

REPORT NO. 563

December 21, 2020

OFFICE OF  
**INSPECTOR  
GENERAL**

OFFICE OF AUDITS

**Fiscal Year 2020 Independent  
Evaluation of SEC's  
Implementation of the Federal  
Information Security  
Modernization Act of 2014**

This report contains non-public information about the U.S. Securities and Exchange Commission's information technology program. We redacted the non-public information to create this public version. All redactions are pursuant to Freedom of Information Act exemption (b)(7)(E) unless otherwise stated.

REDACTED FOR PUBLIC RELEASE



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

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

December 21, 2020

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

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

**SUBJECT:** *Fiscal Year 2020 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014, Report No. 563*

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 Fiscal Year 2020. We contracted with Kearney and Company, P.C., and (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 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 Kearney's report and related documentation.

Kearney reported that the SEC improved aspects of the agency's information security program, such as refining its risk management tools, improving the timeliness of security patch deployments, enhancing its security awareness and training processes, continuing its efforts to enhance its continuous monitoring program, and improving its incident response capabilities. These improvements occurred despite facing unique challenges presented by the ongoing Coronavirus Disease 2019 (COVID-19) pandemic, which included a significant increase in telework.

However, as described in the attached report, Kearney identified opportunities for improvement in key areas and made seven new recommendations to strengthen these areas of the SEC's information security program. As a result, Kearney noted that the agency's information security program did not meet the FY 2020 IG FISMA Reporting Metrics' definition of "effective."

On December 2, 2020, we provided management with a draft of Kearney's report for review and comment. In the agency's December 15, 2020 response, management concurred with Kearney's recommendations. Kearney included management's response as Appendix IV of this report.

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. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits Evaluations, and Special Reports.

Attachment

cc: Jay Clayton, Chairman

Sean Memon, Chief of Staff, Office of Chairman Clayton

Bryan Wood, Deputy Chief of Staff, Office of Chairman Clayton

Kimberly Hamm, Chief Counsel/Senior Policy Advisor, Office of Chairman Clayton

John Moses, Managing Executive, Office of Chairman Clayton

Hester M. Peirce, Commissioner

Benjamin Vetter, Counsel, Office of Commissioner Peirce

Elad L. Roisman, Commissioner

Matthew Estabrook, Counsel, Office of Commissioner Roisman

Allison Herren Lee, Commissioner

Andrew Feller, Counsel, Office of Commissioner Lee

Caroline A Crenshaw, Commissioner

Armita Cohen, Counsel, Office of Commissioner Crenshaw

Gabriel Benincasa, Chief Risk Officer

Matthew Keeler, Management and Program Analyst, Office of Chief Risk Officer

Rick A. Fleming, Investor Advocate, Office of the Investor Advocate

Holli Heiles Pandol, Director, Office of Legislative and Intergovernmental Affairs

John J. Nester, Director, Office of Public Affairs

Robert B. Stebbins, General Counsel

David Bottom, Director/Chief Information Officer, Office of Information Technology

Andrew Krug, Chief Information Security Officer, Office of Information Technology

Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology

Jamey McNamara, Chief Human Capital Officer, Office of Human Resources

***Fiscal Year 2020 Independent Evaluation  
of the U.S. Securities and Exchange  
Commission's Implementation of the  
Federal Information Security  
Modernization Act of 2014***

**December 21, 2020**



*Point of Contact Phil Moore, 1701 Duke Street, Suite 500  
Alexandria, VA 22314  
703-931-5600, 703-931-3655 (fax)  
[Phil.Moore@kearneyco.com](mailto:Phil.Moore@kearneyco.com)*

*Kearney & Company's TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14*

**COVER LETTER**

December 21, 2020

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 in support 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, entitled *Fiscal Year 2020 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014*.

The objectives of this evaluation were to assess the effectiveness of the SEC's information security program and practices and respond to the Department of Homeland Security's (DHS) *Fiscal Year (FY) 2020 Inspector General (IG) FISMA Reporting Metrics Version 4.0 (FY 2020 IG FISMA Reporting Metrics)*, dated April 17, 2020. Kearney's methodology for the FY 2020 FISMA evaluation included testing the effectiveness of selected security controls the SEC has implemented in six sampled information systems for compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013. The *FY 2020 IG FISMA Reporting Metrics* utilize a maturity model and request that IGs evaluate and rate the effectiveness of security controls for each of the five NIST Framework for Improving Critical Infrastructure Cybersecurity ("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 2019, the SEC’s Office of Information Technology (OIT) improved aspects of its information security program. Among other actions taken, OIT made progress in refining its risk management tools, initiating processes to develop a [REDACTED], improving the timeliness of security patch deployments, enhancing its security awareness and training processes, continuing its efforts to enhance its continuous monitoring program, and improving its incident response capabilities. These improvements occurred despite facing unique challenges presented by the ongoing Coronavirus Disease 2019 (COVID-19) pandemic, which included a significant increase in telework.

Although the SEC has strengthened its program since the last FISMA evaluation, Kearney noted that the agency’s information security program did not meet the *FY 2020 IG FISMA Reporting Metrics*’ definition of “effective,” which requires the simple majority of domains to be rated as Level 4: *Managed and Measurable*. As shown in the table below, the SEC’s assessed maturity level for the domains of Risk Management and Incident Response improved one maturity level, to Level 3: *Consistently Implemented* and Level 4: *Managed and Measurable*, respectively. While the agency’s program, as a whole, did not reach the level of an effective information security program, the SEC has shown significant improvements at the domain levels.

***Exhibit 1: Summary of SEC FISMA Ratings***

Domain	Assessed Rating By Fiscal Year (FY)	
	2020	2019
<b>Risk Management</b>	Level 3: <i>Consistently Implemented</i>	Level 2: <i>Defined</i>
<b>Configuration Management</b>	Level 2: <i>Defined</i>	Level 2: <i>Defined</i>
<b>Identity and Access Management</b>	Level 2: <i>Defined</i>	Level 2: <i>Defined</i>
<b>Data Protection and Privacy</b>	Level 3: <i>Consistently Implemented</i>	Level 3: <i>Consistently Implemented</i>
<b>Security Training</b>	Level 2: <i>Defined</i>	Level 2: <i>Defined</i>
<b>Information Security Continuous Monitoring</b>	Level 3: <i>Consistently Implemented</i>	Level 3: <i>Consistently Implemented</i>
<b>Incident Response</b>	Level 4: <i>Managed and Measurable</i>	Level 3: <i>Consistently Implemented</i>
	Level 4: <i>Managed and Measurable</i>	Level 4: <i>Managed and Measurable</i>

Source: Kearney & Company, P.C. (Kearney)-generated based on FYs 2019 and 2020 CyberScope Metric responses.

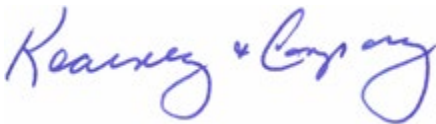
Our report includes seven new recommendations to strengthen the SEC’s information security program. As our report highlights, while the agency made improvements across six of the eight *FY 2020 IG FISMA Reporting Metrics* areas, opportunities exist for the SEC to improve its performance in all eight *FY 2020 IG FISMA Reporting Metrics* areas.<sup>1</sup> Significant opportunities

<sup>1</sup> The SEC achieved a rating of Level 4: *Managed and Measurable*, considered “effective,” in the Incident Response and Contingency Planning domains. However, metric-level improvements can still be made related to current-year and prior-year recommendations.

for improvement remain in key areas such as developing a supply chain management action plan, fully implementing a [REDACTED] enhancing configuration management activities, and delivering specialized security training. 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 & Company". The signature is stylized and cursive.

Kearney & Company, P.C.  
December 21, 2020



## TABLE OF CONTENTS

	<u>Page #</u>
COVER LETTER.....	i
TABLE OF CONTENTS .....	iv
TABLE OF EXHIBITS .....	iv
ABBREVIATIONS.....	v
BACKGROUND AND OBJECTIVES .....	1
Background .....	1
Objectives.....	4
RESULTS .....	6
Domain #1: Risk Management .....	6
Domain #2: Configuration Management.....	10
Domain #3: Identity and Access Management.....	14
Domain #4: Data Protection and Privacy .....	17
Domain #5: Security Training .....	21
Domain #6: Information Security Continuous Monitoring (ISCM) .....	24
Domain #7: Incident Response (IR) .....	26
Domain #8: Contingency Planning.....	27
OVERALL CONCLUSION.....	29
OTHER MATTERS OF INTEREST .....	30
APPENDIX I: SCOPE AND METHODOLOGY .....	34
APPENDIX II: OPEN FISMA RECOMMENDATIONS.....	38
APPENDIX III: SUMMARY OF ASSESSED FISMA RATINGS, FY 2019 & FY 2020....	42
APPENDIX IV: MANAGEMENT COMMENTS.....	45

## TABLE OF EXHIBITS

	<u>Page #</u>
<i>Exhibit 1: Summary of SEC FISMA Ratings.....</i>	<i>ii</i>
<i>Exhibit 2: Cybersecurity Framework Functions Mapped to FY 2020 IG FISMA Reporting Metrics Assessment Domains .....</i>	<i>2</i>
<i>Exhibit 3: IG Assessment Maturity Levels.....</i>	<i>3</i>



<i>Exhibit 4: Security-Focused Configuration Management Phases .....</i>	<i>10</i>
<i>Exhibit 5: SEC Systems Sampled .....</i>	<i>35</i>
<i>Exhibit 6: Open FISMA Recommendations .....</i>	<i>38</i>
<i>Exhibit 7: Summary of Assessed FISMA Ratings between FY 2019 and FY 2020 .....</i>	<i>42</i>

### **ABBREVIATIONS**

CP	Contingency Planning
Cybersecurity Framework	National Institute of Standards and Technology's Framework for Improving Critical Infrastructure of Cybersecurity
DHS	Department of Homeland Security
FISMA	Federal Information Systems Modernization Act of 2014
FY	Fiscal Year
GSS	General Support System
HVA	High -Value Asset
IA	Identity and Access Management
ICAM	Identity Credential and Access Management
ICT	Information and Communications Technology
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
IT	Information Technology
M	Memorandum
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
Rev.	Revision
RM	Risk Management

SEC	U.S. Securities and Exchange Commission
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SP	Special Publication
SSP	System Security Plan
ST	Security Training
TTX	Tabletop Exercise

## **BACKGROUND AND OBJECTIVES**

### **Background**

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law [PL] 113-283), which amended the Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002 (PL 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, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* issued to IGs guidance on FISMA reporting for fiscal year (FY) 2020.<sup>2</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 2020 IG FISMA Reporting Metrics*. The results of these efforts supported the Office of Inspector General's (OIG) FY 2020 CyberScope submission to OMB and DHS.<sup>3</sup>

As **Exhibit 2** illustrates, the *FY 2020 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's (NIST) Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework").<sup>4</sup>

---

<sup>2</sup> *Fiscal Year 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 4.0, dated April 17, 2019 (hereafter referred to as "*FY 2020 IG FISMA Reporting Metrics*").

<sup>3</sup> CyberScope is the platform that Chief Information Officers, Privacy Officers, and IGs use to meet FISMA reporting requirements. The SEC OIG completed its FY 2019 CyberScope submission to DHS and OMB on October 30, 2020.

<sup>4</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 2: Cybersecurity Framework Functions Mapped to FY 2020 IG FISMA Reporting Metrics Assessment Domains***

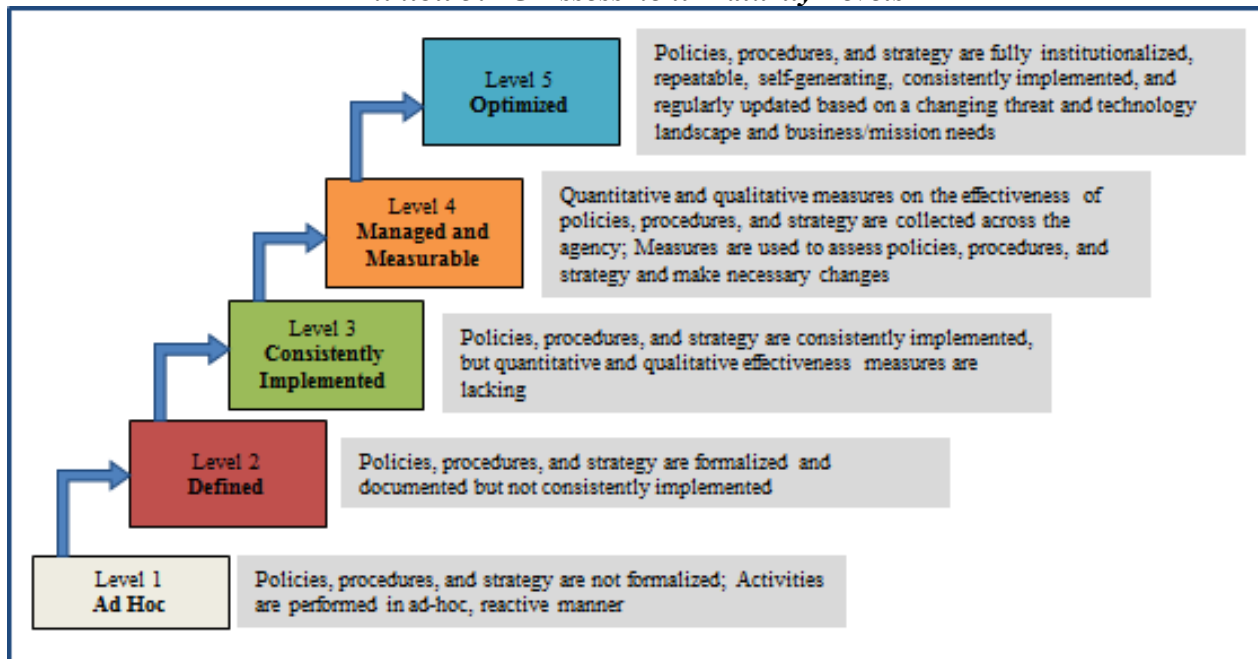
Cybersecurity Framework Functions	FY 2020 IG FISMA Reporting Metrics Assessment Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response (IR)
Recover	Contingency Planning

*Source: Kearney-generated from FY 2020 IG FISMA Reporting Metrics*

**Change in Metrics and Assessment Methodology:** Since FY 2017, when the *IG FISMA Reporting Metrics* required IGs to assess seven domains included in the five Cybersecurity Framework functions, the *IG FISMA Reporting Metrics* were updated to include an eighth domain (i.e., Data Protection and Privacy) in FY 2018 and new requirements for supply chain risk management and the security of Domain Name Systems in FY 2019. In FY 2020, the *FY 2020 IG FISMA Reporting Metrics* remained largely stable with considerations for asset management, security architecture, and flaw remediation to assess agency progress in securing mobile endpoints and employing secure application development processes, as well as considerations for OMB Memorandum (M) M-19-26, *Update to the Trusted Internet Connection Initiative* (September 12, 2019), to assess the agency's progress in planning for the effective implementation of the security capabilities outlined in OMB M-19-26.

As shown in ***Exhibit 3***, the foundation levels of the maturity model ensure that agencies develop sound policies and procedures (Level 2), 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 3: IG Assessment Maturity Levels*



Source: Kearney-generated based on the FY 2020 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 directs OIT and is responsible for ensuring compliance with applicable information security requirements. The Chief Information Security Officer, designated by the Chief Information Officer, is responsible, in part, for developing, maintaining, centralizing, and monitoring ongoing adherence to the SEC's Information Security Program Plan and supporting the Chief Information Officer in annually reporting on the effectiveness of the SEC's information security program.

**Prior Audits and Evaluations:** As of September 30, 2020, the SEC closed 7 total recommendations from prior-year FISMA reports within FY 2020. Specifically, within FY 2020, the SEC closed 3 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; 3 of 11 recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2018<sup>6</sup> (FY 2018 FISMA evaluation), dated December 12, 2018; and 1 of 9 recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2019<sup>7</sup> (FY 2019 FISMA evaluation), dated December 18, 2019. To close these recommendations, OIT made progress in developing and maintaining a comprehensive and accurate inventory of agency information systems, improving aspects of its remote access management activities, ensuring the timely reporting of incidents to agency officials and external stakeholders, updating procedures for digital media sanitization, improving its security awareness training management controls, performing authenticated vulnerability scans, and defining an IT security awareness and training strategy. In total, since the FY 2017 FISMA audit, the SEC has remediated 11 of the 20 recommendations from the FY 2017 FISMA audit, 5 of the 11 recommendations from the FY 2018 FISMA evaluation, and 1 of the 9 recommendations from the FY 2019 FISMA evaluation.

## Objectives

Our overall objective was to evaluate the SEC's implementation of FISMA for FY 2020 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 2020 IG FISMA Reporting Metrics*:

- Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- ISCM
- IR
- Contingency Planning.

To assess the effectiveness and maturity of security controls identified in the *FY 2020 IG FISMA Reporting Metrics*, Kearney judgmentally selected and reviewed a non-statistical sample of 6 information systems from the SEC's May 6, 2020 inventory of 83 FISMA-reportable information systems. Additionally, Kearney performed other tests and assessments.

---

<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").

<sup>6</sup> U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 552; December 12, 2018 (hereafter referred to as "FY 2018 FISMA evaluation").

<sup>7</sup> U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 558; December 18, 2019 (hereafter referred to as "FY 2019 FISMA evaluation").

[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.



## **RESULTS**

### **Domain #1: Risk Management**

The *FY 2020 IG FISMA Reporting Metrics*, in accordance with the NIST Cybersecurity Framework, consider risk management as 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 once determined, and monitoring risk over time. NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, dated March 2011, states 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 assessed maturity level is Level 3: *Consistently Implemented*, meaning the SEC formalized and consistently implemented its continuous monitoring policies, procedures, and strategies for ongoing authorization, but quantitative and qualitative effectiveness measures were lacking. While the agency's assessed maturity improved from Level 2: *Defined* to Level 3: *Consistently Implemented* between FYs 2019 and 2020, it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

**Prior-Year Findings:** Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Develop or maintain an accurate or complete [REDACTED]
- 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 strategic human capital management and performance management.

Specifically, in the FY 2019 FISMA evaluation, Kearney determined that the SEC did not:

- Complete all relevant components [REDACTED] according to [REDACTED]
- Define and communicate Information System Owner and Information System Security Officer roles and responsibilities
- Develop and document a standard [REDACTED]
- Develop a methodology to demonstrate the control assignments from NIST SP 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013 (NIST SP 800-53, Rev. 4), including control tailoring

and inheritance; and update the SEC's System Security Plan (SSP) templates to ensure control tailoring justification corresponds to established methodology.

Similarly, Kearney determined that many of the weaknesses with the SEC's Risk Management program identified during the FY 2017 FISMA audit and FY 2019 FISMA evaluation remained present in FY 2020, as listed below:

- While the SEC implemented a new tool to facilitate standard data elements and [REDACTED] for its [REDACTED] the SEC has not defined a process for developing and maintaining its up-to-date [REDACTED] utilized in the organization's environment
- The SEC did not address strategic capital human management, nor performance management, in key documentation related to enterprise architecture, including the Enterprise Risk Management Strategy and the enterprise architecture policy
- The SEC did not complete all relevant components of its [REDACTED] inventory in its [REDACTED] in accordance with SEC [REDACTED]
- While the SEC informally established the role of the Information System Security Officer, the roles and responsibilities had not formally been defined and communicated in the applicable policies and procedures
- The SEC did not consistently utilize a standard [REDACTED]
- The SEC did not address all of the NIST SP 800-53, Rev. 4 moderate baseline controls in 6 of the 6 (100%) sampled systems. Specifically, the SSPs for 5 of the 6 sampled systems did not address 3 of the 261 (1.15%) of the NIST SP 800-53, Rev. 4 moderate baseline controls, and the SSP for 1 of the 6 sampled systems did not address 1 of the 261 (0.38%) of the NIST SP 800-53, Rev. 4 moderate baseline controls.

These control weaknesses occurred for a variety of reasons. Although the SEC deployed new tools to facilitate its [REDACTED] additional work was ongoing to fully integrate those tools. In addition, OIT was in the process of updating documentation related to enterprise architecture, updating its [REDACTED] updating documentation related to Information System Security Officer roles and responsibilities, and establishing its [REDACTED] in FY 2020. Lastly, while the SEC updated applicable SSP templates to include the absent controls, the sampled systems' SSPs were updated in FY 2020 prior to the modification of the SSP templates or without consideration of the modified SSP template due to extenuating circumstances.

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](#).

**Current-Year Findings:** Kearney has identified additional opportunities for the agency to mature its Risk Management program. See the findings detailed below, as well as **Other Matters of Interest**.

In addition to the prior-year findings, Kearney identified a new weakness related to mobile device management.

**Insufficient Integration of Mobile Device Management Controls into Risk Management**

**Program:** The *FY 2020 IG FISMA Reporting Metrics* place emphasis on the agency's mobile device management and enterprise mobility management. Specifically, the *FY 2020 IG FISMA Reporting Metrics* require that [REDACTED]

[REDACTED] Additionally, the *FY 2020 IG FISMA Reporting Metrics* require that agencies define [REDACTED]

[REDACTED] and [REDACTED] NIST SP 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, dated June 2013, states that organizations should regularly maintain mobile device security. [REDACTED]

[REDACTED] NIST SP 800-163, Rev. 1, *Vetting the Security of Mobile Applications*, dated April 2019, states: [REDACTED]

SEC OIT did not formally document the agency's requirements for applying security and operating system updates within a given period of time to mobile devices, nor has OIT documented the [REDACTED]

[REDACTED] Additionally, OIT did not [REDACTED]

This occurred, in part, because the SEC was still in the process of identifying mobile-specific risks across the agency-wide General Support System (GSS) in FY 2020. Further, the SEC had not responded to updated regulatory requirements from the *FY 2020 IG FISMA Reporting Metrics*.

Maintaining a robust mobile device program is necessary as mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices. Additionally, and similarly noted in the SEC OIG Report, *Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services*, Report No. 562, September 30, 2020, agencies should implement organization-specific mobile application vetting processes as developers may perform their own software assurance processes on an application, but there is no guarantee the application will conform to an agency's security requirements.

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

To mature the U.S. Securities and Exchange Commission's Risk Management program, Kearney & Company, P.C. recommends that the Office of Information Technology continue to work to close open prior-year recommendations. See [APPENDIX II: OPEN FISMA RECOMMENDATIONS](#).

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

**Recommendation 1:** Develop and document a) Agency requirements for applying security and operating system updates to mobile devices in an organizationally defined timeframe; [REDACTED]

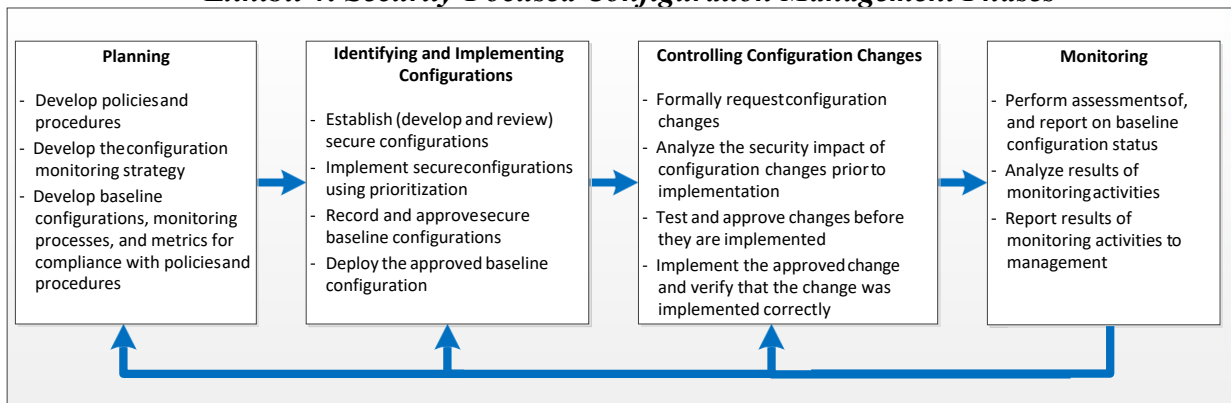
**Management's Response:** We concur. The SEC has begun improving its mobile device program, in accordance with the Office of the Inspector General (OIG) Report 562, *Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services*. We will ensure the [REDACTED] completed will fulfill these recommendations from both reports, and develop and document [REDACTED] Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**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 #2: Configuration Management

The *FY 2020 IG FISMA Reporting Metrics*, in accordance with NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, dated August 2011, consider configuration management 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, 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, 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. Further, NIST SP 800-53, Rev. 4, (SI-2), "Flaw Remediation," states that organizations should identify, report, and correct information system flaws. Finally, as described in **Exhibit 4**, 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 4: Security-Focused Configuration Management Phases**



Source: Kearney-generated based on NIST SP 800-128

Kearney assessed the SEC's Configuration Management program and determined that the program's assessed maturity level is Level 2: *Defined*, meaning that the SEC formalized and documented configuration management policies, procedures, and strategies, but did not consistently implement them. The SEC's assessed maturity remained at Level 2: *Defined* between FYs 2019 and 2020, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

<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.

**Prior-Year Findings:** Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Fully define or [REDACTED] or review and update SSPs [REDACTED] at least annually or within established schedules
- Adequately implement [REDACTED]

Specifically, in the FY 2018 FISMA evaluation, Kearney determined that the SEC did not:

- [REDACTED]
- Perform configuration [REDACTED] procedures to [REDACTED]

Similarly, Kearney determined that many of the weaknesses with the SEC's Configuration Management program identified during the FY 2017 FISMA audit and FY 2018 FISMA evaluation remained present in FY 2020, as listed below:

- The SEC did not define an [REDACTED]. Additionally, while the SEC has increased its overall approved [REDACTED] percentage, only [REDACTED]
- The SEC did not consistently update its flaw remediation procedures to reflect its current practices. Additionally, the SEC did not [REDACTED]
- The SEC did not [REDACTED]
- The SEC did not [REDACTED]

The above weaknesses occurred because SEC management had not fully addressed management challenges identified in FYs 2017 and 2018. While OIT continued to increase its number of approved [REDACTED] the agency was unable to dedicate the necessary resources to approve [REDACTED] for all SEC systems. Additionally, the SEC

[REDACTED]

continued to update its Vulnerability Management Program Standard Operating Procedures to define enhancements to the vulnerability management process for [REDACTED] [REDACTED] however, these processes were not consistent with the processes defined in the vulnerability management policy. Finally, OIT was in the process of formally developing all aspects of configuration management procedures, specifically regarding [REDACTED] [REDACTED]

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](#).

**Current-Year Findings:** Kearney has identified additional opportunities for the agency to mature its Configuration Management program. See the findings detailed below, as well as **Other Matters of Interest**.

In addition to the prior-year findings, Kearney identified new weaknesses related to the agency's inventory of network connections.

[REDACTED] **Agency Network Connections Inventory:** The *FY 2020 IG FISMA Reporting Metrics* require that agencies define processes to develop and maintain an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection. Additionally, OMB M-19-26 states that "agency Chief Information Officers shall maintain an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection."

While OIT documented an inventory of agency network connections, the agency [REDACTED] [REDACTED] as required by OMB M-19-26.

The lack of inventory documentation occurred, in part, because the agency was in the process of responding to the requirements outlined in OMB M-19-26.

Without a [REDACTED] the SEC may not retain strong protections for Federal systems and information and may be unprepared in the event OMB, DHS, or others request the information to assist with Government-wide cybersecurity incident response or other cybersecurity matters.



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

To mature the U.S. Securities and Exchange Commission's Configuration Management program, Kearney & Company, P.C. recommends that the Office of Information Technology continue to work to close prior-year recommendations. See [APPENDIX II: OPEN FISMA RECOMMENDATIONS](#).

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

**Recommendation 2:** Develop and document a process to consistently [REDACTED]

**Management's Response:** We concur. The SEC currently maintains an inventory of network connections, [REDACTED]

[REDACTED] including the details listed in the recommendation. Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**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 #3: Identity and Access Management

The *FY 2020 IG FISMA Reporting Metrics*, in accordance with the NIST Cybersecurity Framework, require agencies to establish an identity and access management program that limits access to physical and logical assets and associated facilities to authorized users, processes, and devices, and it is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. NIST SP 800-53, Rev. 4, (AC-1), "Access Control Policy and Procedures," and (IA-1), "Identification and Authentication Policy and Procedures," require 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 identity and 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 assessed maturity level is Level 2: *Defined*, meaning the SEC formalized and documented identity and access management policies, procedures, and strategies, but did not consistently implement them. While the agency continued to make improvements, the SEC's assessed maturity remained at Level 2: *Defined* between FYs 2019 and 2020, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

**Prior-Year Findings:** Specifically, in the FY 2017 FISMA audit, the OIG identified that the SEC did not:

- [REDACTED]

Specifically, in the FY 2019 FISMA evaluation, Kearney determined that the SEC did not:

- Perform a formal risk assessment to determine the population of users that should be formally recertified and update procedures to document how the new recertification process should be carried out given the volume of SEC GSS users
- Develop and document a formal process to [REDACTED]

Similarly, Kearney determined that many of the weaknesses with the SEC's Identity and Access Management program identified during the FY 2017 FISMA audit and FY 2019 FISMA evaluation remained present in FY 2020, as listed below:

- The SEC did not complete its policies and procedures which describe [REDACTED] including a procedure for [REDACTED]
- The SEC did not consistently complete its [REDACTED] was not completed for [REDACTED]
- The SEC did not develop and document a formal process to [REDACTED] as well as perform a formal review for [REDACTED]

These control weaknesses occurred, in part, because the SEC was in the process of updating its policies and procedures related to [REDACTED] during FY 2020. Further, the completion of the SEC's [REDACTED] process was not completed due to the submission of reports in between review cycles that were deemed incomplete. Finally, while the SEC had procedures in place for [REDACTED] improvements are still being considered and documented for [REDACTED]

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](#).

**Current-Year Findings:** Kearney has identified additional opportunities for the agency to mature its Identity and Access Management program. See the findings detailed below, as well as **Other Matters of Interest**.

In addition to the prior-year findings, Kearney identified new weaknesses related to [REDACTED]

[REDACTED] The *FY 2020 IG FISMA Reporting Metrics* require agencies to review [REDACTED] Additionally, NIST 800-53, Rev. 4, [REDACTED] Further, NIST 800-53, Rev. 4, [REDACTED]

While the SEC implemented processes to [REDACTED]  
[REDACTED]

This occurred, in part, because the SEC did not incorporate policies and procedures for reviewing [REDACTED] within its [REDACTED]  
[REDACTED]

Without a documented process for reviewing [REDACTED] the SEC may be unable to ensure the [REDACTED] In addition, the SEC may be [REDACTED]

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

To mature the U.S. Securities and Exchange Commission's Identity and Access Management program, Kearney & Company, P.C. recommends that the Office of Information Technology continue to work to close prior-year recommendations. See [APPENDIX II: OPEN FISMA RECOMMENDATIONS](#).

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

**Recommendation 3:** Develop and document processes for performing risk-based reviews [REDACTED]  
[REDACTED] on an organizationally defined frequency.

**Management's Response:** We concur. The SEC currently performs reviews of [REDACTED]  
[REDACTED] but a related procedure has not been fully documented. The SEC will develop procedures for performing risk-based reviews of [REDACTED] which will document the frequency and type of reviews. Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**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 #4: Data Protection and Privacy**

The *FY 2020 IG FISMA Reporting Metrics*, in alignment with the NIST Cybersecurity Framework, require agencies to manage information and records (data) consistent with the organization's risk strategy to protect the confidentiality,<sup>10</sup> integrity, and availability of information. In pursuit of its mission to protect investors, the SEC collects sensitive, non-public information that may include Personally Identifiable Information (PII). The collection of sensitive PII 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 Federal 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.

Kearney assessed the SEC's data protection and privacy program and determined that the program's assessed maturity level is Level 3: *Consistently Implemented*, meaning the SEC formalized and consistently implemented privacy policies, procedures, and strategies for data protection and privacy, but quantitative and qualitative effectiveness measures were lacking. While the agency continued to make improvements, the SEC's assessed maturity remained at Level 3: *Consistently Implemented* between FY 2019 and FY 2020, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

**Prior-Year Findings:** Specifically, in the FY 2018 FISMA evaluation, Kearney determined that the SEC did not:

- Implement security controls to protect [REDACTED]

Specifically, in the FY 2019 FISMA evaluation, Kearney determined that the SEC did not:

- Determine the need for privacy official signoff on the Privacy Analysis Worksheet and Privacy Impact Assessment prior to system go-live as part of the SEC's change management processes; and perform an assessment of the status of existing systems' Privacy Analysis Worksheets and Privacy Impact Assessments to confirm the SEC has publically posted the required information in accordance with Section 208 of the E-Government Act.

---

<sup>10</sup> According to 44 United States Code Section 3552 (b) (3) (B), confidentiality is defined as preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Similarly, Kearney determined that many of the weaknesses with the SEC's Data Protection and Privacy program identified during the FY 2018 FISMA evaluation remained present in FY 2020, as listed below:

- [REDACTED]
- The SEC did not publically post 1 out of the 3 (33.3%) Privacy Impact Assessments for the applicable sampled systems.

These control weaknesses occurred for a variety of different reasons. While the SEC prioritized the [REDACTED]

[REDACTED] In addition, OIT stated that, while the agency assessed the need for privacy official sign-off on the Privacy Analysis Worksheet and Privacy Impact Assessment prior to system go-live as part of the SEC's lifecycle processes, the SEC had not yet completed its corrective actions to perform an assessment of the status of existing systems' Privacy Analysis Worksheets and Privacy Impact Assessments to confirm the SEC has publically posted the required information in accordance with Section 208 of the E-Government Act.

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](#).

**Current-Year Findings:** Kearney has identified additional opportunities for the agency to mature its Data Protection and Privacy program. See the findings detailed below, as well as **Other Matters of Interest**.

In addition to the prior-year findings, Kearney identified new weaknesses related to [REDACTED] and monitoring of privacy controls.

[REDACTED] The *FY 2020 IG FISMA Reporting Metrics* require agencies [REDACTED]

Further, NIST SP 800-53, Rev. 4, [REDACTED]

Additionally, NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*, dated August 2012, states that the organization [REDACTED]

[REDACTED] OMB M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, dated May 2017, states: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**Lack of Performance Metrics for Privacy Control Monitoring:** The *FY 2020 IG FISMA Reporting Metrics* require agencies to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its privacy activities. Additionally, NIST SP 800-53, Rev. 4, Appendix J, AR-4, "Privacy Monitoring and Auditing," states that "the organization monitors and audits privacy controls and internal privacy policy." Further, OMB M-17-25 states that "in order to ensure incident response activities function as intended, it is vital that agencies utilize metrics and evaluation criteria to assess their programs as part of an effort to continually improve response performance. These efforts can help to improve the efficacy with which the agency is able to lessen the impact of incidents."

The SEC has not formally documented qualitative and quantitative metrics related to privacy and information assurance activities.

This occurred, in part, because the SEC did not integrate its privacy controls into its ISCM Strategy.

Without proper monitoring of privacy controls, the SEC is vulnerable to the potential weakening of its privacy controls. Additionally, without capturing qualitative and quantitative metrics, the SEC is unable to make improvements to its privacy and information assurance processes as necessary.

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

To mature the U.S. Securities and Exchange Commission's Data Protection and Privacy program, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology continue to work to close prior-year recommendations. See [APPENDIX II: OPEN FISMA RECOMMENDATIONS](#).

Additionally, Kearney & Company, P.C. recommends that the U.S. Securities and Exchange Commission's Office of Information Technology:

**Recommendation 4:** Develop and document a strategy to monitor privacy controls and collect qualitative and quantitative metrics to measure the effectiveness of the U.S. Securities and



Exchange Commission's privacy and information assurance activities and improvements, as appropriate.

**Management's Response:** We concur. OIT Security, Privacy and Information Assurance Branch (the Branch), has developed policies to ensure privacy controls are effectively monitored. The Branch will review and update these policies to ensure that the SEC's strategy to monitor these controls is effective. In addition, the Branch will develop and document qualitative and quantitative metrics and identify the methodology to collecting these metrics to measure the effectiveness of SEC's privacy and information assurance activities. Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**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 5:** Integrate privacy control monitoring practices into the U.S. Securities and Exchange Commission's Information Security Continuous Monitoring Strategy.

**Management's Response:** We concur. OIT Security, Privacy and Information Assurance Branch (the Branch), will align and integrate the privacy continuous monitoring strategy as revised under Recommendation 4 above with the SEC's Information Continuous Monitoring Controls Strategy. In fiscal year 2021, the Branch will identify which controls or continuous monitoring activities may be integrated into the Information Continuous Monitoring Strategy. Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**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 #5: Security Training

FISMA requires agencies to establish an information security program that includes security awareness training.<sup>11</sup> 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*, dated August 2017, 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 800-50, *Building an Information Technology Security Awareness and Training Program*, dated October 2003, 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 great risk because the security of agency resources is as much a human issue as it is a technology concern. Lastly, NIST SP 800-53, Rev. 4, (AT-3), "Role-Based 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 assessed maturity level is Level 2: *Defined*, meaning the SEC formalized and documented security training policies, procedures, and strategies, but did not consistently implement them. While the agency continued to make improvements, the SEC's assessed maturity remained at Level 2: *Defined* between FYs 2019 and 2020, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

**Prior-Year Findings:** Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Ensure that individuals with significant security responsibilities received specialized security training before accessing SEC information systems or performing assigned duties.

Similarly, Kearney determined the weaknesses with the SEC's Security Training program identified during the FY 2017 FISMA audit remained present in FY 2020, as listed below:

- While the SEC has defined individuals with significant security responsibilities, the agency did not define a process to assign specialized security training courses to SEC personnel or disseminate training courses for those individuals with significant security responsibilities.

<sup>11</sup> 44 United States Code Section 3554 (a) (4)

Kearney identified the reasons for the above control weakness. While the SEC has completed specialized security training course development, the agency has not yet assigned the courses to the appropriate individuals. OIT stated that the agency was in the process of defining a process to assign specialized security training courses to SEC personnel with significant security responsibilities during FY 2020.

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](#).

**Current-Year Findings:** Kearney has identified additional opportunities for the agency to mature its Security Training program. See the findings detailed below for additional opportunities.

In addition to the prior-year findings, Kearney identified a new weakness regarding the integration of its knowledge, skills, and abilities assessments with its security training strategy.

**Separation between Knowledge, Skills, and Abilities Assessments and Security Training Strategy:**

The *FY 2020 FISMA IG Reporting Metrics* requires organizations to conduct an assessment of the knowledge, skills, and abilities of its workforce, as well as ensure the assessment serves as a key input to updating the organization's awareness and training strategy. NIST SP 800-50, *Building an Information Technology Security and Awareness Training Program*, dated October 2003, states that, as part of one of the four critical steps in the lifecycle of an IT security awareness and training program, an agency-wide needs assessment, in the form of an assessment of knowledge, skills, and abilities, is conducted and a training strategy is developed and approved. Additionally, formal evaluation and feedback mechanisms are critical components of any security awareness program, and surveys and evaluation forms, in the form of assessments of knowledge, skills, and abilities, serve as mechanisms that can be used to update the awareness and training program plan.

While the SEC performed an assessment of knowledge, skills, and abilities across OIT in FY 2019 in accordance with agency policy, the assessment did not serve as a key input to updating the SEC's security awareness and training strategy in FY 2020.

This occurred, in part, because an effort was launched in FY 2020 to roll out new learning plans which better incorporate skills analysis and training gaps.

Without incorporating evaluation and feedback into the SEC's awareness and training strategy through assessments of knowledge, skills, and abilities, continuous improvement cannot occur. Further, the agency cannot address shifting training needs as new skills and capabilities become necessary in order to respond to new architectural and technology changes.

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

To mature the U.S. Securities and Exchange Commission's Security Training program, Kearney & Company, P.C. recommends that the Office of Information Technology continue to work to close prior-year recommendations. See [APPENDIX II: OPEN FISMA RECOMMENDATIONS](#).

Additionally, Kearney & Company, P.C. recommends that the Office of Human Resources and Office of Information Technology:

**Recommendation 6:** Define and implement a process to incorporate results from the assessments of knowledge, skills, and abilities into the security training strategy.

**Management's Response:** We concur. Based on the results from the most recent competency assessment, the Office of Human resources (OHR) will work with the Office of Information Technology (OIT) to identify approaches to address these gaps, including specialized training and/or hiring actions. OIT and/or OHR will monitor progress via the quarterly Quality of Hire Survey and post-test results of Information Technology-specific training. Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**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)**

The *FY 2020 IG FISMA Reporting Metrics* require agencies to establish an information security program that includes 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, 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*, dated 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 M-14-03, *Enhancing the Security of Federal Information and Information Systems*, dated November 2013, states that agencies were required to implement continuous monitoring of security controls as part of a phased approach through FY 2017.

Kearney assessed the SEC's ISCM program and determined that the program's assessed maturity level was Level 3: *Consistently Implemented*, meaning the SEC formalized and consistently implemented its continuous monitoring policies, procedures, and strategies for ongoing authorization, but quantitative and qualitative effectiveness measures were lacking. While the agency's assessed maturity remained the same between FYs 2019 and 2020, it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

**Prior-Year Findings:** Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- Document a comprehensive ISCM strategy or establish procedures to 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.

Specifically, in the FY 2018 FISMA evaluation, Kearney determined that the SEC did not:

- Establish a process to improve coordination and communication among the various OIT teams [REDACTED]

Similarly, Kearney determined that many of the weaknesses with the SEC's ISCM program identified during the FY 2017 FISMA audit and FY 2018 FISMA evaluation remained present in FY 2020, as listed below:

- The SEC did not update the SEC Continuous Monitoring Strategy to define qualitative and quantitative performance measures related to its continuous monitoring activities to be collected
- The SEC did not finalize its policies and procedures for a process to improve coordination and communication among the various OIT teams [REDACTED]  
[REDACTED]

These control weaknesses occurred, in part, because the ISCM processes did not include procedures for reviewing and modifying all aspects of the ISCM strategy. In addition, the SEC was gathering all the necessary information to develop a finalized Standard Operating Procedure to improve coordination among [REDACTED]

Kearney is not making any new recommendations in this domain, 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 Incident Response program.

**Domain #7: Incident Response (IR)**

FISMA requires agencies to develop, document, 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*, dated August 2012, key phases in the IR process are: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

Kearney assessed the SEC's IR program and determined that the program's assessed maturity level is Level 4: *Managed and Measurable*, meaning the SEC formalized strategies for collecting quantitative and qualitative effectiveness measures to promote continuous improvement. The agency's assessed maturity improved from Level 3: *Consistently Implemented* to Level 4: *Managed and Measurable* between FYs 2019 and 2020. While the agency's IR program is effective, the SEC did not fully implement a recommendation identified in a prior year.

**Prior-Year Findings:** Specifically, in the FY 2017 FISMA audit, the OIG determined that the SEC did not:

- 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 IR 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.

Similarly, Kearney determined that the weaknesses with the SEC's IR program identified during the FY 2017 FISMA audit remained present in FY 2020 as listed below:

- Although updates occurred to the SEC's IR policies and procedures, the updates did not include performance metrics to track and measure the effectiveness of the agency's IR program or include documented incident handlers' training requirements.

These control weaknesses occurred, in part, because while the SEC monitored training completion for incident handlers, the agency did not implement specific training requirements into its IR policies and procedures. Additionally, the SEC was in the process of developing performance measures to track and measure the effectiveness of the agency's IR program.

Kearney is not making any new recommendations in this area, as the SEC is working to address the prior-year FISMA recommendations. Additionally, Kearney determined that the SEC's IR program achieved Level 4: *Managed and Measurable* and, therefore, is effective. 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.<sup>12</sup> Because information system resources are essential to an organization's success, it is critical that systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and efficiently as possible following a disaster. NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010, states that contingency planning activities include developing the planning policy, creating contingency strategies, maintaining contingency plans, conducting Business Impact Analyses, 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 the effectiveness and organizational readiness to execute the plan. Finally, NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (CP-1), "Contingency Planning Policies and Procedures, Supplemental Information and Communications Technology (ICT) Supply Chain Risk Management Guidance," dated April 2015, states that organizations should integrate ICT supply chain concerns into the contingency planning policy.

Kearney assessed the SEC's Contingency Planning program and determined that the program's maturity level is Level 4: *Managed and Measureable*, meaning the SEC formalized strategies for collecting quantitative and qualitative effectiveness measures to promote continuous improvement. The SEC maintained this rating from FYs 2019 to 2020.

**Current-Year Findings:** Kearney has identified additional opportunities for the agency to mature its Contingency Planning program. See the findings detailed below.

Kearney identified a new weakness regarding the SEC's supply chain and contingency planning integration.

**Lack of ICT Supply Chain Integration:** The *FY 2020 IG FISMA Reporting Metrics* require agencies to integrate their ICT Supply Chain concerns and risks into its contingency planning policies and procedures. Additionally, NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (CP-1), "Contingency Planning Policy and Procedures, Supplemental ICT Supply Chain Risk Management Guidance," dated April 2015, states that "organizations should integrate ICT supply chain concerns into the contingency planning policy... [which] should cover ICT information systems and the ICT supply chain infrastructure."

Although the SEC consistently implemented information system contingency planning policies, procedures, and strategies for information system contingency planning, the SEC did not

---

<sup>12</sup> 44 United States Code Section 3554 (b) (8)

integrate ICT Supply Chain concerns and risks into its contingency planning policies and procedures.

This occurred, in part, because the SEC did not develop a supply chain risk management strategy which incorporates requirements related to the ICT Supply Chain and contingency planning program.

Without integration of the ICT Supply Chain into contingency planning policies and procedures, the SEC may be unable to effectively plan [REDACTED]

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

To mature the U.S. Securities and Exchange Commission's Contingency Planning program, Kearney & Company, P.C. recommends that the Office of Information Technology:

**Recommendation 7:** a) Identify and define the U.S. Securities and Exchange Commission's Information and Communications Technology Supply Chain risks; b) develop and define a supply chain risk management strategy which addresses the agency's Information and Communications Technology Supply Chain risks with respect to contingency planning activities; and c) incorporate the supply chain risk management strategy into contingency planning policies and procedures.

**Management's Response:** We concur. The SEC will review the guidance for Information and Communication Technology (ICT) Supply Chain risks identified in National Institute of Standards and Technology publications. The SEC will also: a) identify and define specific ICT supply chain risks, b) develop and document a Supply Chain Risk Management Strategy with the first phase of the strategy development focused on contingency planning activities, and c) implement this strategy into contingency planning policies and procedures. Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**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, the SEC improved its Risk Management and Incident Response programs. Further, there were improvements in individual metrics, including security categorizations and HVA, Plans of Action and Milestones maintenance, risk communication, access agreements, privacy awareness training, security awareness training, security training strategy, ISCM policies and procedures, incident response roles and responsibilities, incident detection, and more. These improvements occurred despite facing unique challenges presented by the ongoing COVID-19 pandemic, which included a significant increase in telework. However, despite achieving Level 4: *Managed and Measurable* in two of the eight *FY 2020 IG FISMA Reporting Metrics* areas, Kearney noted that the SEC's information security program did not meet the *FY 2020 IG FISMA Reporting Metrics*' definition of "effective" because the program's overall maturity did not reach Level 4: *Managed and Measurable*. Implementing Kearney's FY 2020, FY 2019, and FY 2018 recommendations, as well as fully addressing the remaining OIG FY 2017 recommendations, will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, non-public information 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 mature its information security program at the individual metric level, within the domains of Risk Management, Identity and Access Management, Data Protection and Privacy, and Configuration Management. These include opportunities that will increase the agency's ability to strengthen its security and privacy controls, but did not rise to the significance of a formal finding and are included for SEC management's consideration.

***Risk Management: Supply Chain Risk Strategy:*** The *FY 2020 IG FISMA Reporting Metrics* require agencies to develop an action plan and outline its processes to address the supply chain risk management strategy and related policy and procedural requirements of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act 2018. The SECURE Technology Act establishes a council of agency representatives to identify and recommend development by NIST supply chain risk management standards, guidelines, and practices for agencies to use when assessing and developing mitigation strategies to address supply chain risks. The Act further establishes requirements for executive agencies to assess the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as well as to prioritize supply chain risk assessments based on the criticality of the mission, system, component, service, or asset. NIST establishes supply chain criteria in NIST SP 800-53, Rev. 4, SA-12, "Supply Chain Protection," which establishes the requirement that organizations protect against supply chain threats to the information system, system component, or information system service by employing security safeguards as part of a comprehensive, defense-in-breadth information security strategy. NIST specifies that information systems need to be protected throughout the system development lifecycle, including design, development, manufacturing, packaging, assembly, operations, maintenance, and retirement.

Similar to FY 2019, the SEC did not establish policies and procedures regarding supply chain risk management. Further, the agency did not develop an action plan to address the supply chain risk management strategy and related policy and procedural requirements of the SECURE Technology Act.

This occurred, in part, because while the SEC has been an active participant in OMB and DHS Cybersecurity and Infrastructure Agency events that discuss the planning for agency action related to the SECURE Technology Act, the Federal Acquisition Security Council is the body formed by the SECURE Technology Act to develop the standards and procedures that agencies must follow in order to meet the mandates of the Act. As of July 2020, the Federal Acquisition Security Council had not finalized the Charter, Interim Final Rule, or Strategy documents.

Without necessary policies and procedures to address supply chain risks, the SEC may not recognize the full extent of risks involved with the agency's supply chain and, therefore, cannot address those risks, including: 1) reduce the likelihood of unauthorized modifications at each

stage in the supply chain; and 2) protect information systems and information system components, prior to taking delivery of such systems/components.

Kearney encourages the SEC to develop an action plan to help outline its processes to address the supply chain risk. Additionally, Kearney encourages the SEC to implement its risk management supply chain into its relevant policies and procedures.

**Management's Response:** The agency's response can be found in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**Identity and Access Management: Automated Tracking of Risk Designations:** The *FY 2020 IG FISMA Reporting Metrics* require that agencies employ automation to centrally document, track, and share risk designations and screening information with necessary parties. NIST SP 800-53, Rev. 4, PS-2, "Position Risk Designations," and PS-3, "Personnel Screening," requires that agencies assign a risk designation to all positions, establish screening criteria for individuals filling those positions, and review and update position risk designations. Additionally, agencies are required to screen individuals prior to authorizing access to the information system and rescreen periodically.

Similar to FY 2019, while the SEC has ensured that all personnel are assigned a risk designation, appropriately screened prior to being granted system access, and rescreened periodically, the SEC did not have an automated tool in place to centrally document, track, and share risk designations and screening information to all necessary parties to coordinate the process as consistent with its policy.

This occurred, in part, because OIT is still working to implement its new automated risk designation tool, which is set to be deployed [REDACTED]

Without an automated tool to centrally document, track, and share risk designations, the SEC must rely on manual processes to perform these actions. Risk designations are more likely to be appropriately assigned with automated controls, as automated controls are more reliable and less susceptible to human error.

Kearney encourages the SEC to continue with the implementation of an automated risk designation tool to centrally document, track, and share risk designations and screening information.

**Management's Response:** The agency's response can be found in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**Identity and Access Management: Implement ICAM Strategy:** The *FY 2020 IG FISMA Reporting Metrics* require agencies to transition to their desired or "to-be" ICAM architecture and integrate its ICAM strategy and activities with its enterprise architecture and the Federal Identity, Credential, and Access Management segment architecture. According to the Federal

Identity, Credential, and Access Management Roadmap and Implementation Guidance, Federal agencies must ensure that sufficient resources are available for ICAM activities, as well as develop transition plans that include milestones and priorities to guide agency budget requests.

The SEC developed an ICAM Strategy and set target initiatives. However, similar to FY 2019, the agency did not transition to its desired or “to-be” ICAM architecture and did not integrate its ICAM strategy and activities with its enterprise architecture and the Federal Identity, Credential, and Access Management segment architecture.

This occurred, in part, because the SEC has recently developed its ICAM strategy and is transitioning to its “to-be” ICAM architecture. The SEC’s desired ICAM strategy is a multi-year strategy that is set to be complete in FY 2024.

Without transitioning to its desired or “to-be” ICAM architecture, the SEC may not timely remediate risks associated with weak, single-factor authentication and implement initiatives to strengthen identity and access management controls.

Kearney encourages the SEC to continue implementing its ICAM strategy and meeting the remaining target initiatives defined in the strategy.

**Management’s Response:** The agency’s response can be found in [APPENDIX IV: MANAGEMENT COMMENTS](#).

**Data Protection and Privacy: Define Breach Response Metrics:** The *FY 2020 IG FISMA Reporting Metrics* require agencies to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Breach Response Plan. NIST SP 800-53, Rev. 4, Appendix J SE-2, “Privacy Incident Response,” states that the organization shall develop and implement a Privacy Incident Response Plan (Breach Response Plan) and provide an organized and effective response to privacy incidents in accordance with the organizational Breach Response Plan. Further, OMB M-17-25 states: “in order to ensure incident response activities function as intended, it is vital that agencies utilize metrics and evaluation criteria to assess their programs as part of an effort to continuously improve response performance.”

In FY 2019, the SEC performed a Table-Top Exercise (TTX) in accordance with its Breach Response Plan. The TTX measured the SEC’s ability to respond to the loss of PII in physical form. The SEC completed the TTX in accordance with its Breach Response Plan and documented lessons learned resulting from the TTX. However, similar to FY 2019, the agency did not define quantitative measures on the effectiveness of its Breach Response Plan or annual TTX to ensure that the incident response activities functioned as intended or evaluate the continuous improvement of program performance.

This occurred, in part, because the activities performed in the SEC’s most recent TTX did not include measurable activities that would facilitate quantitative and reproducible performance measures, which assist in the continuous improvement of response performance.

Without quantitative metrics for its Breach Response Plan, the agency cannot continuously make improvements to its incident response program; specifically, without quantitative metrics, the SEC cannot make changes to improve the effectiveness of the IR program and, therefore, lessen the impact assessments.

Kearney encourages the SEC to define breach response metrics to measure the effectiveness of its Breach Response Plan. These metrics should ensure that the incident response activities functioned as intended or evaluate the continuous improvement of program performance.

**Management's Response:** The agency's response can be found in [APPENDIX IV: MANAGEMENT COMMENTS](#).

***Configuration Management: Lessons Learned Documentation:*** The *FY 2020 IG FISMA Reporting Metrics* require agencies to utilize lessons learned in the implementation of its policies and procedures and to make improvements, as appropriate.

The SEC has not documented lessons learned for its configuration management policies and procedures, specifically within the Configuration Management Quality Assurance team. Additionally, the SEC did not incorporate lessons learned into change request artifacts.

This occurred, in part, because the SEC only records lessons learned for Configuration Management programs after particular events and activities occur and, therefore, is on an ad hoc basis for the Configuration Management Quality Assurance team.

Without documentation of lessons learned, the SEC is unable to make improvements to its Configuration Management program where necessary.

Kearney encourages the SEC to document lessons learned for its configuration management policies and procedures, as well as to make improvements, as necessary.

**Management's Response:** The agency's response can be found in [APPENDIX IV: MANAGEMENT COMMENTS](#).



## **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 of 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 2020 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, 2019 and August 19, 2020 and addressed the following eight domains specified in DHS's reporting instructions for FY 2020:

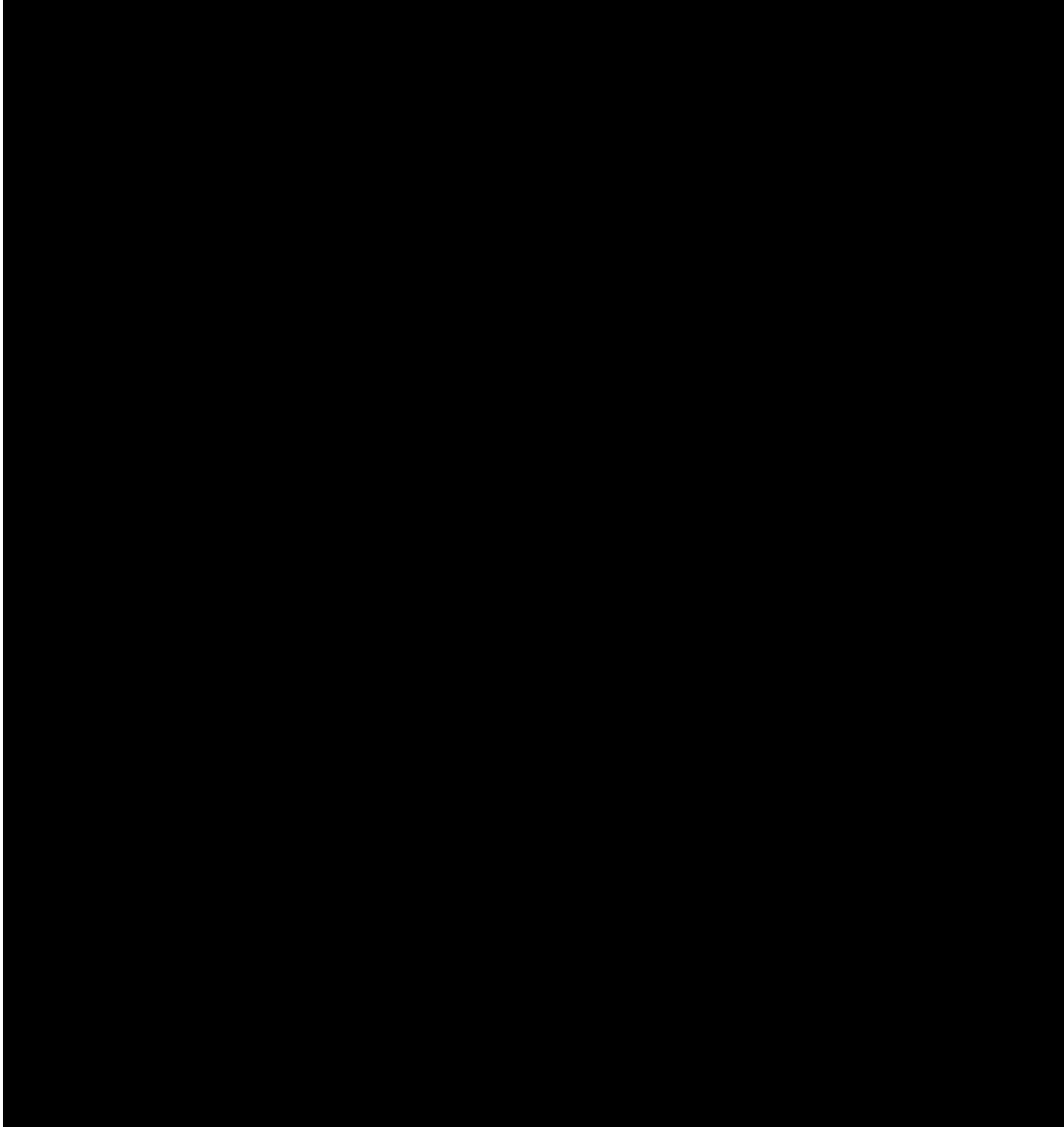
- Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning.

**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 6 of the SEC's 83 FISMA-reportable systems (about 7.2%). The sample consisted of the internally and externally hosted systems shown in *Exhibit 5*.<sup>13</sup> In addition, to address the requirements of the *FY 2020 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>13</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 6, 2020. The inventory included 83 FISMA-reportable information systems (i.e., 47 SEC-operated, and 36 contractor-operated). We selected 6 FISMA-reportable information systems, factoring in: 1) systems that were not previously tested in the prior 3 years; 2) systems that were categorized as "moderate" or "high" under Federal Information Processing Standard (FIPS) Publication (PUB) 199; and 3) systems that contain sensitive and confidential information, including PII data. We also solicited OIT's input for our sample selection.



*Exhibit 5: SEC Systems Sampled*



Source: [REDACTED] enterprise Governance, Risk, and Compliance 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, 2019 and May 31, 2020
- Were confirmed as having compromised the confidentiality, integrity, or availability of information.

According to OIT's records, 1,503 incidents occurred between October 1, 2019 and May 31, 2020. Based on our established criteria, we selected and reviewed a random sample of 28 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 2020 IG FISMA Reporting Metrics*. We interviewed key personnel, including staff from OIT's Policy and Compliance Branch and Security Engineering Branch. 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, PL 113-283
- E-Government Act of 2002, PL 107-347
- Applicable OMB guidance, including OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 2016, and OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 2015
- Various NIST SPs
- SEC Administrative Regulation 24-04, Rev. 4, *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 2020 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 Government Accountability Office's (GAO) *Assessing Data Reliability* (GAO-20-283G, December 2019) states reliability of data means that data are applicable for audit purpose and are sufficiently complete and accurate. Data primarily pertains to information that is entered, processed, or maintained in a data system and is generally organized in, or derived from, structured computer files.

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 enterprise Governance, Risk, and Compliance tool as a data source for obtaining documentation and reports related to the sampled systems and FISMA-reportable information systems inventory. We also used the SEC's training management system. Kearney performed data reliability, completeness, and accuracy testing, in part, by comparing computer-processed information to testimonial evidence obtained from Information System 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:** As of October 1, 2020, the SEC also closed 11 of 20 recommendations from the FY 2017 FISMA audit,<sup>14</sup> dated March 30, 2018, 5 of 11 recommendations from Kearney's FY 2018 FISMA evaluation,<sup>15</sup> and 1 of 9 recommendations from Kearney's FY 2019 FISMA evaluation.<sup>16</sup> 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.

SEC OIG audit and evaluation reports, including the FY 2017, FY 2018, and FY 2019 FISMA reports, can be accessed at: <https://www.sec.gov/oig>.

---

<sup>14</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>15</sup> U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security*; December 12, 2018.

<sup>16</sup> U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security Act*; December 18, 2019

## APPENDIX II: OPEN FISMA RECOMMENDATIONS

*Exhibit 6* lists all FISMA recommendations that remain open from prior FISMA audits as of September 30, 2020.

*Exhibit 6: Open FISMA Recommendations*

Domain	Open Recommendations
<b>FY 2017</b>	
Risk Management (Identify)	<b>Recommendation 3:</b> 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, and [REDACTED]
	<b>Recommendation 5:</b> 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 ensure information technology initiatives undergo an enterprise architecture compliance review before funding.
	<b>Recommendation 7:</b> 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 information technology contracts (including those we reviewed) to ensure the contracts include specific contracting language, such as information security and privacy requirements, material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information; and b) define and implement a process to ensure that future acquisitions of information technology services and products include such provisions.
Configuration Management (Protect)	<b>Recommendation 8:</b> Develop, review, and approve secure baselines for all systems included in the SEC's [REDACTED]
	<b>Recommendation 9:</b> Define and implement a process, including roles and responsibilities, to routinely: a) [REDACTED] b) perform [REDACTED] of all devices within the agency's network; and c) document, track, and address the [REDACTED] including those issues and vulnerabilities identified as unmitigated at the time of our audit.
Identity and Access Management	<b>Recommendation 12:</b> [REDACTED]

Domain	Open Recommendations
(Protect)	
Security Training (Protect)	<b>Recommendation 15:</b> 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.
Information Security Continuous Monitoring (Detect)	<b>Recommendation 16:</b> 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.
Incident Response (Respond)	<b>Recommendation 17:</b> 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.
<b>FY 2018</b>	
Configuration Management (Protect)	<b>Recommendation 1:</b> Update configuration management procedures to require that [REDACTED] are approved.
	<b>Recommendation 2:</b> Update configuration management procedures to require [REDACTED]
Data Protection and Privacy (Protect)	<b>Recommendation 3:</b> Complete initiatives to implement an [REDACTED]
	<b>Recommendation 4:</b> Complete initiatives to implement [REDACTED]
Information Security Continuous Monitoring (Detect)	<b>Recommendation 8:</b> [REDACTED]
	<b>Recommendation 9:</b> Establish a process to improve coordination and communication among the various Office of Information Technology teams [REDACTED]

Domain	Open Recommendations
<b>FY 2019</b>	
Risk Management (Identify)	<b>Recommendation 1:</b> a) Develop and document a formal process to maintain a comprehensive inventory of information systems, including a process to review and update the inventory on a periodic basis; b) Perform a review of Federal Information Systems Modernization Act of 2014-reportable systems to ensure all systems have a documented system categorization, with appropriate justification in accordance with National Institute of Standards and Technology Special Publication 800-60 Volume 1 and Federal Information Processing Standards Publication 199; and c) Implement monitoring procedures to validate that security categorizations are consistent with U.S. Securities and Exchange Commission guidance.
	<b>Recommendation 2:</b> Complete all relevant components of the [REDACTED] including [REDACTED] expiration and review date, according to [REDACTED]
	<b>Recommendation 3:</b> Define and communicate Information System Owner and Information System Security Officer roles and responsibilities.
	<b>Recommendation 4:</b> Develop and document a [REDACTED]
	<b>Recommendation 5:</b> a) Develop a methodology to demonstrate the control assignments from National Institute of Standards and Technology Special Publication 800-53, Revision 4, including control tailoring and inheritance; and b) Update the Securities and Exchange Commission's System Security Plan templates to ensure control tailoring justification corresponds to the methodology covered in part a).
Identity and Access Management (Protect)	<b>Recommendation 6:</b> Perform a formal risk assessment to determine the population of users that should be formally recertified and update procedures to document how the new recertification process should be carried out given the volume of U.S. Securities and Exchange Commission [REDACTED] users.
	<b>Recommendation 7:</b> Develop and document a formal process to either prevent or detect [REDACTED] as well as perform a formal review for [REDACTED] in accordance with U.S. Securities and Exchange Commission [REDACTED]
Data Protection and Privacy (Protect)	<b>Recommendation 8:</b> a) Determine the need for privacy official signoff on the Privacy Analysis Worksheet and Privacy Impact Assessment prior to system go-live as part of the SEC's change management processes; and b) Perform an assessment of the status of existing systems' Privacy Analysis Worksheets and Privacy Impact Assessments to confirm the Securities and Exchange

Domain	Open Recommendations
	Commission has publically posted the required information in accordance with Section 208 of the E-Government Act.

*Source: Kearney-generated based on OIG analysis of open and closed recommendations from SEC OIG Reports No. 546, No. 552, and No. 558*

### **APPENDIX III: SUMMARY OF ASSESSED FISMA RATINGS, FY 2019 & FY 2020**

The table below lists the individual *FY 2020 IG FISMA Reporting Metrics* metric ratings for the SEC in FYs 2019 and 2020, as well as the determination of effective or not effective for each metric in FY 2020. Individual metrics are colored to highlight where the SEC improved or regressed between FYs 2019 and 2020. See the key below.

#### ***Exhibit 7: Summary of Assessed FISMA Ratings between FY 2019 and FY 2020***

Red: Indicates the assessed rating went down from FY 2019 to FY 2020

Green: Indicates the assessed rating went up from FY 2019 to FY 2020

	Domain	#	Metric Title	2019 Assessed Rating	2020 Assessed Rating	2020 Effective/Not Effective
<b>Identify</b>	<b>Risk Management (RM)</b>	1	Inventory of Information Systems and System Interconnections	Defined	Defined	Not Effective
		2	Inventory of Hardware Assets	Consistently Implemented	Consistently Implemented	Not Effective
		3	Inventory of Software Assets	Ad Hoc	Ad Hoc	Not Effective
		4	Security Categorization and HVAs	Defined	Managed and Measurable	Effective
		5	RM Policies, Procedure, Strategy	Defined	Defined	Not Effective
		6	Information Security Architecture	Consistently Implemented	Defined	Not Effective
		7	RM Roles and Responsibilities	Defined	Defined	Not Effective
		8	Plans of Action and Milestones Maintenance	Defined	Consistently Implemented	Not Effective
		9	Risk Assessments	Defined	Defined	Not Effective
		10	Risk Communication	Defined	Managed and Measurable	Effective
		11	Risk Mitigation of Contractor Systems	Defined	Managed and Measurable	Effective
		12	Enterprise-Wide View of Risks	Consistently Implemented	Managed and Measurable	Effective
	<b>Overall</b>	<b>13</b>	<b>Assessed Conclusion</b>	<b>Defined</b>	<b>Consistently Implemented</b>	<b>Not Effective</b>
<b>Protect</b>	<b>Configuration Management (CM)</b>	14	CM Roles and Responsibilities	Defined	Defined	Not Effective
		15	Enterprise-Wide CM Plan	Defined	Defined	Not Effective
		16	CM Policies and Procedures	Defined	Defined	Not Effective
		17	Baseline Configurations	Defined	Defined	Not Effective
		18	Configuration Settings	Defined	Defined	Not Effective
		19	Flaw Remediation	Defined	Defined	Not Effective



	Domain	#	Metric Title	2019 Assessed Rating	2020 Assessed Rating	2020 Effective/Not Effective
		20	Trusted Internet Connection Adoption	Consistently Implemented	Defined	Not Effective
		21	Configuration Change Control	Defined	Defined	Not Effective
	<b>Overall</b>	<b>22</b>	<b>Assessed Conclusion</b>	<b>Defined</b>	<b>Defined</b>	<b>Not Effective</b>
	Identity and Access Management (IA)	23	IA Roles and Responsibilities	Defined	Consistently Implemented	Not Effective
		24	IA Strategy	Consistently Implemented	Consistently Implemented	Not Effective
		25	IA Policies and Procedures	Defined	Defined	Not Effective
		26	Personnel Risk Designations	Consistently Implemented	Consistently Implemented	Not Effective
		27	Access Agreements	Managed and Measureable	Optimized	Effective
		28	Strong Authentication – Non-Privileged	Defined	Defined	Not Effective
		29	Strong Authentication – Privileged	Defined	Defined	Not Effective
		30	Privileged Account Management	Defined	Defined	Not Effective
		31	Remote Access Configurations	Defined	Defined	Not Effective
	<b>Overall</b>	<b>32</b>	<b>Assessed Conclusion</b>	<b>Defined</b>	<b>Defined</b>	<b>Not Effective</b>
	Data Protection and Privacy (DPP)	33	Privacy Program	Consistently Implemented	Consistently Implemented	Not Effective
		34	Protection of PII and Sensitive Data	Defined	Defined	Not Effective
		35	Data Exfiltration Prevention	Consistently Implemented	Consistently Implemented	Not Effective
		36	Data Breach Response Plan	Consistently Implemented	Consistently Implemented	Not Effective
		37	Privacy Awareness Training	Managed and Measurable	Optimized	Effective
	<b>Overall</b>	<b>38</b>	<b>Assessed Conclusion</b>	<b>Consistently Implemented</b>	<b>Consistently Implemented</b>	<b>Not Effective</b>
	Security Training (ST)	39	ST Roles and Responsibilities	Defined	Defined	Not Effective
		40	Assessment of Cybersecurity Workforce	Defined	Defined	Not Effective
		41	ST Strategy	Ad Hoc	Defined	Not Effective
		42	ST Policies and Procedures	Ad Hoc	Defined	Not Effective
		43	Security Awareness Training	Managed and Measureable	Optimized	Effective
		44	Specialized Security Training	Ad Hoc	Ad Hoc	Not Effective

	Domain	#	Metric Title	2019 Assessed Rating	2020 Assessed Rating	2020 Effective/Not Effective
	<b>Overall</b>	<b>45</b>	<b>Assessed Conclusion</b>	<b>Defined</b>	<b>Defined</b>	<b>Not Effective</b>
<b>Detect</b>	<b>ISCM</b>	46	ISCM Strategy	Consistently Implemented	Consistently Implemented	Not Effective
		47	ISCM Policies and Procedures	Defined	Consistently Implemented	Not Effective
		48	ISCM Roles and Responsibilities	Defined	Defined	Not Effective
		49	Ongoing Assessments	Consistently Implemented	Consistently Implemented	Not Effective
		50	ISCM Performance Measures	Managed and Measurable	Managed and Measurable	Effective
	<b>Overall</b>	<b>51</b>	<b>Assessed Conclusion</b>	<b>Consistently Implemented</b>	<b>Consistently Implemented</b>	<b>Not Effective</b>
<b>Respond</b>	<b>Incident Response (IR)</b>	52	IR Policies and Procedures	Defined	Defined	Not Effective
		53	IR Roles and Responsibilities	Defined	Consistently Implemented	Not Effective
		54	Incident Detection and Analysis	Consistently Implemented	Managed and Measurable	Effective
		55	IR Handling Processes	Optimized	Optimized	Effective
		56	Sharing IR Information	Defined	Consistently Implemented	Not Effective
		57	Collaboration with DHS and Other Parties	Managed and Measurable	Managed and Measurable	Effective
		58	IR Technologies Used	Managed and Measurable	Managed and Measurable	Effective
	<b>Overall</b>	<b>59</b>	<b>Assessed Conclusion</b>	<b>Consistently Implemented</b>	<b>Managed and Measurable</b>	<b>Effective</b>
<b>Recover</b>	<b>Contingency Planning (CP)</b>	60	CP Roles and Responsibilities	Consistently Implemented	Consistently Implemented	Not Effective
		61	CP Policies, Procedures, and Strategies	Consistently Implemented	Consistently Implemented	Not Effective
		62	Business Impact Analysis	Consistently Implemented	Consistently Implemented	Effective
		63	Maintain Information Systems CPs	Managed and Measurable	Managed and Measurable	Effective
		64	System CP Testing/ Exercises	Managed and Measurable	Consistently Implemented	Not Effective
		65	Information System Backup and Storage	Consistently Implemented	Consistently Implemented	Effective
		66	Planning and Performance of Recovery Activities	Managed and Measurable	Managed and Measurable	Effective
	<b>Overall</b>	<b>67</b>	<b>Assessed Conclusion</b>	<b>Managed and Measurable</b>	<b>Managed and Measurable</b>	<b>Effective</b>

Source: Kearney-generated based on FY 2019 and FY 2020 SEC CyberScope results

## **APPENDIX IV: MANAGEMENT COMMENTS**

### **MEMORANDUM**

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

From: Kenneth Johnson, Chief Operating Officer **KENNETH JOHNSON** Digitally signed by KENNETH JOHNSON  
Date: 2020.12.15 16:16:26  
+05'00'

Date: December 15, 2020

Subject: Management Response to Draft OIG Report, *"Fiscal Year 2020 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014"*

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) draft report on the Securities and Exchange Commission's (SEC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year (FY) 2020. The report evaluates the SEC's Information Security Program in accordance with the FY 2020 Inspector General FISMA Reporting Metrics,<sup>1</sup> which are designed to assess the maturity levels of controls across the five functional areas of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF)<sup>2</sup>.

I am pleased your report found the SEC's information security program has improved since FY 2019. However, more work remains to be done. Your report contains seven recommendations, with which we concur. More details on management's responses to these recommendations, as well as the Other Matters of Interest cited in your report, are found in Appendix 1.

The agency will continue to prioritize efforts to improve its security posture and make its information systems more robust and resilient. During FY 2020, SEC staff closed 17 OIG information technology-related recommendations and two Government Accountability Office (GAO) recommendations<sup>3</sup>. The Office of Information Technology (OIT) facilitates regular status updates to me and other members of the leadership team to ensure that continued progress is made towards addressing current and prior year audit recommendations. During FY21, agency staff aim to continue our progress closing outstanding OIG and GAO recommendations.

<sup>1</sup> U.S. Department of Homeland Security, [FY 2020 Inspector General Federal Information Security Modernization Act of 2014 \(FISMA\) Reporting Metrics](#), April 17, 2020.

<sup>2</sup> National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018

<sup>3</sup> For reference, during FY19, SEC staff closed 28 OIG IT-related recommendations and three GAO recommendations

We appreciate the professionalism and courtesies provided by the OIG and the staff of its contractor for this independent evaluation, Kearney and Company (Kearney) during this audit, and we look forward to working with your office to address the areas noted in your report.

Attachments: Appendix 1: Management Responses to Recommendations and Other Matters of Interest

cc: Dave Bottom, Chief Information Officer, Office of Information Technology  
Vance Cathell, Director, Office of Acquisitions  
Jamey McNamara, Chief Human Capital Officer, Office of Human Resources  
Barry Walters, Director, Office of Support Services

**Appendix 1: Management Responses to  
Recommendations and Other Matters of Interest**

Below, we have outlined the steps we have already taken or intend to take to mature our program in each area.

**Recommendation 1:** Develop and document a) Agency requirements for applying security and operating system updates to mobile devices in an organizationally defined timeframe; [REDACTED]

[REDACTED]

**Response:** We concur. The SEC has begun improving its mobile device program, in accordance with the OIG's Report 562, *Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services*. [REDACTED]

[REDACTED] We will ensure the [REDACTED]  
[REDACTED] completed will fulfill these recommendations from both reports. We also will develop and document [REDACTED]

**Recommendation 2:** Develop and document a process to consistently [REDACTED]

[REDACTED]

**Response:** We concur. The SEC currently maintains an inventory of network connections, [REDACTED]

[REDACTED] including the details listed in the recommendation.

**Recommendation 3:** Develop and document processes for performing risk-based reviews [REDACTED]  
[REDACTED] on an organizationally defined frequency.

**Response:** We concur. The SEC currently performs reviews of [REDACTED] but a related procedure has not been fully documented. SEC will develop procedures for performing risk-based reviews of [REDACTED] and the procedures will document the frequency and type of reviews.

**Recommendation 4:** Develop and document a strategy to monitor privacy controls and collect qualitative and quantitative metrics to measure the effectiveness of the SEC's privacy and information assurance activities and improvements, as appropriate.

**Response:** We concur. OIT Security, Privacy and Information Assurance Branch, has developed policies 24-08-CMS-01, Privacy Continuous Monitoring Strategy, and 24-08-06-03-PM Privacy Controls Manual to ensure privacy controls are effectively monitored. The Branch will review and update these policies to ensure that the SEC's strategy to monitor these controls are effective. In addition, the Branch will develop and document qualitative and quantitative metrics and identify the methodology to collecting these metrics to measure the effectiveness of SEC's privacy and information assurance activities.

**Recommendation 5:** Integrate privacy control monitoring practices into the SEC's Information Continuous Monitoring Controls Strategy.

**Response:** We concur. OIT Security, Privacy and Information Assurance Branch, will align and integrate the privacy continuous monitoring strategy as revised under Recommendation 4 above with the SEC's Information Continuous Monitoring Controls Strategy. In FY21, the Branch will conduct a gap analysis to identify which controls or continuous monitoring activities may be integrated into the Information Continuous Monitoring Strategy.

**Recommendation 6:** Define and implement a process to incorporate results from the assessments of knowledge, skills, and abilities into the security training strategy.

**Response:** We concur. The results from the most recent competency assessment indicated improvements are needed in several core and technical skill areas including technical communication, customer support, information systems/network security, infrastructure design, and software & systems integration and testing. OHR will work with OIT to identify approaches to address these gaps, including specialized training and/or hiring actions. OIT/OHR will monitor progress via the quarterly Quality of Hire Survey and post-test results of IT-specific training.

**Recommendation 7:** a) Identify and define the SEC's Information and Communications Technology Supply Chain risks; b) develop and define a supply chain risk management strategy which addresses the agency's Information and Communications Technology Supply Chain risks with respect to contingency planning activities; and c) incorporate the supply chain risk management strategy into contingency planning policies and procedures.

**Response:** We concur. The SEC will review the control overlay for Information and Communication Technology (ICT) Supply Chain risks identified in NIST SP 800-161 for the Contingency Planning (CP) family of controls as well as the new Supply Chain control family released as part of Revision 5 (September 2020) to NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*. The SEC will

also: a) identify and define specific ICT supply chain risks, b) develop and document a Supply Chain Risk Management Strategy (SCRMS) with the first phase of the strategy development focused on contingency planning activities, and c) implement this strategy into contingency planning policies and procedures.

Although this finding did not result in a new recommendation, we would like to provide additional context with respect to the discussion on page 10 on configuration management. The report states: "Additionally, the SEC did not [REDACTED]"

[REDACTED] As we have previously made you aware, we would like to clarify that the data cited in this section is related to [REDACTED]. The identified [REDACTED] are based on [REDACTED] do not use [REDACTED] and are not high risk vulnerabilities. When a [REDACTED] identifies a [REDACTED] the report output [REDACTED] indicating that [REDACTED] This means all [REDACTED]

[REDACTED] therefore, we do not believe that this is an accurate representation of the state of SEC's [REDACTED] program. OIT staff review [REDACTED] as part of its configuration management program, and ensured its [REDACTED] are up to date to accurately validate our established configuration baselines.

*Other Matters of Interest*

With regards to the Other Matters of Interest identified in the OIG report, the SEC appreciates the information and input provided by the auditor in this section. We are committed to working towards improvement in these areas, and believe that the efforts underway and soon to be completed will further support achieving higher maturity ratings in future audits.

**Develop a Supply Chain Risk Strategy:** Kearney encourages the SEC to develop an action plan to help outline its processes to address the supply chain risk. Additionally, Kearney encourages the SEC to implement its risk management supply chain into its relevant policies and procedures.

**Response:** The SEC continues to follow the progress made by the Federal Acquisition Security Council (FASC), the body created by the SECURE Technology Act to promulgate the standards, guidance and practices for supply chain risk management. SEC will develop an action plan to outline processes to address supply chain risk and [REDACTED]

As a result of management's response, we modified the report language on Page 10, within Domain #2: Configuration Management to state that [REDACTED] as opposed to the previous language of [REDACTED]

where appropriate, create new policies or update existing policies and procedures. The action plan will inform SEC's development of a Supply Chain Risk Management Strategy (SCRMS), with the action plan being required to meet Defined (Level 2) rating in Risk Management Metric 5 and the Strategy being required to meet Consistently Implemented (Level 3).

**Implement an Automated Risk Designation Tool:** Kearney encourages the SEC to continue with the implementation of an automated risk designation tool to centrally document, track, and share risk designations and screening information.

**Response:** The SEC's Office of Security Services, Personnel Security Operations (PSO) office is required, in accordance with Federal requirements,<sup>5</sup> to establish the risk and sensitivity level of all positions within the SEC and utilize the Defense Counterintelligence and Security Agency (DCSA) Automated Position Designation Tool (PDT) to arrive at all risk and sensitivity designations. At the SEC, the PDT has been utilized since 2012 to designate the risk and sensitivity level of all new SEC positions. The process begins once OHR establishes a position, which is immediately sent to PSO for assessment via the PDT. The PDT is automated tool used by all federal agencies, which provides definitive results for sensitivity level. Those results are shared with the necessary parties upon receipt.

PSO maintains the output of results of the PDT in a library on a shared network drive that may be accessed only by individuals in PSO. In addition, PSO maintains an Excel spreadsheet that serves as the automated record which centrally documents, tracks, and is available to share risk designations and screening information with necessary parties.

PSO plans to continue using the PDT as mandated by DCSA and as the federal community moves to further automation, SEC will seek the opportunity to leverage those systems.

**Implement an ICAM Strategy:** Kearney encourages the SEC to continue implementing its ICAM strategy and meeting the remaining target initiatives defined in the strategy.

**Response:** The SEC will continue implementing its Identity, Credential, and Access Management (ICAM) Strategy,<sup>6</sup> and we will map the Strategy to the new requirements identified in OMB Memorandum 19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*<sup>7</sup> and identify target implementation dates.

<sup>5</sup> Parts 1400 and 731 of Title 5, Code of Federal Regulations

<sup>6</sup> SEC *Identity, Credential and Access Management (ICAM) Strategy*, February 2019

<sup>7</sup> OMB Memorandum 19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019



***Define Breach Response Metrics:*** Kearney encourages the SEC to define breach response metrics to measure the effectiveness of its Breach Response Plan. These metrics should ensure that the incident response activities functioned as intended or evaluate the continuous improvement of program performance.

**Response:** The SEC has updated its Breach Response Plan to include metrics to evaluate the effectiveness of its plan and processes. The metrics found in section 9.2 "Tracking and Documenting the Response," include qualitative and quantitative performance measures to ensure that the incident response activities function as intended and as required by OMB Memorandum M-17-12.

***Configuration Management Lessons Learned:*** Kearney encourages the SEC to document lessons learned for its configuration management policies and procedures, as well as to make improvements, as necessary.

**Response:** The OIT Governance Branch will define the frequency for conducting lessons learned sessions related to Operation Configuration Control Board and change management policies and procedures, and document the outcome of those lessons learned sessions. If areas for improvement are identified based on the lessons learned, OIT Governance Branch will define a schedule for implementing those lessons learned.

## 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 below.

---

# TO REPORT

# fraud, waste, and abuse

Involving SEC programs, operations, employees,  
or contractors

FILE A COMPLAINT ONLINE AT

[www.sec.gov/oig](http://www.sec.gov/oig)



CALL THE 24/7 TOLL-FREE OIG HOTLINE

**833-SEC-OIG1**

CONTACT US BY MAIL AT

**U.S. Securities and Exchange Commission  
Office of Inspector General  
100 F Street, N.E.  
Washington, DC 20549**

