systems inventory. We also used the SEC's training management system. We performed data reliability, completeness, and accuracy testing, in part, by comparing computer-processed information to testimonial evidence obtained from system and information owners and comparing system outputs for consistency. As a result of these tests, we determined that the computer-processed data we reviewed was sufficiently reliable to support our conclusions.

Prior Coverage. We reviewed prior year OIG FISMA reports. The FY 2015 report included four recommendations for corrective action. As of the date of this report, OIT has implemented all four recommendations. Although OIT addressed these recommendations, as we noted in the report, areas for improvement still exist.

- *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015*, Report No. 535; June 2, 2016
- *Federal Information Security Management Act: Fiscal Year 2014 Evaluation*, Report No. 529; February 5, 2015.

Unrestricted SEC OIG audit and evaluation reports can be accessed at: http://www.sec.gov/about/offices/oig/inspector_general_audits_reports.shtml.

Appendix II. Management Comments



MEMORANDUM

To: Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects

From: Kenneth Johnson, Acting Chief Operating Officer

Date: February 23, 2017

Subject: Management Response to OIG Draft Report No. 539, "Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2016"

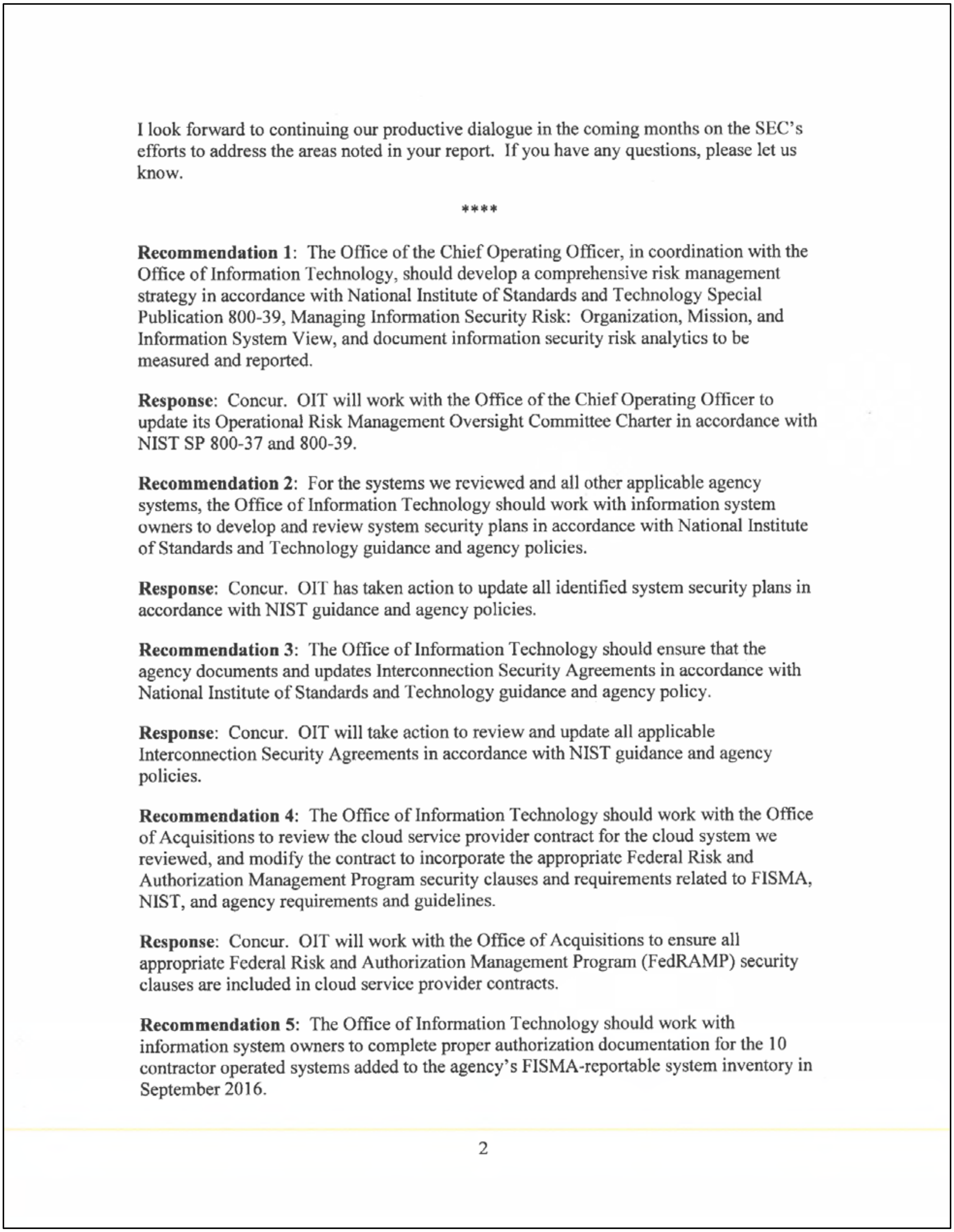
Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report and assessment of the SEC's compliance with the Federal Information Security Modernization Act (FISMA) for fiscal year 2016. The report evaluates the SEC's Information Security Program based on new guidance issued by the U.S. Department of Homeland Security (DHS),[1] which leverages a maturity model for five functional areas based on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. The report also notes the SEC's successful completion of all prior-year OIG recommendations and improvements in key information security program areas related to developing additional policies and procedures, enhancing the functionality of OIT's Risk Committee, strengthening the system authorization process, and more efficiently addressing plan of action and milestones items.

The OIG concludes and is reporting that the SEC's Information Security program is not "effective" based on the new FY 2016 IG FISMA reporting metrics.[2] We believe that this characterization is not reflective of our program's performance. In fiscal year 2016, the SEC continued to enhance its security capabilities through further development of both an Information Security Continuous Monitoring (ISCM) Program and proactive security capabilities and detection mechanisms, as well as numerous application and database security and vulnerability assessment tools. The SEC also completed corrective actions for all prior-year audit recommendations as acknowledged in this draft report and continued to provide timely support to our oversight partners.

We agree with the individual recommendations offered in your report and have already initiated actions to further enhance our security controls. Below, I have indicated the actions we have taken or intend to take for each recommendation.

[1] U.S. Department of Homeland Security, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metric*s, September 9, 2016.

[2] OIG determined that the SEC information security program does not meet the FY 2016 IG FISMA Reporting Metrics' definition of "effective" because, "none of the functions reached Level 4 ("Managed and Measurable"), which the FY 2016 IG FISMA Reporting Metrics identifies as the level reflective of an effective information security program."



I look forward to continuing our productive dialogue in the coming months on the SEC's efforts to address the areas noted in your report. If you have any questions, please let us know.

****

Recommendation 1: The Office of the Chief Operating Officer, in coordination with the Office of Information Technology, should develop a comprehensive risk management strategy in accordance with National Institute of Standards and Technology Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, and document information security risk analytics to be measured and reported.

Response: Concur. OIT will work with the Office of the Chief Operating Officer to update its Operational Risk Management Oversight Committee Charter in accordance with NIST SP 800-37 and 800-39.

Recommendation 2: For the systems we reviewed and all other applicable agency systems, the Office of Information Technology should work with information system owners to develop and review system security plans in accordance with National Institute of Standards and Technology guidance and agency policies.

Response: Concur. OIT has taken action to update all identified system security plans in accordance with NIST guidance and agency policies.

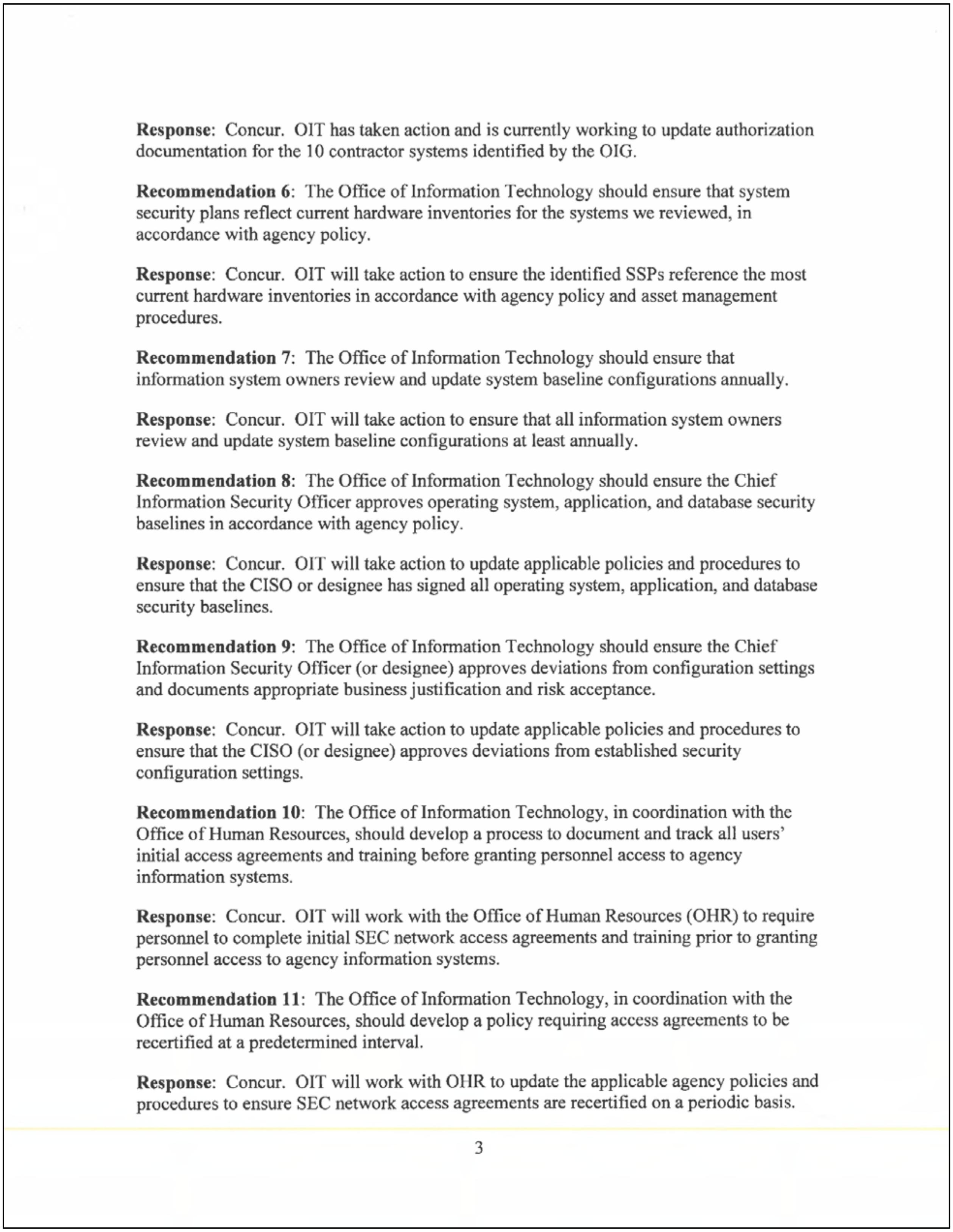
Recommendation 3: The Office of Information Technology should ensure that the agency documents and updates Interconnection Security Agreements in accordance with National Institute of Standards and Technology guidance and agency policy.

Response: Concur. OIT will take action to review and update all applicable Interconnection Security Agreements in accordance with NIST guidance and agency policies.

Recommendation 4: The Office of Information Technology should work with the Office of Acquisitions to review the cloud service provider contract for the cloud system we reviewed, and modify the contract to incorporate the appropriate Federal Risk and Authorization Management Program security clauses and requirements related to FISMA, NIST, and agency requirements and guidelines.

Response: Concur. OIT will work with the Office of Acquisitions to ensure all appropriate Federal Risk and Authorization Management Program (FedRAMP) security clauses are included in cloud service provider contracts.

Recommendation 5: The Office of Information Technology should work with information system owners to complete proper authorization documentation for the 10 contractor operated systems added to the agency's FISMA-reportable system inventory in September 2016.



Response: Concur. OIT has taken action and is currently working to update authorization documentation for the 10 contractor systems identified by the OIG.

Recommendation 6: The Office of Information Technology should ensure that system security plans reflect current hardware inventories for the systems we reviewed, in accordance with agency policy.

Response: Concur. OIT will take action to ensure the identified SSPs reference the most current hardware inventories in accordance with agency policy and asset management procedures.

Recommendation 7: The Office of Information Technology should ensure that information system owners review and update system baseline configurations annually.

Response: Concur. OIT will take action to ensure that all information system owners review and update system baseline configurations at least annually.

Recommendation 8: The Office of Information Technology should ensure the Chief Information Security Officer approves operating system, application, and database security baselines in accordance with agency policy.

Response: Concur. OIT will take action to update applicable policies and procedures to ensure that the CISO or designee has signed all operating system, application, and database security baselines.

Recommendation 9: The Office of Information Technology should ensure the Chief Information Security Officer (or designee) approves deviations from configuration settings and documents appropriate business justification and risk acceptance.

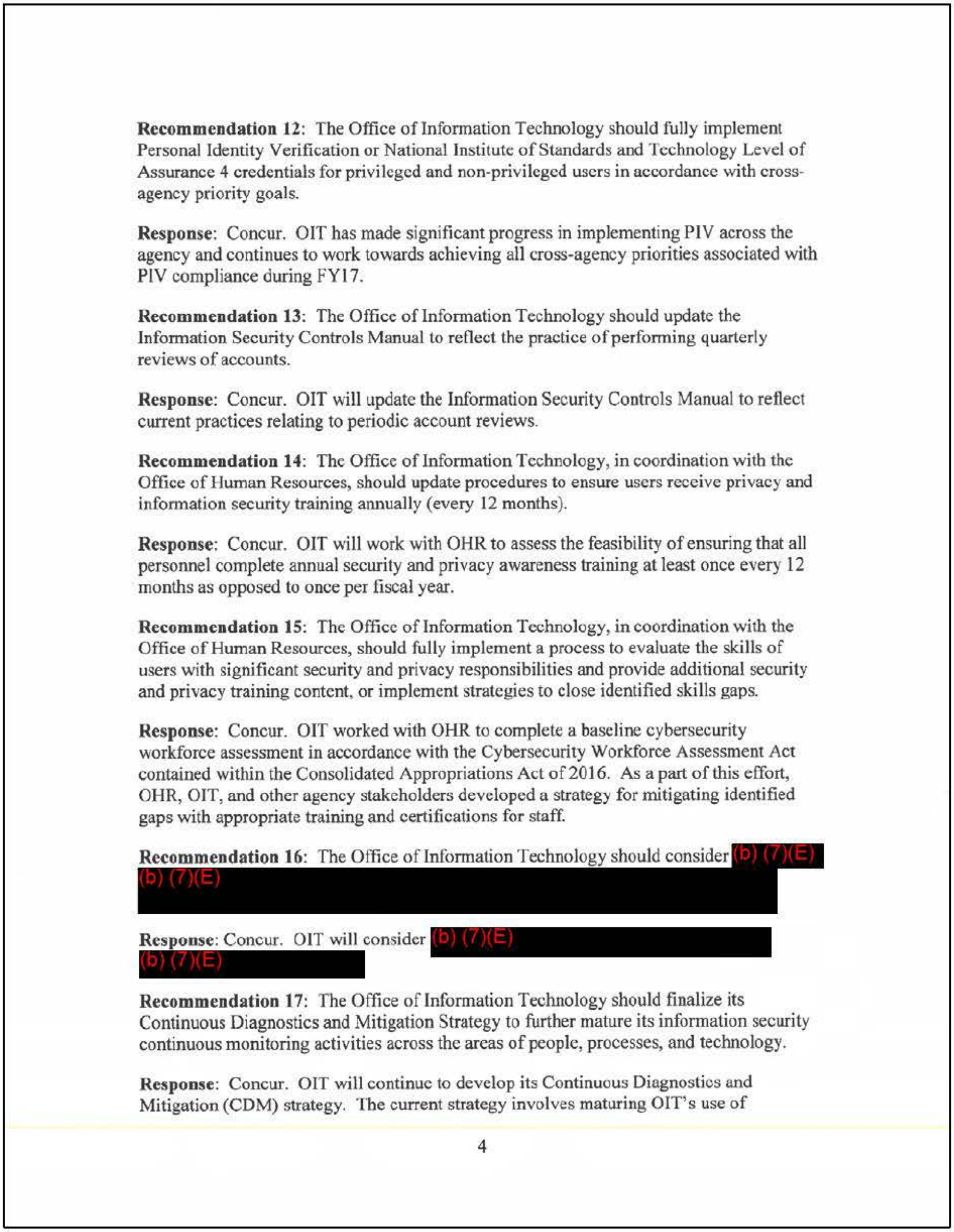
Response: Concur. OIT will take action to update applicable policies and procedures to ensure that the CISO (or designee) approves deviations from established security configuration settings.

Recommendation 10: The Office of Information Technology, in coordination with the Office of Human Resources, should develop a process to document and track all users' initial access agreements and training before granting personnel access to agency information systems.

Response: Concur. OIT will work with the Office of Human Resources (OHR) to require personnel to complete initial SEC network access agreements and training prior to granting personnel access to agency information systems.

Recommendation 11: The Office of Information Technology, in coordination with the Office of Human Resources, should develop a policy requiring access agreements to be recertified at a predetermined interval.

Response: Concur. OIT will work with OHR to update the applicable agency policies and procedures to ensure SEC network access agreements are recertified on a periodic basis.



Recommendation 12: The Office of Information Technology should fully implement Personal Identity Verification or National Institute of Standards and Technology Level of Assurance 4 credentials for privileged and non-privileged users in accordance with cross-agency priority goals.

Response: Concur. OIT has made significant progress in implementing PIV across the agency and continues to work towards achieving all cross-agency priorities associated with PIV compliance during FY17.

Recommendation 13: The Office of Information Technology should update the Information Security Controls Manual to reflect the practice of performing quarterly reviews of accounts.

Response: Concur. OIT will update the Information Security Controls Manual to reflect current practices relating to periodic account reviews.

Recommendation 14: The Office of Information Technology, in coordination with the Office of Human Resources, should update procedures to ensure users receive privacy and information security training annually (every 12 months).

Response: Concur. OIT will work with OHR to assess the feasibility of ensuring that all personnel complete annual security and privacy awareness training at least once every 12 months as opposed to once per fiscal year.

Recommendation 15: The Office of Information Technology, in coordination with the Office of Human Resources, should fully implement a process to evaluate the skills of users with significant security and privacy responsibilities and provide additional security and privacy training content, or implement strategies to close identified skills gaps.

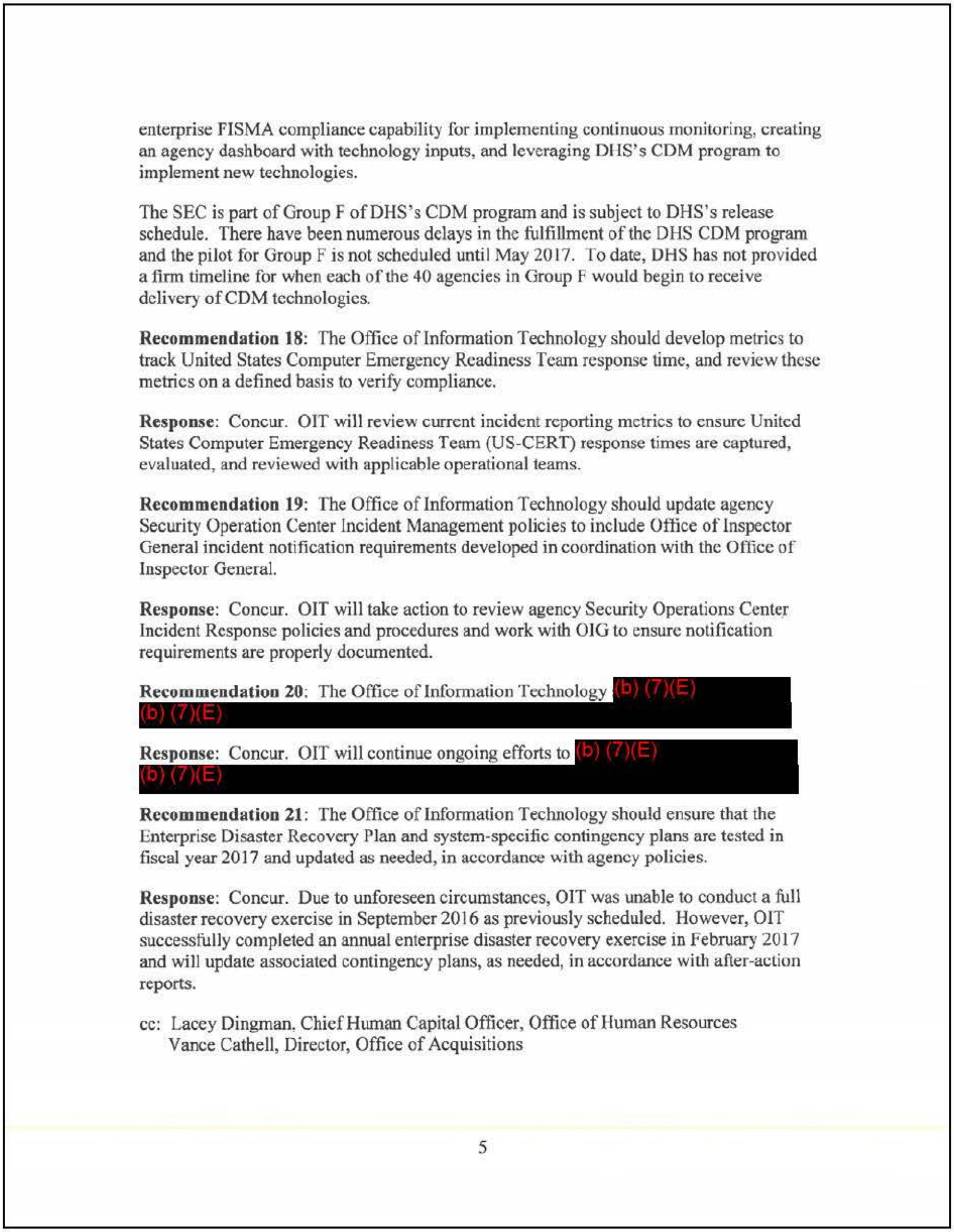
Response: Concur. OIT worked with OHR to complete a baseline cybersecurity workforce assessment in accordance with the Cybersecurity Workforce Assessment Act contained within the Consolidated Appropriations Act of 2016. As a part of this effort, OHR, OIT, and other agency stakeholders developed a strategy for mitigating identified gaps with appropriate training and certifications for staff.

Recommendation 16: The Office of Information Technology should consider (b) (7)(E) (b) (7)(E)

Response: Concur. OIT will consider (b) (7)(E) (b) (7)(E)

Recommendation 17: The Office of Information Technology should finalize its Continuous Diagnostics and Mitigation Strategy to further mature its information security continuous monitoring activities across the areas of people, processes, and technology.

Response: Concur. OIT will continue to develop its Continuous Diagnostics and Mitigation (CDM) strategy. The current strategy involves maturing OIT's use of



enterprise FISMA compliance capability for implementing continuous monitoring, creating an agency dashboard with technology inputs, and leveraging DHS's CDM program to implement new technologies.

The SEC is part of Group F of DHS's CDM program and is subject to DHS's release schedule. There have been numerous delays in the fulfillment of the DHS CDM program and the pilot for Group F is not scheduled until May 2017. To date, DHS has not provided a firm timeline for when each of the 40 agencies in Group F would begin to receive delivery of CDM technologies.

Recommendation 18: The Office of Information Technology should develop metrics to track United States Computer Emergency Readiness Team response time, and review these metrics on a defined basis to verify compliance.

Response: Concur. OIT will review current incident reporting metrics to ensure United States Computer Emergency Readiness Team (US-CERT) response times are captured, evaluated, and reviewed with applicable operational teams.

Recommendation 19: The Office of Information Technology should update agency Security Operation Center Incident Management policies to include Office of Inspector General incident notification requirements developed in coordination with the Office of Inspector General.

Response: Concur. OIT will take action to review agency Security Operations Center Incident Response policies and procedures and work with OIG to ensure notification requirements are properly documented.

Recommendation 20: The Office of Information Technology (b) (7)(E)
(b) (7)(E)

Response: Concur. OIT will continue ongoing efforts to (b) (7)(E)
(b) (7)(E)

Recommendation 21: The Office of Information Technology should ensure that the Enterprise Disaster Recovery Plan and system-specific contingency plans are tested in fiscal year 2017 and updated as needed, in accordance with agency policies.

Response: Concur. Due to unforeseen circumstances, OIT was unable to conduct a full disaster recovery exercise in September 2016 as previously scheduled. However, OIT successfully completed an annual enterprise disaster recovery exercise in February 2017 and will update associated contingency plans, as needed, in accordance with after-action reports.

cc: Lacey Dingman, Chief Human Capital Officer, Office of Human Resources
Vance Cathell, Director, Office of Acquisitions

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Mike Burger, Lead Auditor

John Dettinger, Auditor

Jacob Dull, Auditor

Sean Morgan, Assistant Counsel to the Inspector General

To Report Fraud, Waste, or Abuse, Please Contact:

Web:	www.reportlineweb.com/sec_oig
Telephone:	(877) 442-0854
Fax:	(202) 772-9265
Address**:**	U.S. Securities and Exchange Commission Office of Inspector General 100 F Street, N.E. Washington, DC 20549

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov. Comments, suggestions, and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.