



U.S. Securities and Exchange Commission  
Office of Inspector General  
Office of Audits

---

Fiscal Year 2018 Independent Evaluation of SEC's  
Implementation of the Federal Information Security  
Modernization Act of 2014



December 17, 2018  
Report No. 552

REDACTED FOR PUBLIC RELEASE



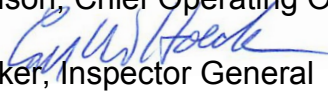
OFFICE OF  
INSPECTOR GENERAL

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

**M E M O R A N D U M**

December 17, 2018

**TO:** Kenneth Johnson, Chief Operating Officer

**FROM:** Carl W. Hoecker, Inspector General 

**SUBJECT:** *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014, Report No. 552*

Attached is the Independent Auditor's Report on the U.S. Securities and Exchange Commission's (SEC or agency) compliance with the Federal Information Security Modernization Act for Fiscal Year 2018. We contracted with Kearney and Company, P.C., (Kearney) to conduct this independent evaluation. SEC's Office of Inspector General (OIG) monitored Kearney's work to ensure it met professional standards and contractual requirements. Kearney conducted the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Kearney is wholly responsible for the attached evaluation report and the conclusions expressed therein. The OIG monitored Kearney's performance throughout the evaluation and reviewed their report and related documentation.

Kearney reported the SEC improved aspects of the agency's information security program, such as enhancing certain information security policies and procedures, strengthening authentication mechanisms, reducing the number of critical vulnerabilities, enhancing security awareness and training processes, and continuing efforts to enhance the agency's continuous monitoring program. However, as described in the attached report, Kearney identified opportunities for improvement in key areas and made 11 new recommendations to strengthen the SEC's information security program. As a result, Kearney noted that the agency's information security program did not meet the *FY 2018 IG FISMA Reporting Metrics'* definition of "effective."

On November 30, 2018, we provided management with a draft of Kearney' report for review and comment. In the agency's December 10, 2018 response, management concurred with Kearney' recommendations. Kearney included management's response as Appendix II in the final report.

**REDACTED FOR PUBLIC RELEASE**

To improve the SEC's information security program, we urge management to take action to address areas of potential risk identified in this report. Please provide the OIG with a written corrective action plan within the next 45 days 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 SEC will address the recommendations.

We appreciate management's courtesies and cooperation during the evaluation. Kearney's report contains non-public information about the SEC's information security program. As a result, the SEC OIG redacted the non-public information to create this public version. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits Evaluations, and Special Projects.

Attachment

cc: Jay Clayton, Chairman  
Lucas Moskowitz, Chief of Staff, Office of Chairman Clayton  
Sean Memon, Deputy Chief of Staff, Office of Chairman Clayton  
Peter Uhlmann, Managing Executive, Office of Chairman Clayton  
Kara M. Stein, Commissioner  
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein Robert J. Jackson, Jr., Commissioner  
Caroline Crenshaw, Counsel, Office of Commissioner Jackson  
Prashant Yerramalli, Counsel, Office of Commissioner Jackson  
Hester M. Peirce, Commissioner  
Jonathan Carr, Counsel, Office of Commissioner Peirce  
Elad L. Roisman, Commissioner  
Matthew Estabrook, Counsel, Office of Commissioner Roisman  
Robert B. Stebbins, General Counsel  
Rick A. Fleming, Investor Advocate  
John J. Nester, Director, Office of Public Affairs  
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs Charles Riddle, Acting Director/Chief Information Officer, Office of Information Technology  
Andrew Krug, Chief Information Security Officer, Office of Information Technology  
Vance Cathell, Director, Office of Acquisitions  
Jamey McNamara, Acting Chief Human Capital Officer, Office of Human Resources  
Julie Erhardt, Acting Chief Risk Officer, Office of the Chief Operating Officer

***Fiscal Year 2018 Independent Evaluation  
of the U.S. Securities and Exchange  
Commission's Implementation of the  
Federal Information Security  
Modernization  
Act of 2014***

**December 14, 2018**



*1701 Duke Street, Suite 500  
Alexandria, VA 22314*

---

## COVER LETTER

---

December 14, 2018

Mr. Carl W. Hoecker  
Inspector General  
U. S. Securities and Exchange Commission  
100 F Street, NE  
Washington, D.C. 20549

Dear Mr. Hoecker:

This report presents the results of Kearney & Company, P.C.'s (referred to as "Kearney," "we," and "our" in this report) independent evaluation of the U.S. Securities and Exchange Commission's (referred to as "SEC" or "agency") information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires all Federal agencies to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, FISMA requires Federal agencies or a contracted independent external auditor to conduct an annual independent evaluation of its information security program and practices, as well as an assessment of its compliance with the requirements of FISMA. Kearney conducted this independent evaluation of the SEC's information security program and practices on behalf of the SEC Office of Inspector General (OIG) in accordance with the Council of Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Kearney's evaluation included inquiries, observations, and inspection of SEC documents and records, as well as direct testing of controls. We are pleased to provide our report, the *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014*.

The objectives of this evaluation were to evaluate the effectiveness of the SEC's information security program and practices and respond to the Department of Homeland Security's (DHS) *Fiscal Year 2018 Inspector General FISMA Reporting Metrics (FY 2018 IG FISMA Reporting Metrics)*, dated May 24, 2018. Kearney's methodology for the FY 2018 FISMA evaluation included testing the effectiveness of selected security controls the SEC has implemented in eight sampled information systems, including the (b) (7)(E) [REDACTED], for compliance with the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53, Rev. 4). The *FY 2018 IG FISMA Reporting Metrics* utilize a maturity model and request that Inspectors General (IG) evaluate and rate the effectiveness of security controls for each of the five NIST Cybersecurity Framework Functions (i.e., Identify, Protect, Detect, Respond, and Recover). To achieve an effective level of information security under the maturity model, agencies must reach Level 4: *Managed and Measurable*.



Since FY 2017, the SEC’s Office of Information Technology (OIT) improved aspects of its information security program. Among other actions taken, OIT made progress by enhancing information security policies and procedures to address security risks at the organizational and information system levels, strengthening authentication mechanisms, reducing the number of critical vulnerabilities, enhancing its security awareness and training processes, and continuing its efforts to enhance its continuous monitoring program.

Although the SEC strengthened its program since the OIG’s last FISMA audit, Kearney noted that the agency’s information security program did not meet the *FY 2018 IG FISMA Reporting Metrics*’ definition of “effective.” As shown in the table below, we determined that the SEC’s maturity level for the five Cybersecurity Framework Functions was Level 2: *Defined*. None of the functions reached Level 4: *Managed and Measurable*, which the *FY 2018 IG FISMA Reporting Metrics* identified as the level reflective of an effective information security program.

***SEC’s Information Security Program Maturity***

NIST Cybersecurity Framework Function	<i>FY 2018 IG FISMA Metric</i>	Security Control Maturity
Identify	Risk Management	<i>Level 2: Defined</i>
Protect	Configuration Management	<i>Level 2: Defined</i>
	Identity and Access Management	<i>Level 2: Defined</i>
	Data Protection and Privacy	<i>Level 3: Consistently Implemented</i>
	Security Training	<i>Level 2: Defined</i>
Detect	Information Security Continuous Monitoring	<i>Level 2: Defined</i>
Respond	Incident Response	<i>Level 2: Defined</i>
Recover	Contingency Planning	<i>Level 2: Defined</i>

Our report includes 11 new recommendations to strengthen the SEC’s information security program. As our report highlights, opportunities exist for the SEC to improve its performance in all eight IG FISMA metric areas. Significant opportunities for improvement remain in key areas such as improving its comprehensive risk management strategy, improving hardware and (b) (7)(E) management, enhancing configuration management activities, improving the (b) (7)(E), strengthening incident response practices, and (b) (7)(E). Acting on these opportunities for improvement will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC’s sensitive, non-public information, as well as assist the SEC’s information security program reach the next maturity level.



In closing, we appreciate the courtesies extended to the Kearney Evaluation Team by the SEC during this engagement.

Sincerely,

A handwritten signature in blue ink that reads "Kearney &amp; Company". The signature is written in a cursive, flowing style.

Kearney & Company, P.C.  
December 14, 2018

**TABLE OF CONTENTS**

	<b><u>Page #</u></b>
<b>COVER LETTER.....</b>	<b>i</b>
<b>BACKGROUND AND OBJECTIVES .....</b>	<b>1</b>
<b>Background .....</b>	<b>1</b>
<b>Objectives.....</b>	<b>4</b>
<b>RESULTS .....</b>	<b>5</b>
<b>Domain #1: Risk Management .....</b>	<b>5</b>
<b>Domain #2: Configuration Management.....</b>	<b>7</b>
<b>Domain #3: Identity and Access Management.....</b>	<b>11</b>
<b>Domain #4: Data Protection and Privacy .....</b>	<b>13</b>
<b>Domain #5: Security Training .....</b>	<b>16</b>
<b>Domain #6: Information Security Continuous Monitoring (ISCM).....</b>	<b>20</b>
<b>Domain #7: Incident Response .....</b>	<b>25</b>
<b>Domain #8: Contingency Planning.....</b>	<b>28</b>
<b>OVERALL CONCLUSION.....</b>	<b>31</b>
<b>OTHER MATTERS OF INTEREST .....</b>	<b>32</b>
<b>Appendix I: Scope and Methodology .....</b>	<b>34</b>
<b>Appendix II: Open FISMA Recommendations.....</b>	<b>39</b>
<b>Appendix III: Management Comments .....</b>	<b>43</b>



**TABLE OF EXHIBITS**

	<b><u>Page #</u></b>
Exhibit 1: Cybersecurity Framework Functions Mapped to FY 2018 IG FISMA Reporting Metrics Assessment Domains .....	2
Exhibit 2: IG Assessment Maturity Levels .....	2
Exhibit 3: Security-Focused Configuration Management Phases .....	7
Exhibit 4: Timeliness of Incident Reporting to US-CERT .....	26
Exhibit 5: SEC Systems Sampled .....	35
Exhibit 6: Open FISMA Recommendations .....	39

**ABBREVIATIONS**

ATO	Authorization-to-Operate
BIA	Business Impact Analysis
CIO	Chief Information Officer
DHS	U.S. Department of Homeland Security
EDRP	Enterprise Disaster Recovery Plan
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
(b) (7) (E)	(b) (7)(E)
HVA	High Value Asset
(b) (7) (E)	(b) (7)(E)
IG	Inspector General
(b) (7) (E)	(b) (7)(E)
(b) (7) (E)	(b) (7)(E)
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
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
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

PISA	Privacy and Information Security Awareness
(b) (7) (E)	(b) (7)(E)
POA&M	Plan of Action and Milestones
PUB	Publication
Rev.	Revision
SEC or agency	U.S. Securities and Exchange Commission
(b) (7) (E)	(b) (7)(E)
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team

---

## BACKGROUND AND OBJECTIVES

---

### Background

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law [P.L.] 113-283), which amended the Federal Information Security Management Act of 2002 (FISMA-2002), Title III of the E-Government Act of 2002 (P.L. 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 (IG) to assess annually the effectiveness of information security programs and practices and to report the results to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). This assessment includes testing and assessing the effectiveness of information security policies, procedures, and practices, as well as a subset of information systems. In support of these requirements, DHS issued to IGs guidance on FISMA reporting for fiscal year (FY) 2018.<sup>1</sup>

To comply with FISMA, Kearney & Company, P.C. (referred to as “Kearney,” “we,” and “our”) assessed the U.S. Securities and Exchange Commission’s (referred to as “SEC” or “agency”) implementation of key security controls identified in the *FY 2018 IG FISMA Reporting Metrics*. The results of these efforts supported the Office of Inspector General’s (OIG) FY 2018 CyberScope submission to OMB and DHS.<sup>2</sup>

As *Exhibit 1* illustrates, the *FY 2018 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”).<sup>3</sup>

---

<sup>1</sup> *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.0.1 dated May 24, 2018 (hereafter referred to as “*FY 2018 IG FISMA Reporting Metrics*”).

<sup>2</sup> CyberScope is the platform that CIOs, Privacy Officers, and IGs use to meet FISMA reporting requirements. The SEC OIG completed its FY 2018 CyberScope submission to DHS and OMB on October 30, 2018.

<sup>3</sup> The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, as well as provides IGs with the guidance for assessing the maturity of controls to address those risks.

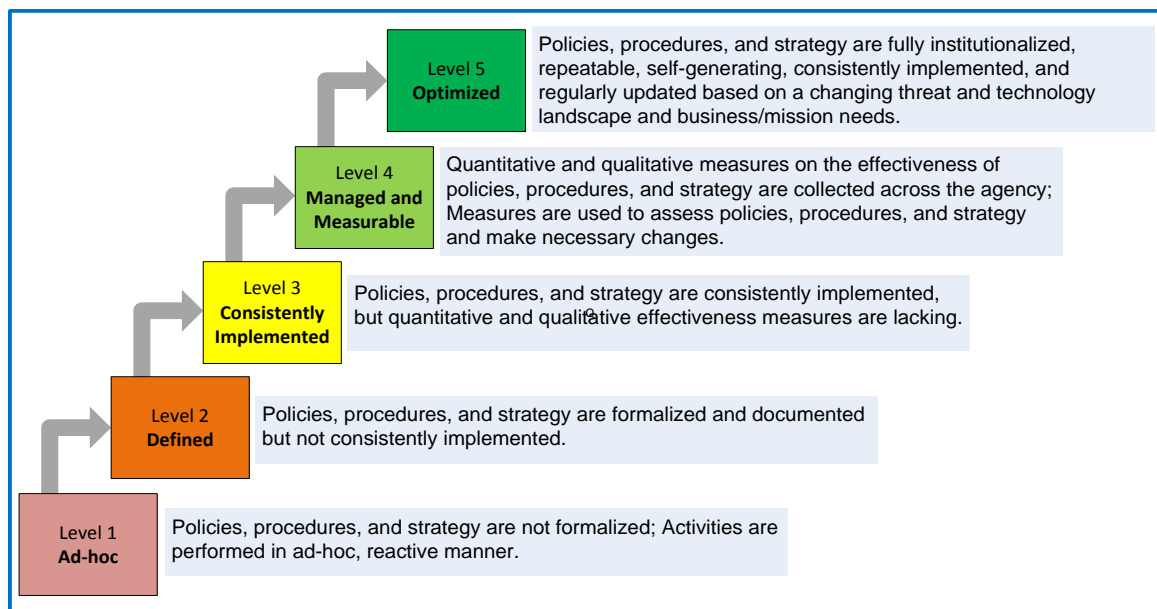
**Exhibit 1: Cybersecurity Framework Functions Mapped to FY 2018 IG FISMA Reporting Metrics Assessment Domains**

Cybersecurity Framework Functions	FY 2018 IG FISMA Reporting Metrics Assessment Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: Kearney-generated from FY 2018 IG FISMA Reporting Metrics.

**Change in Metrics and Assessment Methodology:** The FYs 2015 and 2016 IG FISMA Reporting Metrics required IGs to assess two Cybersecurity Framework functions (i.e., Detect and Respond) using a maturity model approach. In contrast, the FY 2017 IG FISMA Reporting Metrics required IGs to assess seven domains included in the five Cybersecurity Framework functions using a maturity model approach. In FY 2018, the IG FISMA Reporting Metrics expanded to include an eighth domain, Data Protection and Privacy. As shown in *Exhibit 2*, the foundation levels of the maturity model ensure that agencies develop sound policies and procedures, whereas the advanced levels capture the extent to which agencies institutionalize those policies and procedures (Level 3), establish performance measures (Level 4), and aim to improve and optimize performance against established goals (Level 5).

**Exhibit 2. IG Assessment Maturity Levels**



Source: Kearney-generated graphic based on the FY 2018 IG-FISMA reporting metrics

The maturity model also summarizes the status of agencies' information security programs, provides transparency on what has been accomplished and what still needs to be implemented to improve the information security program, and helps ensure consistency across the IGs in their

annual FISMA reviews. Within the context of the maturity model, Level 4: *Managed and Measurable* represents an effective level of security at the domain, function, and overall program levels.

**Responsible Office:** The SEC's Office of Information Technology (OIT) holds overall management responsibility for the SEC's information technology (IT) program, including information security. OIT establishes IT security policies and provides technical support, assistance, direction, and guidance to the SEC's divisions and offices. The Chief Information Officer (CIO) directs OIT and is responsible for ensuring compliance with applicable information security requirements. The Chief Information Security Officer, designated by the CIO, is responsible, in part, for developing, maintaining, centralizing, and monitoring ongoing adherence to the SEC's Information Security Program Plan and supporting the CIO in annually reporting on the effectiveness of the SEC's information security program.

**Prior Audits and Evaluations:** Prior to the start of the FY 2018 FISMA evaluation, the SEC closed 19 of 21 recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2016<sup>4</sup> (FY 2016 FISMA audit). The SEC also closed 1 of 20 recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2017<sup>5</sup> (FY 2017 FISMA audit), dated March 30, 2018. In coordination with the OIG, Kearney proposed closure of one further open recommendation from the FY 2017 FISMA audit as a result of improvements to the risk management program. Among actions taken, OIT made progress by enhancing information security policies and procedures to address security risks at the organizational and information system levels, strengthening authentication mechanisms, reducing the number of critical vulnerabilities, enhancing its security awareness and training processes, and continuing its efforts to improve its continuous monitoring program. The OIG will close the remaining recommendations upon completion and verification of corrective actions taken.

---

<sup>4</sup> 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 2016*, Report No. 539; March 7, 2017 (hereafter referred to as "FY 2016 FISMA audit").

<sup>5</sup> 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 2017*, Report No. 546; March 30, 2018 (hereafter referred to as "FY 2017 FISMA audit").

## Objectives

Our overall objective was to evaluate the SEC's implementation of FISMA for FY 2018 based on guidance issued by OMB, DHS, and NIST. Specifically, as discussed in the **Results** section of this report, we assessed the effectiveness of the SEC's information security program for the following eight domains in accordance with the *FY 2018 IG FISMA Reporting Metrics*:

- Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning.

To assess the effectiveness and maturity of security controls identified in the *FY 2018 IG FISMA Reporting Metrics*, Kearney judgmentally selected and reviewed a non-statistical sample of eight information systems from the SEC's May 10, 2018 inventory of 86 FISMA-reportable information systems (or about 9 percent).<sup>6</sup> We also performed other tests and assessments. [Appendix I: Scope and Methodology](#) describes our scope and methodology (including sampled systems), our review of internal controls and computer-processed data, and prior coverage.

---

<sup>6</sup> Per OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 2016, a major information system is a "system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources."

---

## RESULTS

---

### Domain #1: Risk Management

Risk management is the ongoing process of identifying, assessing, and responding to risk. 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*, March 2011, states that in order 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).

Kearney assessed the SEC's risk management program and determined that the program's maturity level is Level 2: *Defined*, meaning the SEC formalized and documented risk management policies and procedures but did not consistently implement them.

Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Institutionalize and mature its enterprise architecture program by defining or formalizing a plan to address how the SEC's enterprise architecture program management will be integrated with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control
- Develop or maintain an accurate or complete inventory of hardware assets connected to the SEC's network or (b) (7)(E)
- Always ensure that IT contracts include certain contracting language defined by OIT.

Similarly, Kearney determined that many of the weaknesses with the SEC's risk management program identified during the FY 2017 FISMA audit remained present in FY 2018, as listed below:

- The SEC did not describe how the information security architecture is integrated into and supports the organization's enterprise architecture, including institutional management disciplines, such as organizational strategic planning, strategic human capital management, and performance management
- Opportunities exist for the SEC to improve the accuracy and completeness of its hardware inventory. For example, the SEC's hardware inventory system of record contained hardware assets assigned to 25 of 681 separated individuals (or about 4 percent) as of June 10, 2018. All 25 of the separated individuals with assigned hardware assets were contractor personnel. In addition, opportunities exist to improve the completeness of the SEC's assets, as a random sample of 45 of 8,802 computers tracked in the SEC's software patching tool revealed that 2 of 45 (4 percent) sampled computers were not found in the SEC's hardware inventory system



- The SEC's software inventory did not have an automated solution to maintain software licenses
- The SEC did not update all three sampled IT contracts to ensure appropriate security clauses were included, as of the close of fieldwork.

These control weaknesses occurred for a variety of different reasons. The SEC's enterprise architecture team relied on shared resources and was unable to complete remediation activities in FY 2018. Subsequently, OIT obtained funding for five contract resources fully dedicated to enterprise architecture. Specific to weaknesses regarding discrepancies with hardware and (b) (7)(E) records, these differences occurred because the SEC relied on manual, rather than automated, processes<sup>7</sup> to review hardware and (b) (7)(E) for completeness and accuracy. In addition, the SEC stated that it has implemented a new initiative to review a backlog of IT contracts and is attempting to update contractual language upon the exercise of option years.

Kearney is not making any new recommendations in relation to the prior year findings noted above, as the SEC is working to address the prior year FISMA recommendations. See Appendix II: Open FISMA Recommendations. Additionally, see Other Matters of Interest regarding additional opportunities for SEC management to improve its risk management program.

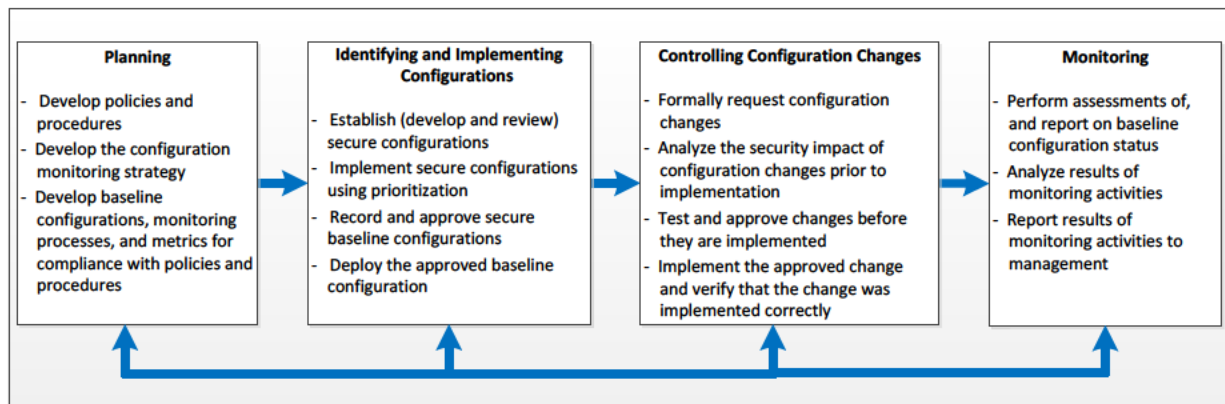
---

<sup>7</sup> (b) (7)(E)

## Domain #2: Configuration Management

According to NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011, configuration management is an important process for establishing and maintaining secure information system configurations, in addition to providing important support for managing security risks in information systems. Configuration management activities include developing baseline configurations,<sup>8</sup> establishing a configuration change control process, and implementing a configuration monitoring and reporting process. NIST SP 800-53, Revision (Rev.) 4, (CM-2), *Baseline Configuration*, requires that organizations develop, document, and maintain, under configuration control, a current baseline configuration of information systems. The approved baseline configuration for an information system and associated components represents the most secure state consistent with operational requirements and constraints. In addition, as described in *Exhibit 3*, security-focused configuration management of information systems involves a set of activities that can be organized into the following four major phases: 1) Planning; 2) Identifying and Implementing Configurations; 3) Controlling Configuration Changes; and 4) Monitoring.

*Exhibit 3: Security-Focused Configuration Management Phases*



Source: OIG-generated based on NIST SP 800-128.

Kearney assessed the SEC's configuration management program and determined that the program's maturity level is Level 2: *Defined*, meaning the SEC formalized and documented configuration management policies and procedures but did not consistently implement them.

<sup>8</sup> NIST SP 800-128 defines a baseline configuration as a set of specifications for a system or part of a system that has been formally reviewed and agreed on at a given point in time and which can be updated only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Fully (b) (7)(E) or review and update system security plans (SSP) (b) (7)(E) at least annually or within established schedules
- Adequately implement (b) (7)(E)

Similarly, Kearney determined that many of the weaknesses with the SEC's configuration management practices identified during the FY 2017 FISMA audit remained present in FY 2018, as listed below:

- Although the SEC deployed a new version of a sampled system to the production environment in (b) (7)(E), the agency did not establish a (b) (7)(E)
- The SEC did not configure and execute (b) (7)(E)
- Although the SEC reduced its number of critical vulnerabilities, the agency did not consistently follow its vulnerability management policy, which requires the remediation of (b) (7)(E).

The above weaknesses occurred because SEC management had not fully addressed management challenges identified in FY 2017. During FY 2018, the SEC took steps to address previously noted weaknesses by improving its reporting, analysis, and metrics related to vulnerability management. Identified issues related to (b) (7)(E) vulnerabilities occurred, in part, because the SEC (b) (7)(E)

Overall, weaknesses with the SEC's vulnerability remediation process continued in FY 2018 because the agency did not include an effective oversight function to monitor vulnerability identification and flaw remediation processes and practices.

Kearney is not making any new recommendations in relation to the prior year findings noted above, as the SEC is working to address the prior year FISMA recommendations. See Appendix II: Open FISMA Recommendations.

In addition to the prior year findings, Kearney identified (b) (7)(E)

(b) (7)(E). The SEC's (b) (7)(E) states that OIT shall develop a continuous monitoring strategy, including establishing approved baseline configurations for each environment, as well as develop, document, and maintain, under configuration control, a current baseline configuration for SEC information systems and constituent components. Further, the SEC's (b) (7)(E) states that OIT shall review and update baseline configurations (documented in SSPs) at least annually. Furthermore, NIST SP 800-53, Rev. 4, (CM-3 (f)), *Configuration Change Control*, states that organizations should audit and review activities associated with configuration-controlled changes to the information system.

(b) (7)(E). As of July 2018, the SEC's configuration change control process (b) (7)(E)

(b) (7)(E). Without up-to-date (b) (7)(E), the SEC's ability to (b) (7)(E) is reduced. According to OIT management, this condition occurred because limited individuals had the knowledge and skills to more frequently update the (b) (7)(E).

(b) (7)(E). OIT did not define and implement (b) (7)(E)

This condition occurred because OIT relied upon preventative controls, such as access controls and separation of duties, rather than a detective control, as it did not perceive a detective control to be valuable. Additionally, OIT management reported to Kearney that they requested an additional Federal employee and contractor to fill the

<sup>9</sup> (b) (7)(E)

resource gap in the configuration management area; however, senior management denied the request, citing budget constraints.

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

To mature the SEC's configuration management program from Level 2: *Defined* to Level 3: *Consistently Implemented*, Kearney recommends that the Office of Information Technology continue to work and close prior year recommendations. See Appendix II: Open FISMA Recommendations.

Additionally, Kearney recommends that the SEC's Office of Information Technology:

**Recommendation 1:** Update configuration management procedures to require that (b) (7)(E) (b) (7)(E) are approved.

**Management's Response.** The Office of Information Technology concurs it is important to (b) (7)(E) (b) (7)(E) are approved. Pursuant to this recommendation, the Office of Information Technology will update configuration management procedures to (b) (7)(E) (b) (7)(E) are approved.

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

**Recommendation 2:** Update configuration management procedures to require (b) (7)(E) (b) (7)(E)

**Management's Response.** The Office of Information Technology concurs it is important to (b) (7)(E) (b) (7)(E) Pursuant to this recommendation, the Office of Information Technology will update configuration management procedures to (b) (7)(E) (b) (7)(E)

**Kearney's Evaluation of OIT'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: Identity and Access Management

NIST SP 800-53, Rev. 4, (AC-1), *Access Control Policy and Procedures*, and (IA-1), *Identification and Authentication Policy and Procedures*, requires organizations to develop, document, and disseminate an access control policy and an identification and authentication policy that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. 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 users before granting access to SEC information and information systems. The continued development of a strong identity and access management program may decrease the risk of unauthorized access to the SEC's network, information systems, and data.

Kearney assessed the SEC's identity and access management program and determined that the program's maturity level is Level 2: *Defined*, meaning the SEC formalized and documented identity and access management policies and procedures but did not consistently implement them.

Specifically, in the FY 2017 FISMA audit, the OIG identified that the SEC did not:

- Develop a transition plan to include milestones and priorities for aligning its identity, credential, and access management strategy with Federal initiatives
- (b) (7)(E)
- Define processes for ensuring compliance with (b) (7)(E).

Similarly, Kearney determined that many of the weaknesses with the SEC's identity and access management practices identified during the FY 2017 FISMA audit remained present in FY 2018, as listed below:

- The SEC did not document a strategy to align its identity and access management program with the Federal Identity, Credential, and Access Management initiatives
- (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

- The SEC did not enhance access controls for (b) (7)(E) through the formal documentation of its provisioning and review process
- The SEC did not document a process for (b) (7)(E)
- (b) (7)(E)

These control weaknesses occurred for a variety of reasons. Regarding the documentation of a strategy to align with Federal Identity, Credential, and Access Management initiatives, OIT management stated that the SEC was in the process of documenting a strategy, but it was not completed by the end of our fieldwork. Regarding the deployment of (b) (7)(E) for authentication, SEC management explained that the SEC was under the (b) (7)(E) for several reasons, which are formally detailed in a (b) (7)(E) document. (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Lastly, regarding the use of (b) (7)(E), the SEC's team acknowledged that it was an oversight and took immediate corrective action.

Kearney is not making any new recommendations in relation to the prior year findings noted above, as the SEC is working to address the prior year FISMA recommendations. See Appendix II: Open FISMA Recommendations. Additionally, see Other Matters of Interest regarding additional opportunities for SEC management to improve its identity and access management program.

<sup>10</sup> (b) (7)(E)

<sup>11</sup> (b) (7)(E)



## Domain #4: Data Protection and Privacy

In pursuit of its mission to protect public investors, the SEC collects sensitive, non-public information that may include personally identifiable information (PII). The collection of sensitive PII, such as Social Security numbers and possibly brokerage account numbers, requires the SEC to take additional precautions to prevent accidental disclosure, such as encrypting sensitive data at rest, as well as in transit. The collection of sensitive PII also requires the SEC to notify the public of why information is collected, its intended use, with whom it will be shared, and how the information will be protected. In light of recent and successful attacks by hackers against both Federal and commercial entities that resulted in the disclosures of sensitive PII, organizations have placed increased attention on protecting sensitive information by limiting its collection, encrypting the data at rest, and monitoring for potential exfiltration of sensitive data.

Data Protection and Privacy is a new domain within the NIST Cybersecurity "Protect" function for the *FY 2018 IG FISMA Reporting Metrics*. Kearney assessed the SEC's data protection and privacy program and determined that the program's maturity level is Level 3: *Consistently Implemented*, meaning the SEC formalized and consistently implemented privacy policies and procedures for data protection and privacy, but quantitative and qualitative effectiveness measures were lacking.

Kearney identified three opportunities for improvement associated with the SEC's data protection and privacy procedures and practices. Specifically, we found limitations in (b) (7)(E) (b) (7)(E), and outdated procedures for (b) (7)(E) (b) (7)(E).

### Data Protection and Privacy Procedures and Practices Need Improvement. (b) (7)(E)

(b) (7)(E)

(b) (7)(E) . The SEC did not fully implement security controls to (b) (7)(E) (b) (7)(E).

(b) (7)(E) [REDACTED]

At the conclusion of the FISMA evaluation in September 2018, the SEC reported that it planned to (b) (7)(E) [REDACTED].

(b) (7)(E) [REDACTED]. The SEC did not implement security controls to protect (b) (7)(E) [REDACTED].

(b) (7)(E) [REDACTED]

*Outdated Procedures for* (b) (7)(E) [REDACTED]. The SEC did not update procedures for the (b) (7)(E) [REDACTED].

According to the Q2 CIO metrics, the CIO self-identified that (b) (7)(E) [REDACTED] procedures were out of date and that the SEC planned to update the procedures during 2018. However, during our evaluation, the SEC was unable to provide updated procedures for Kearney to review.

See Other Matters of Interest regarding additional opportunities for SEC management to improve its data protection and privacy program.

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

To mature the SEC's data protection and privacy program from Level 3: *Consistently Implemented* to Level 4: *Managed and Measurable*, Kearney recommends that the SEC's Office of Information Technology:

**Recommendation 3:** Complete initiatives to implement (b) (7)(E) [REDACTED]

**Management's Response.** The Office of Information Technology concurs and, pursuant to this recommendation, will complete its initiatives to implement (b) (7)(E) [REDACTED]

(b) (7)(E)

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

**Recommendation 4:** Complete initiatives to implement (b) (7)(E)

**Management's Response.** The Office of Information Technology concurs. During FY 2018, SEC staff began executing a strategy to (b) (7)(E) and, pursuant to this recommendation, the Office of Information Technology will review and update the project plan and continue its implementation of (b) (7)(E)

**Kearney's Evaluation of OIT'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:** Update procedures for the (b) (7)(E)

**Management's Response.** The Office of Information Technology concurs. Pursuant to this recommendation, the Office of Information Technology will update existing procedures for the (b) (7)(E)

**Kearney's Evaluation of OIT'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 Training

The *FY 2018 IG FISMA Reporting Metrics* require agencies to establish an information security program that includes security awareness training. Such training informs personnel, including contractors, of information security risks associated with their activities, as well as their responsibilities for complying with agency policies and procedures. NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, provides guidance on a superset of cybersecurity knowledge, skills, and abilities and tasks for each work role. The NICE Cybersecurity Workforce Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development. NIST SP 800-53, Rev. 4, (PS-6), *Access Agreements*, further requires the organization to develop and document access agreements for individuals, ensure individuals sign appropriate access agreements prior to being granted access, and individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or on an organization-defined frequency. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, mandates that organizations monitor their information security training program for compliance and effectiveness and that failure to encourage IT security training puts an enterprise at greater risk because the security of agency resources is as much a human issue as it is a technology issue. Lastly, NIST SP 800-53, Rev. 4, (AT-3), *Security Training*, requires that Federal agencies provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access or performing assigned duties.

Kearney assessed the SEC's security training program and determined that the program's maturity level is Level 2: *Defined*, meaning the SEC formalized and documented security training policies and procedures but did not consistently implement them.

Specifically, in the FY 2016 and 2017 FISMA audits, the OIG determined that the SEC did not:

- Fully implement 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
- Ensure that users requiring access to SEC information and information systems signed appropriate access agreements and participated in required training before gaining access
- Document a process to ensure that SEC employees receive privacy and information security awareness training annually (every 12 months)
- Ensure that individuals with significant security responsibilities received specialized security training before accessing SEC information systems or performing assigned duties.

Similarly, Kearney determined that many of the weaknesses with the SEC's security training practices identified during the FY 2016 and FY 2017 FISMA audits remained present in the FY 2018 evaluation, as listed below:

- The SEC's Office of Human Resources did not document its process for assessing knowledge, skills, and abilities of the cybersecurity workforce
- The SEC did not ensure that new employees signed access agreements prior to gaining system access. All five randomly sampled new employees did not sign their access agreement, known as (b) (7)(E), prior to accessing the SEC network
- The SEC did not follow its documented process for assigning training to SEC employees and failed to document its new process
- The SEC did not document or consistently implement a process for assigning specialized training to privileged users prior to granting them privileged system access. Specifically, the SEC did not assign specialized security training (authorization-to-operate [ATO] training and privileged user role-based training) to the appropriate employees through the SEC learning management tool. For 5 of 7 FY 2018 sampled FISMA systems (or about 71 percent), the SEC did not assign privileged user role-based training to 36 of 62 privileged users (or about 58 percent) and did not assign ATO training to 10 of 14 users with significant security responsibilities (or about 71 percent). As the SEC did not assign these privileged users training through the learning management tool, these employees did not complete the specialized training prior to obtaining system access or performing security responsibilities.

Kearney identified multiple reasons for the above control weaknesses. While the SEC distributed an assessment of cybersecurity certifications,<sup>12</sup> it did not develop a corresponding procedure. Regarding the inability to complete access agreements prior to gaining system access, OIT stated that the Office of Human Resources was leading an effort to implement a major system modification to facilitate requiring personnel to sign applicable access agreements prior to obtaining system access. Regarding the lack of a documented training assignment process, the Office of Human Resources documented a solution to assign awareness training to employees every 270 days; later, it realized this process was challenging to implement and, therefore, assigned training to incoming employees in an ad hoc manner, but failed to document the new process. Lastly, regarding specialized security training, OIT and the Office of Human Resources have not documented a process for identifying each user with significant security responsibilities; therefore, the Office of Human Resources could not identify personnel to whom to assign specialized security training.

Kearney is not making any new recommendations in relation to the prior year findings noted above, as the SEC is working to address the prior year FISMA recommendations. See [Appendix II: Open FISMA Recommendations](#).

---

<sup>12</sup> Examples of these cybersecurity certifications include the Certified Information Systems Security Professional (CISSP), Security+, Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), and Certified Information Security Manager (CISM).

In addition to the prior year findings, Kearney identified a new weakness regarding data integrity within the learning management system. Specifically, the learning management tool did not consistently track all personnel within the system.

**Data Integrity Issue within Learning Management System.** According to NIST SP 800-53, Rev. 4, (AT-2), *Security Awareness*, organizations must provide basic security awareness training to information system users (including managers, senior executives, and contractors): a) as part of initial training for users; b) when required by information system changes; and c) an agency-defined frequency thereafter. In FY 2018, the SEC implemented new functionality to automate the training and tracking of SEC personnel through dashboards within the centralized learning management tool. According to the learning management tool's dashboard, 99 percent of SEC personnel completed the privacy and information security awareness (PISA) training for FY 2018. However, Kearney identified the following weakness regarding data integrity within the learning management tool.

*Opportunities Exist to Improve Tracking of Contractor Personnel within Learning Management System.* The SEC's learning management system did not consistently track all contractor personnel and their completion of PISA training. Upon review of the learning management tool's PISA dashboard report, Kearney observed that the tool did not track 6 of 376 contractor personnel (or about 2 percent), who were onboarded between October 1, 2017 and May 31, 2018, with active network accounts.

Without a control in place to ensure that all contractor personnel are assigned training and tracked within the learning management tool, some contractor personnel may not receive PISA training. Further, the omission of contractor personnel in the learning management system leads to inaccurate reporting of training completion.

This condition occurred, in part, because the Contracting Officer's Representative must manually input contractor personnel information into a contractor database, which is used to feed new contractor personnel to the learning management system. In addition, the SEC did not have a control to detect instances where contractor personnel received network accounts, but were not assigned PISA training.

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

To mature the SEC's security training program from Level 2: *Defined* to Level 3: *Consistently Implemented*, Kearney recommends that the Office of Information Technology continue to work and close prior year recommendations. See [Appendix II: Open FISMA Recommendations](#).

Additionally, Kearney recommends that the Office of Human Resources and Office of Information Technology:

**Recommendation 6:** Define and implement a control to detect instances where contractor personnel received network accounts but were not assigned privacy and information security awareness training, nor tracked within system reporting tools.

**Management's Response.** The Office of Information Technology concurs. During early FY 2019, SEC staff completed an enhancement to the agency's learning management system and updated internal protocols to facilitate the issuance of required privacy and security awareness training for personnel before they receive system credentials. This will also ensure that the training status for new staff are tracked within the agency's learning management system. Pursuant to this recommendation, the SEC will define and implement controls to track and detect instances where contractors receive system credentials prior to completing privacy and information security awareness training.

**Kearney'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)**

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An effective ISCM program results in ongoing updates to the organization's security plans, security assessment reports, and Plans of Action and Milestones (POA&M), which are the three principal documents in a system's security authorization package. According to NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, organizations should take steps to establish, implement, and maintain an ISCM program, including defining an ISCM strategy, analyzing and reporting findings, and reviewing and updating the ISCM strategy and program, as necessary. In addition, OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 2013, states that agencies were required to implement continuous monitoring of security controls as part of a phased approach through FY 2017.<sup>13</sup>

Kearney assessed the SEC's ISCM program and determined that the program's maturity level was Level 2: *Defined*, meaning the SEC formalized and documented ISCM policies and procedures but did not consistently implement them.

Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Document a comprehensive ISCM strategy and did not establish procedures for reviewing and modifying all aspects of the ISCM strategy
- Perform ongoing authorizations of its information systems and the environments in which they operate.

Similarly, Kearney determined that many of the weaknesses with the SEC's ISCM practices identified during the FY 2017 FISMA audit remained present in the FY 2018 FISMA evaluation, as listed below:

- ISCM strategy did not define how ISCM activities support risk management in accordance with organizational risk tolerance, nor the criteria for how the SEC plans to assess, respond to, and monitor risk, as well as the oversight required to ensure that the risk management strategy is effective in accordance with NIST
- The SEC did not have specific procedures for reviewing and modifying all aspects of the ISCM strategy
- Seven of 86 SEC systems (or about 8 percent) operated with an expired ATO as of September 19, 2018.

---

<sup>13</sup> OMB Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 2018, supersedes OMB M-14-03 and expands upon prior continuous monitoring requirements.

These control weaknesses occurred, in part, because the ISCM processes did not include review procedures for modifying all aspects of the ISCM strategy. Additionally, according to OIT, it implemented a rigorous POA&M closure process, which requires a critical analysis of closure requests performed by an independent team prior to closing a particular POA&M. OIT asserts it is currently aware of and tracking all expired ATOs through monthly meetings. Overall, the above weaknesses occurred, in part, because the current ISCM processes did not include an effective oversight function to review ISCM strategy, procedures, and the ongoing authorization processes.

Kearney is not making any new recommendations in relation to the prior year findings noted above, as the SEC is working to address the prior year FISMA recommendations. See Appendix II: Open FISMA Recommendations.

In addition to the prior year findings, Kearney identified a new weakness associated with (b) (7)(E). Specifically, the SEC did not consistently perform

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

---

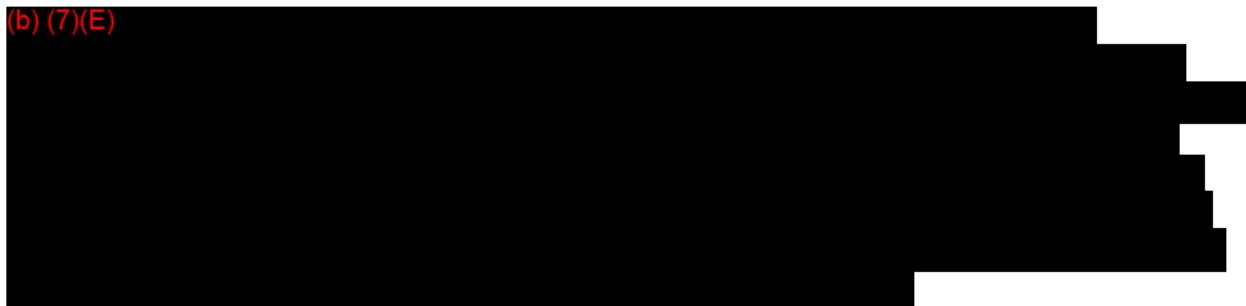
<sup>14</sup> (b) (7)(E)

<sup>15</sup> (b) (7)(E)

(b) (7)(E)

A large rectangular area of the document is completely redacted with a solid black fill. The text "(b) (7)(E)" is printed in red at the top left corner of this redacted area.

(b) (7)(E)

A large rectangular area of the document is completely redacted with a solid black fill. The text "(b) (7)(E)" is printed in red at the top left corner of this redacted area.

(b) (7)(E)

A large rectangular area of the document is completely redacted with a solid black fill. The text "(b) (7)(E)" is printed in red at the top left corner of this redacted area. Two small white vertical bars are visible within the redacted area, possibly representing a table or list structure.

(b) (7)(E)

A large rectangular area of the document is completely redacted with a solid black fill. The text "(b) (7)(E)" is printed in red at the top left corner of this redacted area.

---

<sup>16</sup> (b) (7)(E)

A single line of text is redacted with a solid black fill. The text "<sup>16</sup> (b) (7)(E)" is printed in red at the beginning of this line.

(b) (7)(E)

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

To mature the SEC's ISCM program from Level 2: *Defined* to Level 3: *Consistently Implemented*, Kearney recommends that the Office of Information Technology continue to work and close prior year recommendations. See [Appendix II: Open FISMA Recommendations](#).

Additionally, Kearney recommends that the Office of Information Technology:

**Recommendation 7:** (b) (7)(E)

. Additionally, Office of Information Technology should develop procedures that (b) (7)(E)

. Accordingly, Office of Information Technology should update policies and procedures to (b) (7)(E)

**Management's Response.** The Office of Information Technology concurs that it is important to (b) (7)(E)

Pursuant to this recommendation, the Office of Information Technology will also develop procedures to (b) (7)(E)

. Additionally, the Office of Information Technology will work to (b) (7)(E)

**Kearney's Evaluation of OIT'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:** (b) (7)(E)

**Management's Response.** The Office of Information Technology concurs. Pursuant to this recommendation, the Office of Information Technology will take steps to (b) (7)(E)

**Kearney's Evaluation of OIT'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:** Establish a process to improve coordination and communication among the various Office of Information Technology teams (b) (7)(E)

**Management's Response.** The Office of Information Technology concurs. Pursuant to this recommendation, the Office of Information Technology will (b) (7)(E)

**Kearney's Evaluation of OIT'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 an organization-wide information security program that includes procedures for detecting, reporting, and responding to security incidents, including mitigating the risks of such incidents before substantial damage occurs. According to NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*, August 2012, key phases in the incident response process are: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

Kearney assessed the SEC's incident response program and determined that the program's maturity level is Level 2: *Defined*, meaning the SEC formalized and documented incident response policies and procedures but did not consistently implement them.

As the OIG reported in its report entitled (b) (7)(E)

(b) (7)(E). Several weaknesses with the SEC's incident response practices, identified in the OIG's Report No. (b) (7)(E) and the FY 2017 FISMA audit, remained present in FY 2018 regarding incomplete incident response plans, (b) (7)(E), and untimely reporting of security incidents to United States Computer Emergency Readiness Team (US-CERT).

Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Maintain up-to-date and comprehensive incident response plans, policies, procedures, and strategies
- Fully and consistently implement incident detection and analysis processes and technologies
- Timely report incidents to the US-CERT.

Similarly, Kearney determined many of the weaknesses with the SEC's incident response practices identified during the OIG's Report No. (b) (7)(E) and the FY 2017 FISMA audit remained present in the FY 2018 FISMA evaluation, as listed below:

- The SEC has defined its plan, policies, procedures, and strategies for responding to incidents; however, the SEC did not consistently maintain and execute its incident response policies and procedures. Kearney reviewed the SEC's incident response plan, policies, procedures, and strategies and determined that the SEC did not identify and define performance metrics that will be used to measure and track the effectiveness of its incident response program. The incident management plan mentioned training at a high level and did not detail the type of training or frequency of training requirements for incident response personnel. In addition, the incident management plan did not define a formalized process for consistently capturing lessons learned. For example, all seven

sampled incident response tickets failed to include any evidence of lessons learned documentation within the section

- The SEC has defined the incident detection, prevention, and analysis technologies leveraged for incident response activities; however, the SEC did not always (b) (7)(E)



- According to policy, the SEC is required to report incidents to US-CERT within one hour of identification; however, according to records from the (b) (7)(E) the SEC failed to timely report 143 of 434 incidents (or about 33 percent) to US-CERT within one hour. In 26 of 143 cases, the (b) (7)(E) did not report the incidents to US-CERT for more than five days. See *Exhibit 4* below for a breakdown of the SEC's timeliness of incident reporting to US-CERT.

*Exhibit 4: Timeliness of Incident Reporting to US-CERT*


Timeframe Reported to US-CERT	Number of Incidents	Total Number of Incidents
<b>Reported within 1 hour (compliant)</b>		<b>288 (66%)</b>
1-24 hours	101	
1-5 days	16	
5+ days	26	
<b>Reported after 1 hour (non-compliant)</b>		<b>143 (33%)</b>
<b>Other Circumstances</b>		<b>3 (1%)</b>
<b>Total FY 2018 Incidents</b>		<b>434 (100%)</b>

Source: Kearney analysis of (b) (7)(E)-reported incidents between October 1, 2017 and June 30, 2018





These weaknesses related to incident response continued to exist during FY 2018, as, according to the SEC (b) (7)(E) organizational charts, the (b) (7)(E) organization was short-staffed during FY 2018, with seven vacant positions as of June 26, 2018. Kearney concluded that these vacancies in the (b) (7)(E) contributed to the decreased performance of the team, lack of documented performance metrics and post-incident activity processes (i.e., lessons learned), the prolonged timeframes to resolve technical challenges with (b) (7)(E), and the untimely communication of incidents to US-CERT. OIT reported to Kearney that it has an ongoing project to (b) (7)(E)



Kearney is not making any new recommendations in relation to the prior year findings noted above, as the SEC is working to address the prior year FISMA recommendations. See Appendix II: Open FISMA Recommendations.

## Domain #8: Contingency Planning

FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems supporting the operations and assets of the organization. Because information system resources are essential to an organization's success, it is critical that systems are able to operate effectively without excessive interruption. Business Impact Analyses (BIA) help organizations identify and prioritize information systems and components critical to supporting the organization's operations. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and efficiently as possible following a disaster. NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, states that contingency planning activities include developing the planning policy, creating contingency strategies, maintaining contingency plans, conducting BIAs, testing contingency plans, and conducting exercises. In addition, NIST SP 800-53, Rev. 4, (CP-4), *Contingency Plan Testing and Exercises*, requires organizations to perform periodic testing of contingency plans to determine effectiveness and organizational readiness.

Kearney assessed the SEC's contingency planning program and determined that the program's maturity level is Level 2: *Defined*, meaning the SEC defined its contingency planning policies and procedures but did not consistently implement them.

Kearney identified a new control weakness related to inconsistent updates and testing of contingency planning documentation. Specifically, the SEC did not consistently update and maintain contingency planning documentation, which includes the Enterprise Disaster Recovery Plan (EDRP), Information System Contingency Plans (ISCP), and BIAs. In addition, the SEC did not perform an annual test of its EDRP in FY 2018.

**Inconsistent Update and Testing of Contingency Planning Documentation.** According to the SEC's (b) (7)(E), the agency should update and test its ISCPs and EDRP on an annual basis. The SEC has established a business continuity and disaster recovery policy that provides the authority and guidance necessary to reduce the impact of a disaster. The SEC has also dedicated teams toward specific areas of disaster recovery activities, including maintenance of contingency planning documents, such as BIAs and ISCPs. In addition, the SEC consistently implemented its strategies and technologies for information backup and storage, including the use of alternate storage and data replication services between its primary and alternate data centers. However, the SEC did not adequately perform all of its contingency planning activities during FY 2018.

*Inconsistent Updates to Contingency Planning Documentation.* The SEC did not consistently update and maintain its contingency planning documentation, which includes the EDRP, ISCPs, and BIAs. Specifically for the sampled systems, the SEC did not update the EDRP and three ISCPs in accordance with SEC policy. In addition, the SEC did not update the BIAs for two of the sampled systems. Without up-to-date contingency planning documentation, the SEC may be unable to efficiently and effectively respond to a disaster.

This condition occurred because of the SEC's data center migration effort required resources to be allocated to the data center migration instead of contingency planning and associated documentation updates.

*Failure to Test Enterprise Disaster Recovery Plan.* The SEC did not perform its annual test of the EDRP in FY 2018. Without annual testing of the EDRP, the SEC may be susceptible to an extended loss of system availability in an actual disaster, as personnel may be unfamiliar with their roles and responsibilities.

This condition also occurred because, rather than conducting a test of the EDRP, the SEC performed a data center migration during the audit period. SEC management documented a formal risk acceptance pertaining to the delayed testing of the EDRP in accordance with its policies and procedures. In addition, OIT reported that it has scheduled their FY 2019 disaster recovery test for (b) (7)(E) 2019.

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

To mature the SEC's contingency planning program from Level 2: *Defined* to Level 3: *Consistently Implemented*, Kearney recommends that the Office of Information Technology:

**Recommendation 10:** Update and maintain contingency planning documentation (i.e., Enterprise Disaster Recovery Plan, Business Impact Analyses, and Information System Contingency Plans) in accordance with SEC policies and procedures.

**Management's Response.** The Office of Information Technology concurs. The Office of Information Technology will update and maintain contingency planning documentation in accordance with SEC policies and procedures during FY 2019.

**Kearney'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:** Test the Enterprise Disaster Recovery Plan in accordance with SEC's policies and procedures for fiscal year 2019.

**Management's Response.** The Office of Information Technology concurs. The Office of Information Technology will test the Enterprise Disaster Recovery Plan in accordance with SEC's policies and procedures in fiscal year 2019. The Office of Information Technology notes that SEC staff completed a data center migration during FY 2018. This migration, which was completed in October 2018, has improved the agency's resiliency and addressed a number of recommendations issued by the OIG in its 2017 report on the agency's management of its data centers. Planning for our annual disaster recovery exercise is ongoing, and the exercise is scheduled for (b) (7)(E) FY 2019.

**Kearney'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.

## OVERALL CONCLUSION

---

Overall, the SEC improved aspects of its information security program. For example, since the FY 2017 FISMA audit, the SEC made progress in enhancing information security policies and procedures to address security risks at the organizational and information system levels, strengthening authentication mechanisms, reducing the number of critical vulnerabilities, enhancing security awareness and training processes, and continuing efforts to improve its continuous monitoring program. However, Kearney noted that the SEC's information security program did not meet the *FY 2018 IG FISMA Reporting Metrics*' definition of "effective" because the program's overall maturity did not reach Level 4: *Managed and Measurable*. Implementing Kearney's recommended corrective actions will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, non-public information; improve compliance with FISMA requirements; and assist the SEC's information security program reach the next maturity level.

**OTHER MATTERS OF INTEREST**

This section highlights opportunities for the SEC to strengthen its security and privacy controls that did not rise to the significance of a formal finding and are included for SEC management's consideration.

**Review FIPS PUB 199 Ratings Annually.** The SEC did not review FIPS PUB 199 ratings annually for all SEC information systems in order to re-affirm or revise the FIPS PUB 199 rating based on changes in data type or mission-essential functions.<sup>18</sup> During FY 2018, the SEC reported to DHS and OMB that its FISMA inventory included (b) (7)(E) HVAs, but it did not include the SEC's (b) (7)(E) in this count. Moreover, as discussed further below, the SEC did not apply the HVA Control Overlay<sup>19</sup> as requested by DHS and update the SSPs for one sampled system and (b) (7)(E).

Kearney encourages the SEC to annually review and update, if needed, the FIPS PUB 199 impact rating as part of the annual SSP review process for all SEC information systems.

**Consider Implementation of the HVA Control Overlay.** The SEC did not apply DHS's HVA Control Overlay and associated control enhancements to the (b) (7)(E) relying extensively on the (b) (7)(E)

(b) (7)(E). The SEC operates (b) (7)(E) HVAs, as defined by OMB and DHS. OMB Memorandum M-17-09, *Management of Federal High Value Assets*, December 2016, requires that Federal agencies identify and assess the security posture of their HVA systems. DHS's Office of Cybersecurity and Communications published the *HVA Control Overlay* in November 2017 to provide further technical guidance to Federal agencies for protecting HVAs and encourages Federal agencies to implement additional security controls above the NIST SP 800-53, Rev. 4, moderate baseline to their HVAs and (b) (7)(E). OIT informed Kearney that it intends to implement the security control enhancements associated with the HVA Control Overlay to the (b) (7)(E) in FY 2019.

Kearney encourages the SEC to consider implementing DHS's HVA Control Overlay and associated security control enhancements to all (b) (7)(E) HVAs and the (b) (7)(E) in FY 2019.

**Improve the Review and Update of SSP.** The SEC's (b) (7)(E) requires the SEC to prepare and annually update an information system's security plan and related security and privacy control descriptions in accordance with NIST SP 800-53, Rev 4. The SEC did not effectively review and update SSPs. Specifically, the SEC did not update one sampled system's SSP to reflect updates in security control practices within the past year. In addition, another

<sup>18</sup> See related discussion of HVA systems.

<sup>19</sup> The DHS HVA Control Overlay encourages Federal agencies to implement additional security controls and security control enhancements from NIST SP 800-53, Rev. 4, that are found in the FIPS PUB 199 "high" impact category.

sampled system's SSP was missing information related to key security controls, such as: AU-1, *Audit and Accountability Policy and Procedures*; CM-11, *User Installed Software*; CP-9, *Information System Backup*; MA-2, *Controlled Maintenance*; and PE-10, *Emergency Shutoff*. Furthermore, the failure to review and update SSPs has been a finding each year since the FY 2015 FISMA audit.

Kearney encourages the SEC to strengthen its annual review and update of SSPs for information systems by developing a quality control checklist.

***Improve Processes to Ensure Appropriate Supporting Documents are Maintained in the Enterprise Risk Management (ERM) Tool.*** The OIT's (b) (7)(E) states the SEC's ERM tool is the "official compliance tool for SEC information systems" and "maintains an inventory of all SEC information systems and supporting documentation," such as SSPs, Security Assessment Reports, Interconnection Security Agreements, and POA&Ms. While OIT largely populated and stored security artifacts in the SEC's ERM tool as required by SEC policy, we identified one instance where the SEC did not post the most recent Security Assessment Report for the (b) (7)(E) within the ERM tool. In addition, after a four-week search through system records and two separate WebEx meetings with key SEC personnel, the SEC was ultimately able to provide the Security Impact Analysis for the sampled configuration management changes. These challenges highlight the inefficiencies created when SEC personnel do not centrally store required security artifacts. Finally, the SEC did not include POA&Ms for one sampled system, despite the system going live in (b) (7)(E).

Kearney encourages the SEC to implement its policies and procedures in regards to populating the ERM tool with all required security artifacts for its information systems.

(b) (7)(E)

(b) (7)(E)



---

## Appendix I: Scope and Methodology

---

Kearney conducted this independent evaluation of the SEC's information security program and practices under the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Our evaluation included inquiries, observations, and inspection of SEC documents and records, as well as direct testing of controls.

**Scope:** Our overall objective was to assess the SEC's implementation of FISMA and respond to the *FY 2018 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 evaluation covered the period between October 1, 2017 and September 14, 2018 and addressed the following eight domains specified in DHS's reporting instructions for FY 2018:

- Risk Management
- Configuration Management
- Identity and Access Management
- Security Training
- Data Protection and Privacy
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning.

**Methodology:** We conducted an evaluation of the SEC's information security posture sufficient to address our objective. Specifically, to assess system security controls, Kearney reviewed the security assessment packages for a non-statistical, judgmentally selected sample of 8 of the SEC's 86 FISMA-reportable systems (or about 9 percent). The sample consisted of the internally and externally hosted systems shown in *Exhibit 4*.<sup>20</sup> Kearney also selected a random sample of 45 computers from the SEC's software patching tool to evaluate the completeness and accuracy of the SEC's hardware inventory. In addition, to address the requirements of the *FY 2018 IG FISMA Reporting Metrics* for the *Identity and Access Management*, *Security Training*, and *Incident Response* domains, we judgmentally selected and reviewed a non-statistical sample of controls related to those domains. Because sampled items were non-statistical, we did not project our results and conclusions to the total user population or measure overall prevalence.

---

<sup>20</sup> We selected information systems based on the SEC's inventory of FISMA-reportable systems maintained in OIT's system of record as of May 10, 2018. The inventory included 86 information systems (i.e., 45 SEC-operated, 29 contractor-operated, and 12 Federal shared services). We selected eight FISMA-reportable information systems factoring in: 1) whether the system was included in prior FISMA audits or covered in audits conducted by the OIG in the past two years; 2) whether the system was hosted internally or externally; 3) system risk categorization; and 4) the system's ATO status. We also solicited OIT's input for our sample selection.

*Exhibit 5: SEC Systems Sampled*

System Name	System Description	Internally/ Externally Hosted	System Categorization
[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]	[REDACTED]	[REDACTED]

System Name	System Description	Internally/ Externally Hosted	System Categorization
[REDACTED]	(b) (7)(E) [REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Source: ERM tool, SEC System of Record

To assess the SEC's procedures for detecting, reporting, and responding to security incidents, we selected and reviewed a non-statistical, judgmental sample of incidents, as well as supporting documents. Specifically, we selected incidents that:

- Occurred between October 1, 2017 and June 30, 2018
- Were confirmed as having compromised the confidentiality, integrity, or availability of information
- Were from all nine US-CERT threat taxonomies where a confirmed incident occurred
- Were representative of each incident priority type (i.e., high, medium, or low) as classified by OIT.

According to OIT's records, 434 incidents occurred between October 1, 2017 and June 30, 2018. OIT confirmed that 62 of these 434 incidents (or about 14 percent) impacted the confidentiality, integrity, or availability of SEC information. Based on our established criteria, we selected and reviewed 7 of the 62 incidents.

To rate the maturity level of the SEC's information security program and functional areas, Kearney used the scoring methodology defined in the *FY 2018 IG FISMA Reporting Metrics*. We interviewed key personnel, including staff from (b) (7)(E) [REDACTED]. Kearney also examined documents and records relevant to the SEC's information security program, including applicable Federal laws and guidance; SEC administrative regulations, policies, and procedures; system-level documents; and reports. As discussed throughout this report, these included, but were not limited to, the following:

- Federal Information Security Modernization Act of 2014, P.L. 113-283
- E-Government Act of 2002, P.L. 107-347
- Applicable OMB guidance, including OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 2016, and OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 2015
- Various NIST SPs
- SEC Administrative Regulation (SECR) 24-04, *Information Technology Security Program*
- SEC OIT policies.

Finally, Kearney reviewed the SEC's progress towards implementing recommendations from prior FISMA reports.

**Internal Controls:** Consistent with our evaluation objective, we did not assess OIT's overall management control structure. Instead, Kearney reviewed the SEC's controls specific to the *FY 2018 IG FISMA Reporting Metrics*. To understand OIT's management controls pertaining to its policies, procedures, and methods of operation, we relied on information requested from and supplied by OIT staff and information from interviews with OIT personnel. Kearney noted that the SEC generally complied with applicable FISMA and SEC policies and procedures, except as identified in this report. Our recommendations, if implemented, should address the areas of improvement we identified, as well as assist the SEC's information security program reach the next maturity level.

**Computer-Processed Data:** The U.S. Government Accountability Office's *Assessing the Reliability of Computer-Processed Data*, July 2009, (GAO-09-680G) 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.

Kearney used the SEC's ERM 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. Kearney performed data reliability, completeness,

and accuracy testing, in part, by comparing computer-processed information to testimonial evidence obtained from system and information owners and by 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:** The FY 2017 FISMA audit report included 20 recommendations for corrective action.<sup>21</sup> As of the date of this report, OIT had implemented one of the 20 recommendations. Kearney recommended closure of one additional FY 2017 recommendation (#6) as part of FY 2018 testing. Further, the FY 2016 FISMA audit report included 21 recommendations for corrective action.<sup>22</sup> As of the date of this report, OIT had implemented 19 of the 21 recommendations, with two remaining open. Although OIT addressed these recommendations, as we noted in this report, areas for improvement still exist. Appendix II: Open FISMA Recommendations lists all open OIG recommendations from prior FISMA audits.

Unrestricted SEC OIG audit and evaluation reports, including the FY 2016 and FY 2017 FISMA audit reports, can be accessed at: <https://www.sec.gov/oig>.

---

<sup>21</sup> 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 2017*, Report No. 546; March 30, 2018.

<sup>22</sup> 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 2016*, Report No. 539; March 7, 2016.

**Appendix II: Open FISMA Recommendations**

*Exhibit 6* below lists all FISMA recommendations that remain open from prior FISMA audits as of the date of this report.

*Exhibit 6: Open FISMA Recommendations*

Domain	Open Recommendations
<b>FY 2016</b>	
Identity and Access Management (Protect)	<b>Recommendation 10:</b> 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.
Security Training (Protect)	<b>Recommendation 15:</b> 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.
<b>FY 2017</b>	
Risk Management (Identify)	<b>Recommendation 1:</b> The Office of Information Technology define and implement a process that includes clear roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of agency information systems, (b) (7)(E)
	<b>Recommendation 2:</b> The Office of Information Technology define and implement a process (b) (7)(E)
	<b>Recommendation 3:</b> The Office of Information Technology define and implement a process to develop and maintain up-to-date inventories that include detailed information necessary for tracking and reporting of hardware assets connected to the agency's network, as well as (b) (7)(E)
	<b>Recommendation 4:</b> The Office of Information Technology perform a comprehensive review of its processes and resource needs to adequately support the agency's security assessment and authorization program (including creating and managing plans of actions and milestones) and, based on the results, take corrective action to ensure plans of action and milestones are timely documented, periodically updated, and accurately reflected in internal reports.
	<b>Recommendation 5:</b> The Office of Information Technology: (a) Continue efforts to define and formalize a plan addressing how enterprise architecture program management will be integrated with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control; and (b) define and implement a process to



Domain	Open Recommendations
	<p>ensure IT initiatives undergo an enterprise architecture compliance review before funding.</p> <p><b>Recommendation 6:</b> The Office of Information Technology continue efforts to implement a comprehensive risk management strategy by: (a) clearly defining and communicating roles and responsibilities for Tiers 1 and 2 information security risks and the risk executive function; and (b) identifying and defining requirements for an automated enterprise-wide solution to provide a centralized view of information security risks across the organization.</p> <p><b>Recommendation 7:</b> The Office of Information Technology improve the agency's acquisition of information systems, system components, and information system services by coordinating with the Office of Acquisitions to: (a) identify, review, and modify, as necessary, the agency's existing IT contracts (including those OIG reviewed) to ensure the contracts include specific contracting language, such as information security and privacy requirements, material disclosures, Federal Acquisition Regulation (FAR) clauses, and clauses on protection, detection, and reporting of information; and (b) define and implement a process to ensure that future acquisitions of IT services and products include such provisions.</p>
<p>Configuration Management (Protect)</p>	<p><b>Recommendation 8:</b> The Office of Information Technology develop, review, and approve secure baselines for all systems included in the (b) (7)(E) [REDACTED]</p> <p><b>Recommendation 9:</b> The Office of Information Technology define and implement a process, including roles and responsibilities, to routinely: (a) (b) (7)(E) [REDACTED]; (b) perform (b) (7)(E) [REDACTED] of all devices within the agency's network; and (c) document, track, and address the (b) (7)(E) [REDACTED], including those issues and vulnerabilities identified as unmitigated at the time of our audit.</p> <p><b>Recommendation 10:</b> The Office of Information Technology update its existing processes to ensure that the Information Security Office consistently performs and documents security impact analyses for proposed configuration changes before implementation.</p>
<p>Identity and Access Management (Protect)</p>	<p><b>Recommendation 11:</b> The Office of Information Technology develop and implement a transition plan or strategy, including milestones and priorities, for aligning the agency's identity, credential, and access management strategy with Federal initiatives.</p> <p><b>Recommendation 12:</b> (b) (7)(E) [REDACTED]</p>



Domain	Open Recommendations
	<p>(b) (7)(E)</p> <p><b>Recommendation 13:</b> (b) (7)(E)</p>
Security Training (Protect)	<p><b>Recommendation 15:</b> The Office of Information Technology develop and implement a process to ensure that all individuals with significant security responsibilities receive required specialized training before gaining access to information systems or before performing assigned duties.</p>
Information System Continuous Monitoring (Detect)	<p><b>Recommendation 16:</b> The Office of Information Technology update the existing continuous monitoring strategy to define: (a) qualitative and quantitative performance measures or data that should be collected to assess the effectiveness of the agency's continuous monitoring program; (b) procedures for reviewing and modifying all aspects of the agency's continuous monitoring strategy; and (c) the agency's ongoing authorization process.</p>
Incident Response (Respond)	<p><b>Recommendation 17:</b> The Office of Information Technology review and update incident response plans, policies, procedures, and strategies to: (a) address all common threat and attack vectors and the characteristics of each particular situation; (b) identify and define performance metrics that will be used to measure and track the effectiveness of the agency's incident response program; (c) develop and implement a process to ensure that incident response personnel obtain data supporting the incident response metrics accurately, consistently, and in a reproducible format; (d) define incident response communication protocols and incident handlers' training requirements; and (e) remove outdated terminology and references.</p> <p><b>Recommendation 18:</b> The Office of Information Technology fully implement processes to: (a) consistently document and timestamp every step in the incident response process, from detection to resolution; and (b) ensure a personnel other than the incident ticket creator reviews incident documentation (including logs and tickets) and confirms that consistent and complete information is maintained for every step in the incident response process.</p> <p><b>Recommendation 19:</b> The Office of Information Technology improve its ability to review indicators of compromise by (b) (7)(E)</p>

Domain	Open Recommendations
	<p data-bbox="480 264 1390 373">(b) (7)(E)</p> <p data-bbox="480 380 1398 518"><b>Recommendation 20:</b> The Office of Information Technology perform an assessment of existing incident response reporting mechanisms, as well as develop a process to periodically measure and ensure the timely reporting of incidents to agency officials and external stakeholders.</p>

## Appendix III: Management Comments

MEMORANDUM

December 12, 2018

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

From: Kenneth Johnson, Chief Operating Officer

Subject: Management Response to Draft Report No. 552, "Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2018"

**KENNETH  
JOHNSON**Digitally signed by  
KENNETH JOHNSON  
Date: 2018.12.12 14:25:26  
-05'00'

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) recommendations related to its evaluation of the SEC's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year (FY) 2018 (Report No. 552). The report evaluates the SEC's Information Security Program in accordance with the FY18 Inspector General FISMA Reporting Metrics,<sup>1</sup> which are designed to assist Inspectors General in assessing the maturity levels of controls across seven domains aligned to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

I am pleased that you found that the SEC improved its information security program in FY 2018. While more remains to be done, we have worked hard to strengthen the agency's cybersecurity posture, cultivate a cybersecurity-minded workforce, and ensure that the staff is appropriately equipped to identify and mitigate risks agency-wide. Your feedback—and that of other agencies—is crucial to these efforts. Indeed, as you know, in FY 2018, SEC staff supported five separate information technology-related audits conducted by the OIG and the Government Accountability Office (GAO). And, in response to feedback arising from both these and prior audits, the agency has, among other things, enhanced its policies, strengthened authentication mechanisms, reduced the number of critical vulnerabilities, enhanced security awareness training processes, and improved its continuous monitoring program. The SEC also completed a data center migration during FY 2018, which will help ensure that agency data is adequately safeguarded and enhance the agency's resiliency in response to physical and environmental threats and certain disruptions to telecommunications infrastructure.

Our progress against previous audit recommendations also reflects these improvements. By the end of FY 2018, the SEC was able to close 17 open OIG recommendations. Notably, the staff

<sup>1</sup> U.S. Department of Homeland Security, FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, May 24, 2018.

was able to achieve this progress while also supporting fieldwork for the OIG's FY 2018 FISMA evaluation, which began a little more than month after the OIG issued its FY 2017 FISMA report on March 30, 2018. Going forward, in FY 2019, the agency plans to hire additional staff in order to continue to prioritize and address recommendations made by both the OIG and the GAO.

Turning to your most recent report issued on November 30, 2018, we agree with your recommendations and, as noted below, we have outlined the steps we have already taken or intend to take as to each one. As we have discussed, a number of these recommendations relate to an evaluation of the SEC's compliance with the Department of Homeland Security's (DHS's) High Value Assets Control Overlay (HVA Overlay). We agree that it is vitally important to protect the SEC's high value assets. To that end, SEC staff had begun implementing critical facets of the HVA Overlay even before DHS issued this guidance in November 2017. During FY 2018, the staff continued efforts to implement security controls included in the HVA Overlay, including (b) (7)(E) [REDACTED]. Additionally, SEC staff engaged with DHS concerning agency HVAs, including by having DHS complete technical reviews of agency HVAs. The staff is also working to execute a strategy to provide (b) (7)(E) [REDACTED] (b) (7)(E) [REDACTED]. Further, in FY 2019, the staff plans to continue the implementation of the HVA Overlay within the agency's Governance, Risk, and Compliance tool, RSA Archer, which will assist in helping to implement and monitor security compliance across the agency HVAs. As these ongoing efforts indicate, we have prioritized and invested substantial resources in implementing enhanced controls for agency HVAs, even though DHS does not require agencies to implement the HVA Overlay.<sup>2</sup>

We appreciate the professionalism and courtesies provided by the OIG and Kearney staff during this audit and we look forward to working with your office to address the areas noted in your report.

<sup>2</sup> DHS High Value Asset Control Overlay Frequently Asked Questions, available at <https://www.dhs.gov/sites/default/files/publications/HVA%20Control%20Overlay%20v1.0%20FAQ.pdf>.

**Management Response to Recommendations**

**Recommendation 1:** Update configuration management procedures to require that (b) (7)(E) (b) (7)(E) are approved.

**Response:** We concur it is important to (b) (7)(E) (b) (7)(E) are approved. Pursuant to this recommendation, the Office of Information Technology (OIT) will update configuration management procedures to (b) (7)(E) (b) (7)(E) are approved.

**Recommendation 2:** Update configuration management procedures to require (b) (7)(E) (b) (7)(E) (b) (7)(E)

**Response:** We concur it is important to (b) (7)(E) (b) (7)(E) Pursuant to this recommendation, OIT will update configuration management procedures to (b) (7)(E) (b) (7)(E) (b) (7)(E)

**Recommendation 3:** Complete initiatives to implement (b) (7)(E) (b) (7)(E) (b) (7)(E)

**Response:** We concur and, pursuant to this recommendation, will complete our initiatives to implement (b) (7)(E) (b) (7)(E) (b) (7)(E)

**Recommendation 4:** Complete initiatives to implement (b) (7)(E) (b) (7)(E) (b) (7)(E)

**Response:** We concur. During FY 2018, SEC staff began executing a strategy to (b) (7)(E) (b) (7)(E) and, pursuant to this recommendation, OIT will review and update the project plan and continue its implementation of (b) (7)(E) (b) (7)(E) (b) (7)(E)

**Recommendation 5:** Update procedures for the (b) (7)(E)

(b) (7)(E)

**Response:** We concur. Pursuant to this recommendation, OIT will update existing procedures for the (b) (7)(E)

**Recommendation 6:** Define and implement a control to detect instances where contractor personnel received network accounts but were not assigned privacy and information security awareness training, nor tracked within system reporting tools.

**Response:** We concur. During early FY 2019, SEC staff completed an enhancement to the agency's learning management system and updated internal protocols to facilitate the issuance of required privacy and security awareness training for personnel before they receive system credentials. This will also ensure that the training status for new staff are tracked within the agency's learning management system. Pursuant to this recommendation, the SEC will define and implement controls to track and detect instances where contractors receive system credentials prior to completing privacy and information security awareness training.

**Recommendation 7:** (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Additionally, Office of Information Technology should develop procedures that (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Accordingly, Office of Information Technology should update policies and procedures to (b) (7)(E)

(b) (7)(E)

**Response:** We concur that it is important to (b) (7)(E)

(b) (7)(E)

Pursuant to this recommendation, OIT will also develop procedures to (b) (7)(E)

(b) (7)(E)

Additionally, OIT will work to (b) (7)(E)

(b) (7)(E)

**Recommendation 8:** (b) (7)(E)

(b) (7)(E)

(b) (7)(E)



**Response:** We concur. Pursuant to this recommendation, OIT will take steps to (b) (7)(E)  
(b) (7)(E)  
(b) (7)(E)

**Recommendation 9:** Establish a process to improve coordination and communication among the various Office of Information Technology teams (b) (7)(E)  
(b) (7)(E)  
(b) (7)(E)

**Response:** We concur. Pursuant to this recommendation, OIT will (b) (7)(E)  
(b) (7)(E)  
(b) (7)(E)

**Recommendation 10:** Update and maintain contingency planning documentation (i.e., Enterprise Disaster Recovery Plan, Business Impact Analyses, and Information System Contingency Plans) in accordance with SEC policies and procedures.

**Response:** We concur. OIT will update and maintain contingency planning documentation in accordance with SEC policies and procedures during FY 2019.

**Recommendation 11:** Test the Enterprise Disaster Recovery Plan in accordance with SEC's policies and procedures for fiscal year 2019.

**Response:** We concur. OIT will test the Enterprise Disaster Recovery Plan in accordance with SEC's policies and procedures in fiscal year 2019. We note that SEC staff completed a data center migration during FY 2018. This migration, which was completed in October 2018, has improved the agency's resiliency and addressed a number of recommendations issued by the OIG in its 2017 report on the agency's management of its data centers. Planning for our annual disaster recovery exercise is ongoing, and the exercise is scheduled for (b) (7)(E) FY 2019.



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

Web: <https://www.sec.gov/oig>

Telephone: 1-833-SEC-OIG1 (833-732-6441)

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](mailto:AUDplanning@sec.gov). Comments 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.