U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014

December 18, 2019
Report No. 558

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.

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

December 18, 2019

TO: Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014*, Report No. 558

Attached is the Independent Auditor's Report on the U.S. Securities and Exchange Commission's (SEC or agency) compliance with the Federal Information Security Modernization Act for Fiscal Year 2019. We contracted with Kearney and Company, P.C., (Kearney) to conduct this independent evaluation. SEC's Office of Inspector General (OIG) monitored Kearney's work to ensure it met professional standards and contractual requirements. Kearney conducted the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

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

Kearney reported that the SEC improved aspects of the agency's information security program, such as enhancing certain information security policies and procedures, strengthening authentication mechanisms, reducing the number of critical vulnerabilities, enhancing security awareness and training processes, and continuing efforts to enhance the agency's continuous monitoring program.

However, as described in the attached report, Kearney identified opportunities for improvement in key areas and made nine 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 2019 IG FISMA Reporting Metrics*' definition of "effective."

On November 22, 2019, we provided management with a draft of Kearney' report for review and comment. In the agency's December 10, 2019 response, management concurred with

Kearney' recommendations. Kearney included management's response as Appendix II in the final 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 Projects.

Attachment

cc: Jay Clayton, Chairman
Sean Memon, Chief of Staff, Office of Chairman Clayton
Bryan Wood, Deputy Chief of Staff, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Kimberly Hamm, Chief Counsel/Senior Policy Advisor, Office of Chairman Clayton
Robert J. Jackson, Jr., Commissioner
Prashant Yerramalli, Counsel, Office of Commissioner Jackson
Hester M. Peirce, Commissioner
Jonathan Carr, Counsel, Office of Commissioner Peirce
Elad L. Roisman, Commissioner
Matthew Estabrook, Counsel, Office of Commissioner Roisman
Allison Herren Lee, Commissioner
Andrew Feller, Counsel, Office of Commissioner Lee
Robert B. Stebbins, General Counsel
John J. Nester, Director, Office of Public Affairs
Holli Heiles Pandol, Director, Office of Legislative and Intergovernmental Affairs
Gabriel Benincasa, Chief Risk Officer
Charles Riddle, Acting Director/Chief Information Officer, Office of Information Technology
Andrew Krug, Chief Information Security Officer, Office of Information Technology
Vance Cathell, Director, Office of Acquisitions
Michael Whisler, Assistant Director, Office of Acquisitions
Jamey McNamara, Chief Human Capital Officer, Office of Human Resources

Fiscal Year 2019 Independent Evaluation of the U.S. Securities and Exchange Commission's Implementation of the Federal Information Security Modernization Act of 2014

December 18, 2019

Point of Contact Phil Moore, 1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
Phil.Moore@kearneyco.com
Kearney & Company's TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14

REDACTED FOR PUBLIC RELEASE

KEARNEY&
COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

COVER LETTER

December 18, 2019

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, the *Fiscal Year 2019 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 2019 Inspector General (IG) FISMA Reporting Metrics Version 1.3* (*FY 2019 IG FISMA Reporting Metrics*), dated April 9, 2019. Kearney's methodology for the FY 2019 FISMA evaluation included testing the effectiveness of selected security controls the SEC has implemented in eight sampled information systems, including the [redacted], 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* (NIST SP 800-53, Rev. 4). The *FY 2019 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 Cybersecurity Framework Functions (i.e., Identify, Protect, Detect, Respond, and Recover). To achieve an effective level of

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

information security under the maturity model, agencies must reach Level 4: *Managed and Measurable*.

Since FY 2018, the SEC's Office of Information Technology (OIT) improved aspects of its information security program. Among other actions taken, OIT made progress in implementing information security policies and procedures to address security risks at the organizational level, creating an entity-wide Identity and Access Management strategy, enhancing its security awareness and training processes, continuing its efforts to enhance its continuous monitoring program, and improving its incident response capabilities.

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 2019 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 Information Security Continuous Monitoring and Incident Response improved one maturity level, to Level 3: *Consistently Implemented*, and Contingency Planning improved two maturity levels, to Level 4: *Managed and Measurable*. 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.

Summary of SEC FISMA Ratings

Domain	Assessed Rating By Fiscal Year (FY)	
	2018	2019
Risk Management	Level 2: *Defined*	Level 2: *Defined*
Configuration Management	Level 2: *Defined*	Level 2: *Defined*
Identity and Access Management	Level 2: *Defined*	Level 2: *Defined*
Data Protection and Privacy	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Security Training	Level 2: *Defined*	Level 2: *Defined*
Information Security Continuous Monitoring	Level 2: *Defined*	Level 3: *Consistently Implemented*
Incident Response	Level 2: *Defined*	Level 3: *Consistently Implemented*
Contingency Planning	Level 2: *Defined*	Level 4: *Managed and Measurable*

Source: Kearney & Company, P.C. (Kearney)-generated based on FYs 2018 and 2019 CyberScope Metric responses.

Our report includes nine new recommendations to strengthen the SEC's information security program. As our report highlights, opportunities exist for the SEC to improve its performance in seven of the eight IG *FY 2019 IG FISMA Reporting Metrics* areas. Significant opportunities for improvement remain in key areas such as improving [redacted], Information System Owners performing assigned responsibilities, [redacted]

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

[redacted] 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,

Kearney & Company, P.C.
December 18, 2019

TABLE OF CONTENTS

TABLE OF EXHIBITS

ABBREVIATIONS

ATO	Authorization-to-Operate
BIA	Business Impact Analysis
CAP	Corrective Action Plan
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
[redacted]	[redacted]
DHS	U.S. Department of Homeland Security
DNS	Domain Name System
EDRP	Enterprise Disaster Recovery Plan
[redacted]	[redacted]
eGRC	Enterprise Governance, Risk, and Compliance
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Modernization Act of 2014
FY	Fiscal Year
[redacted]	[redacted]
[redacted]	[redacted]
IA	Identity and Access Management
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IR	Incident Response
[redacted]	[redacted]
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
MOU	Memorandum of Understanding

NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
Cybersecurity Framework	National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity
[redacted]	[redacted]
OHR	Office of Human Resources
[redacted]	[redacted]
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PAW	Privacy Analysis Worksheet
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
[redacted]	[redacted]
P.L.	Public Law
POA&M	Plans of Action and Milestones
PUB	Publication
Rev.	Revision
[redacted]	[redacted]
SDLC	Systems Development Lifecycle
SEC or agency	U.S. Securities and Exchange Commission
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
ST	Security Training
TTX	Table-Top Exercise
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
Vol.	Volume

BACKGROUND AND OBJECTIVES

Background

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

In addition, FISMA requires Inspectors General (IG) to assess annually the effectiveness of information security programs and practices and to report the results to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). This assessment includes testing and assessing the effectiveness of information security policies, procedures, and practices, as well as a subset of information systems. In support of these requirements, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* issued to IGs guidance on FISMA reporting for fiscal year (FY) 2019.[1]

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 2019 IG FISMA Reporting Metrics*. The results of these efforts supported the Office of Inspector General's (OIG) FY 2019 CyberScope submission to OMB and DHS.[2]

As ***Exhibit 1*** illustrates, the *FY 2019 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").[3]

[1] *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.3 dated April 9, 2019 (hereafter referred to as "*FY 2019 IG FISMA Reporting Metrics*").
[2] CyberScope is the platform that Chief Information Officers (CIO), 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 31, 2019.
[3] The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, as well as provides IGs with the guidance for assessing the maturity of controls to address those risks.

Exhibit 1: Cybersecurity Framework Functions Mapped to FY 2019 IG FISMA Reporting Metrics Assessment Domains

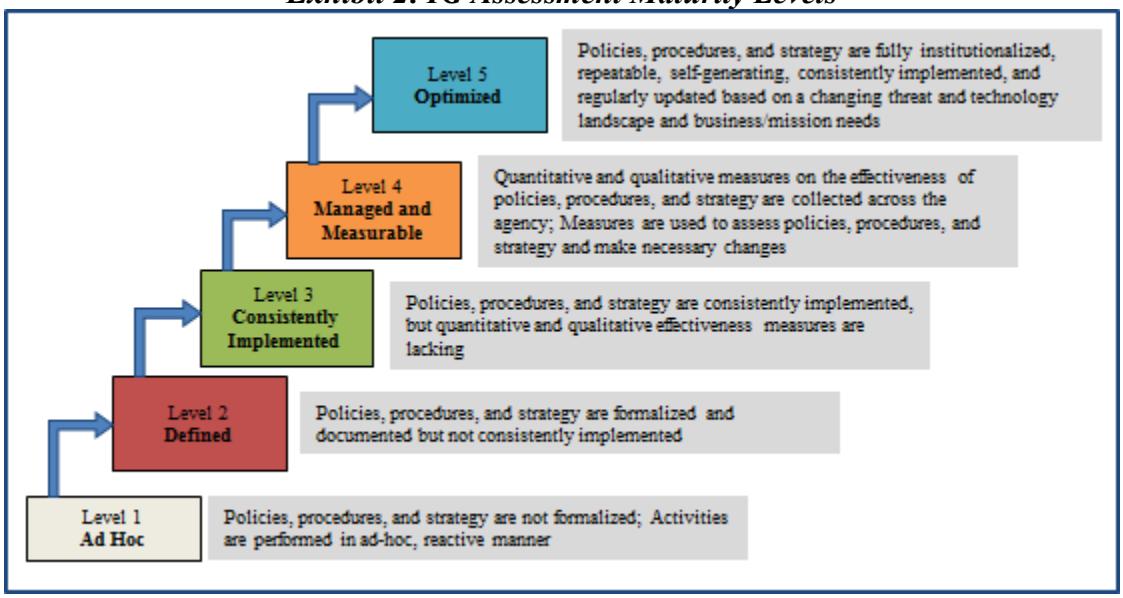
Cybersecurity Framework Functions	*FY 2019 IG FISMA Reporting Metrics* Assessment Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Source: Kearney-generated from FY 2019 IG FISMA Reporting Metrics.

Change in Metrics and Assessment Methodology: The *FYs 2015 and 2016 IG FISMA Reporting Metrics* required IGs to assess two Cybersecurity Framework functions (i.e., Detect and Respond) using a maturity model approach. In contrast, the *FY 2017 IG FISMA Reporting Metrics* required IGs to assess seven domains included in the five Cybersecurity Framework functions using a maturity model approach. In FY 2018, the *FY 2018 IG FISMA Reporting Metrics* expanded to include an eighth domain (i.e., Data Protection and Privacy). The *FY 2019 IG FISMA Reporting Metrics* remained largely stable with slight revisions to the attributes for Level 1: *Ad Hoc*, Level 2: *Defined*, Level 3: *Consistently Implemented*, and Level 4: *Managed and Measureable,* and Level 5: *Optimized*. Specifically, in FY 2019, the *FY 2019 IG FISMA Reporting Metrics* added new requirements for supply chain risk management in the Risk Management domain and for security of Domain Name System (DNS) in the Data Protection and Privacy and Identity and Access Management domains. These topics were included in accordance with the publication of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act 2018 and DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*.

As shown in ***Exhibit 2***, 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 2: IG Assessment Maturity Levels



Source: Kearney-generated graphic based on the FY 2019 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 CIO directs OIT and is responsible for ensuring compliance with applicable information security requirements. The Chief Information Security Officer, designated by the CIO, is responsible, in part, for developing, maintaining, centralizing, and monitoring ongoing adherence to the SEC's Information Security Program Plan and supporting the CIO in annually reporting on the effectiveness of the SEC's information security program.

Prior Audits and Evaluations: Prior to the start of the FY 2019 FISMA evaluation, and throughout FY 2019, the SEC closed the remaining 2 of 21 recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2016[4] (FY 2016 FISMA audit), dated March 7, 2017. As of October 1, 2019, the SEC also closed 8 of 20 recommendations from the

[4] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016*, Report No. 539; March 7, 2017 (hereafter referred to as "FY 2016 FISMA audit").

OIG's audit of the SEC's compliance with FISMA for FY 2017[5] (FY 2017 FISMA audit), dated March 30, 2018, and 2 of 11 recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2018[6] (FY 2018 FISMA evaluation), dated December 12, 2018. To close these recommendations, OIT made progress in tracking access agreements, evaluating skills of users with significant security and privacy responsibilities, documenting requirements for system interconnections, consistently performing security impact analyses, improving incident response processes, maintaining up-to-date contingency planning documentation, and performing an annual test of the agency Enterprise Disaster Recovery Plan (EDRP).

Objectives

Our overall objective was to evaluate the SEC's implementation of FISMA for FY 2019 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 2019 IG FISMA Reporting Metrics*:

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

To assess the effectiveness and maturity of security controls identified in the *FY 2019 IG FISMA Reporting Metrics*, Kearney judgmentally selected and reviewed a non-statistical sample of 8 information systems from the SEC's April 29, 2019 inventory of 80 FISMA-reportable information systems (10%). Additionally, Kearney performed other tests and assessments.

APPENDIX I: SCOPE AND METHODOLOGY describes our scope and methodology (including sampled systems), our review of internal controls and computer-processed data, and prior coverage.

[5] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017*, Report No. 546; March 30, 2018 (hereafter referred to as "FY 2017 FISMA audit").
[6] 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").

RESULTS

Domain #1: Risk Management

The *FY 2019 IG FISMA Reporting Metrics*, in accordance with the NIST Cybersecurity Framework, considers 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*, 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 2: *Defined*, meaning the SEC formalized and documented risk 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 FY 2017, FY 2018, and FY 2019, as it has not fully implemented the recommendations identified in prior years; therefore, these 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.
- Always ensure that IT contracts include certain contracting language defined by OIT.

Similarly, Kearney determined that many of the weaknesses with the SEC's Risk Management program identified during the FY 2017 FISMA audit remained present in FY 2018 and FY 2019, as listed below:

- While the SEC defined a standard taxonomy for [redacted], the agency [redacted]
- The SEC did not define or formalize a plan to address how the SEC's Information and Communications Technology supply chain will be integrated with its enterprise architecture program management.
- The SEC OIT and Office of Acquisitions have not consistently implemented a process to ensure applicable IT security clauses are included in system contracts. Specifically:
  - All four (100%) sampled systems failed to include multiple contract clauses.

- Of the four sampled systems, three required Federal Risk and Authorization Management Program (FedRAMP) clauses, and all three (100%) were lacking the specified FedRAMP clause, [redacted] *[Issues related to SEC's security requirements for Cloud systems are further discussed in the SEC OIG Report No. 556 Cloud Audit Report Dated November 7, 2019]*.

These control weaknesses occurred for a variety of different reasons. The SEC was in the process of implementing a tool to [redacted] In addition, OIT stated that the Council established by the SECURE Technology Act 2018 did not release the standards, guidance, and practices for agencies to self-assess against in accordance with the SECURE Technology Act 2018. Lastly, the SEC stated that it was in the process of attempting to update contractual language upon the exercise of option years.

Kearney is not making any new recommendations in relation to the prior-year findings noted above, as the SEC is working to address the prior-year FISMA recommendations. See APPENDIX II: OPEN FISMA RECOMMENDATIONS.

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 new weaknesses related to system inventories and categorizations, [redacted] inventories, risk management roles and responsibilities, integrated hardware management systems, and the application of the NIST SP 800-53, Revision (Rev.) 4 baseline of controls.

Insufficient Maintenance of Information System and [redacted] Inventory: FISMA requires all Federal agencies to "develop and maintain an inventory of major information systems operated by or under the control of such agency… The identification of information systems in an inventory… shall include an identification of interfaces between each such system and all other systems or networks… Such inventory shall be updated at least annually."[7] Part of maintaining an inventory of information systems includes categorizing information based upon the potential impact of loss to determine the level of security protections required. NIST SP 800-60, Volume (Vol.) 1, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, states: "An initial security categorization should occur early in the agency's system development lifecycle (SDLC)… [and] feed into security requirements identification… and other related activities." According to NIST SP 800-53, Rev. 4, the Risk Management Framework establishes the categorization process as a foundational step that leads to the selection of applicable security control baselines based on the results of that categorization.

[7] 44 United States Code (U.S.C.) Section 3505 (C)

Closely related to the maintenance of an inventory of information systems is tracking the [redacted] The SEC has defined a policy for the maintenance of [redacted] and Memoranda of Understanding (MOU), [redacted] The document states: [redacted] Further, OIT establishes in [redacted]

Based on the results of system inventory control testing, Kearney identified that the SEC did not correctly identify one of its information systems as FISMA-reportable in its information system inventory and did not have a formal process to maintain the inventory, ensuring completeness and accuracy, on a regular basis. Further, the SEC did not consistently categorize four of the eight (50%) sampled systems in accordance with NIST SP 800-60, Vol. 1, Rev. 1. Of these four systems, the agency did not document a Federal Information Processing Standards (FIPS) Publication (PUB) 199 categorization worksheet for two of the eight (25%) sampled systems, including [redacted] until July 15, 2019, subsequent to receiving a recent re-authorization of the Authorization-to-Operate (ATO). The other two (25%) systems were inconsistently categorized, where the data types defined in NIST SP 800-60, Vol.1, Rev. 1 did not support the initial categorization for [redacted] Lastly, the SEC [redacted]

This occurred, in part, because the SEC did not define and implement a process to maintain a comprehensive inventory of information systems. Further, the SEC did not follow its documented process to ensure that each system was categorized appropriately in accordance with NIST SP 800-60, Vol. 1, Rev. 1. Lastly, SEC employees were unable to [redacted] in the eGRC tool, leading to a lack of compliance with [redacted], which requires the annual review of [redacted]

Without regular and consistent inventory management (including categorization of its systems or identification of incorrect information through regular review), the SEC will be unable to appropriately align its systems with the security control baselines in accordance with NIST SP 800-60. Further, the SEC will potentially miss the impact of changes to [redacted]

Inconsistent Performance of Risk Management Roles and Responsibilities: FISMA requires all agencies to "ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control."[8]

[8] 44 U.S.C Section 3554 (a) (2)

NIST SP 800-53, Rev. 4, PL-2, *System Security Plan*, states that the organization reviews the security plan for the information system at an organization-defined frequency. Further, NIST SP 800-53, Rev. 4, CA-5, *Plans of Action and Milestones*, states that the organization develops and updates Plans of Action and Milestones (POA&M) for the information system. While these controls define the activities that must take place, NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, defines the roles responsible for these activities, as well as the roles that support the organization's overall risk management program. These roles include, but are not limited to, the Information System Owner (ISO) and Information System Security Officer (ISSO).

Responsibilities of the ISO include assistance with the development and maintenance of the System Security Plan (SSP). Additionally, the ISO informs the appropriate officials of the need to conduct the security authorization and provides the required information system access, information, and documentation to the security control assessor. Further, the ISO is responsible for ensuring compliance with security requirements and deciding who has access to the system. Meanwhile, the ISSO is responsible for ensuring the maintenance of the appropriate operational security posture for an information system and works in close collaboration with the ISO. The ISSO also often plays an active role in the monitoring of a system and its environment of operation, to include developing and updating the SSP, managing and controlling system changes, and assessing the security impact of those changes.

The SEC has not fully implemented the role of the ISSO across the agency. Instead, the agency assigned an ISO to each information system; these individuals are expected to perform ISO functions, as well as the operational and security compliance activities traditionally covered by the ISSO. However, the SEC did not ensure that ISOs consistently performed their roles and responsibilities in a timely manner, including [redacted]

OIT recognized these weaknesses in the process and developed an integrated team-based ISSO approach with the purpose of supporting current ISOs in completing the operational and security compliance tasks. However, these conditions occurred as the ISSO team was recently implemented and ISOs were not yet fully aware of this available resource to support the completion of system security responsibilities.

Without timely remediation of identified weaknesses, including control weaknesses in [redacted] could experience a loss of confidentiality, integrity, or availability.

Lack of Hardware Asset Management Systems [redacted]: To achieve Level 4: *Managed and Measurable* for hardware asset tracking activities, the *FY 2019 IG FISMA Reporting Metrics* requires agencies to ensure hardware assets connected to the network are covered by an organization-wide hardware asset management capability, and they are subject to the monitoring processes defined within the organization's ISCM strategy. NIST SP 800-53, Rev. 4, CM-8, *Information System Component Inventory*, states that the organization develops and documents an inventory of information system components, which would include hardware inventory specifications. Further, NIST SP 800-53, Rev. 4, CA-7, *Continuous Monitoring*, states that the organization develops a continuous monitoring strategy and implements a continuous monitoring program. Specifically, Control CA-7 states that this program should include the correlation and analysis of security-related information generated by assessments and monitoring, as well as response actions to address results of the analysis of security-related information.

While the SEC implemented a hardware asset inventory management system, the agency [redacted]

This occurred, in part, because the SEC implemented a hardware asset inventory that satisfied financial inventory management requirements. However, the agency [redacted]

[redacted] the SEC may [redacted] accurately and effectively, as well as take subsequent actions to address the results of that analysis.

Incomplete Evaluation of Applicable [redacted]-Impact System Controls: FISMA requires all agencies to develop and maintain "information security policies, procedures, and control techniques to address all applicable requirements including those issued [by NIST pertaining to Federal information systems]."[9] NIST SP 800-53, Rev. 4, Control PL-2, *System Security Plan*, states that the organization shall develop a security plan for the information systems that… describes the security controls in place or planned for meeting the security requirements of a system, including a rationale for the tailoring decisions. Further, NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, identifies the development of organizationally tailored control baselines to address the organizational mission or business need for specialized sets of controls to reduce risk. This guidance notes instances where an agency can appropriately add or eliminate controls to accommodate organizational requirements, while continuing to protect information commensurate with risk. Examples include unique security or privacy risks, organization-specific mission or business needs, or plans to operate in environments not addressed in the initial baselines.

[9] 44 U.S.C Section 3554 (a) (3) (C)

The SEC did not include all of the applicable NIST SP 800-53, Rev. 4 controls at the [redacted] SSPs and did not include a rationale for tailoring decisions. Specifically, of the eight systems sampled, four (50%) of the information systems classified as [redacted] excluded between [redacted] and [redacted] baseline controls in the SSP and did not include a rationale to support those decisions.

This occurred because the SEC did not effectively implement NIST SP 800-37, Rev. 2 and OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016), guidance when tailoring its SSP template. Instead of ensuring that all required NIST SP 800-53, Rev. 4 [redacted] security controls were accounted for as either common, hybrid, or system-specific, OIT stated that it relied on SEC guidance published approximately five years ago which established tailoring guidance across all major or minor systems without documenting or periodically re-evaluating that rationale.

Without the effective evaluation of its implementation of system baseline controls required at the [redacted] level, the SEC has a higher potential of control failures or continuously unmitigated weaknesses. For example, [redacted] controls and control enhancements from the [redacted] were not included in [redacted] of the 8 SSPs reviewed, relating to the inconsistent review in of [redacted] across 4 sampled systems, 3 of which were [redacted] systems.

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 and 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: 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

[redacted]

199; and c) Implement monitoring procedures to validate that security categorizations are consistent with U.S. Securities and Exchange Commission guidance.

Management's Response. Management concurred with the recommendation. The SEC is updating its existing procedures to formally require reviews for the FISMA reportable systems and security categorizations, including a review as part of the annual Information System Owner (ISO) review. Additionally, OIT will perform a comprehensive review of existing FISMA-reportable systems to validate each has a documented system categorization and correct any deficiencies. 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 2: Complete all relevant components of the [redacted], including [redacted] expiration and review date, according to [redacted]

Management's Response. Management concurred with the recommendation. The SEC will complete an analysis of existing System Security Plans to ensure the [redacted] is complete and is supported by the required documentation. 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 3: Define and communicate Information System Owner and Information System Security Officer roles and responsibilities.

Management's Response. Management concurred with the recommendation. The SEC will formally define the roles of agency Information System Owner and Information System Security Officer and communicate that information to individuals in these roles. 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 4: Develop and document a [redacted]

Management's Response. Management concurred with the recommendation. The SEC is in the process of implementing a solution for [redacted] Additionally, the agency has developed a [redacted], and has acquired a new [redacted] tool to ensure the [redacted] are applied. Once this tool is implemented, the SEC will perform analysis and data normalization [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.

Recommendation 5: 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).

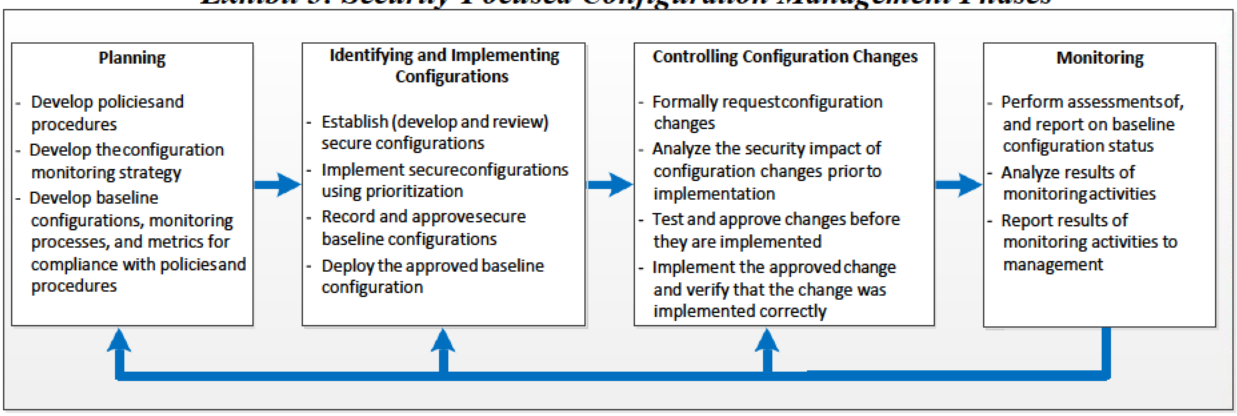
Management's Response. Management concurred with the recommendation. The SEC is developing a new methodology that will update the control mapping source documents and the SSP templates to ensure consistency and completeness. In November 2019, the SEC updated its SSP template for [redacted] to more clearly identify inherited controls, SEC program-level controls, and controls tailored for inclusion or exclusion, and will continue to update System Security Plans for all [redacted] during fiscal year 2020. 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 2019 IG FISMA Reporting Metrics*, in accordance with NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011, considers configuration management a critical 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,[11] 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. Finally, as described in ***Exhibit 3***, security-focused configuration management of information systems involves a set of activities that can be organized into the following four major phases: 1) Planning; 2) Identifying and Implementing Configurations; 3) Controlling Configuration Changes; and 4) Monitoring.

Exhibit 3: Security-Focused Configuration Management Phases



Source: 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 FY 2017, FY 2018, and FY 2019, as it has not fully implemented the recommendations identified in prior years; therefore, these conditions still exist.

[11] 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 [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 2019, as listed below:

- While the SEC has improved its approved [redacted] percentage by about 5% since the FY 2018 evaluation, there were still [redacted] pending the review and approval process. Additionally, the SEC did not define a performance measure as an acceptable target level of [redacted] across the agency.
- The SEC [redacted]
- The SEC did not consistently deploy [redacted] across the agency.
- Although the SEC reduced its number of critical vulnerabilities, the agency did not consistently follow its vulnerability management policy, which requires the [redacted]. Additionally, the SEC did not create [redacted] in accordance with its vulnerability management policy. The SEC was in process of revising the vulnerability management policy during FY 2019.
- The SEC did not update its [redacted]
- The SEC did not fully implement a [redacted]

[redacted]

[redacted]

The above weaknesses occurred because SEC management had not fully addressed management challenges identified in FY 2017 and FY 2018. During FY 2019, the SEC took steps to address previously noted weaknesses by improving its [redacted] related to vulnerability management. Identified issues related to [redacted] occurred, in part, because the SEC [redacted] Although the SEC regularly provides [redacted] to ISOs, the approach relied on information system owners to review vulnerabilities for their respective application and database servers and then determine the necessary corrective actions. Often, ISOs did not review the vulnerability management reports and [redacted] because of unawareness of their assigned responsibilities and/or competing priorities for IT contractor support. Overall, weaknesses with the SEC's vulnerability remediation process continued in FY 2019 because the agency did not include an effective oversight function to monitor vulnerability identification and flaw remediation processes and practices.

Kearney is not making any new recommendations in this area, as the SEC is working to address the prior-year FISMA recommendations. See APPENDIX II: OPEN FISMA RECOMMENDATIONS.

Domain #3: Identity and Access Management

The *FY 2019 IG FISMA Reporting Metrics*, in accordance with the NIST Cybersecurity Framework, requires 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 FY 2017, FY 2018, and FY 2019, as it has not fully implemented the recommendations identified in prior years; therefore, these conditions still exist.

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

- [redacted]
- Define processes for ensuring compliance with [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 remained present in FY 2018 and in FY 2019, as listed below:

- [redacted]

[redacted]

- The SEC has not defined a process for adding users to [redacted], nor removing them from those groups in a timely manner.
- The SEC did not define a process for reviewing monitoring reports related [redacted]

These control weaknesses occurred for a variety of reasons. Regarding the deployment of [redacted] SEC management explained that, while the agency has defined [redacted], as it did not maintain up-to-date policies and procedures for the management of these [redacted] Further, regarding [redacted] SEC management demonstrated a dashboard that [redacted], but they have not yet documented a procedure that details how [redacted] should be reviewed.

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 user access recertifications.

Inconsistent Performance of User Access Recertifications: The *FY 2019 IG FISMA Reporting Metrics* require that agencies consistently implement policies and procedures for identity, credential, and access management (ICAM), including identifier and authenticator management and identification and authentication of non-organizational users. Additionally, NIST SP 800-53, Rev. 4, AC-2, *Account Management*, requires agencies to review accounts for compliance with account management requirements on an organizationally defined basis. [redacted]

The SEC did not complete its [redacted] review of accounts for accuracy, as it did not perform a user access recertification for the [redacted] users that included reviewing [redacted] group membership.

This occurred, in part, because the SEC has not defined and implemented a process for reviewing accounts for accuracy for [redacted] group membership and accounts. Additionally,

the SEC did not consistently apply the defined [redacted] of such accounts.

Without reviewing accounts for accuracy and performing [redacted] access recertifications for the over [redacted] user accounts, including [redacted], the SEC may allow unnecessary [redacted] accounts to exist and/or these accounts to possess logical access to information where the business need no longer exists.

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 and 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 6: 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.

> **Management's Response.** Management concurred with the recommendation. OIT will update the SEC's user recertification procedures to document the formal recertification process for the [redacted]. Additionally, OIT will perform an account recertification for each group of [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.

Recommendation 7: 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].

> **Management's Response.** Management concurred with the recommendation. The SEC will a) develop and document a formal process to prevent the creation of [redacted] (b) perform a formal review of [redacted] and correct any deviations from the [redacted] and c) distribute instructions to stakeholders

involved in the [redacted] to reaffirm existing guidance and standard operating procedures regarding [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 #4: Data Protection and Privacy

The *FY 2019 IG FISMA Reporting Metrics*, in alignment with the NIST Cybersecurity Framework, requires agencies to manage information and records (data) consistent with the organization's risk strategy to protect the confidentiality,[13] 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 both Federal and commercial entities that resulted in the disclosures of sensitive PII, organizations have placed increased attention on protecting sensitive information by limiting its collection, encrypting the data at rest, and monitoring for potential exfiltration of sensitive data.

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 2018 and FY 2019, as it has not fully implemented the recommendations identified in prior years; therefore, these 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 its [redacted]
- Update procedures for the [redacted]

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 2019, as listed below:

- The SEC did not implement [redacted]

[13] According to 44 U.S.C 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.

- The SEC was in the process of updating its procedures for the [redacted], but it had not fully documented the procedure as of June 24, 2019.

These control weaknesses occurred for a variety of different reasons. While the SEC prioritized the [redacted] In addition, OIT stated that the agency was in the process of updating the SEC's procedure for [redacted] during FY 2019 as part of identified remediation activities.

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 complete and timely privacy documentation.

Limitations in Controls to Ensure Complete and Timely Privacy Documentation: According to the E-Government Act of 2002, Section 208, an agency shall conduct a Privacy Impact Assessment (PIA) and, if practicable, make the PIA publicly available through the website of the agency, publication in the Federal Register, or other means before developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form.[14]

The SEC did not complete and publish the PIA prior to the collection and maintenance of information in an identifiable form about the public for one of the eight (about 13%) sampled systems. The agency completed a Privacy Analysis Worksheet (PAW) in [redacted] which identified the need for a PIA. However, the PIA was not completed until [redacted], approximately [redacted] after the PAW was completed and the system entered production and began collecting and maintaining information in identifiable form.

This occurred, in part, because the SEC's change management processes did not have a control to prevent systems from collecting information in identifiable form without a completed and publicly posted PIA prior to entering production or timely thereafter, despite the requirement for a PIA being a documented part of the change management process. Although the Privacy Team performs activities to track the status of outstanding privacy documents for systems, at times there were further delays in completing PIAs in a timely manner which may be related to the agency lacking appropriate resources (i.e., processes, technology).

[14] Information in identifiable form is also referred to as PII.

Without completing a system's PIA prior to the collection, maintenance, and dissemination of information in identifiable form, the agency did not: 1) ensure handling conformed to applicable legal, regulatory, and policy requirements; 2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

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 and 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 8: 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 Commission has publically posted the required information in accordance with Section 208 of the E-Government Act.

> **Management's Response.** Management concurred with the recommendation. The SEC will a) update its policy to require the Senior Agency Official for Privacy to review the results of a Privacy Impact Assessment prior to authorizing the use of a system to collect, process, or store personally identifiable information; b) review the status of Privacy Assessment Worksheets and Privacy Impact Assessment documentation for existing systems to ensure that required documents are accurate and accessible for review in accordance with Section 208 of the E-Government Act; and c) based on the review, develop a timetable to correct noted deficiencies. 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.[15] Such training informs personnel, including contractors, of information security risks associated with their activities, as well as their responsibilities for complying with agency policies and procedures. NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, provides guidance on a superset of cybersecurity knowledge, skills, and abilities and tasks for each work role. The NICE Cybersecurity Workforce Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development. NIST SP 800-53, Rev. 4, (PS-6), *Access Agreements*, further requires the organization to develop and document access agreements for individuals, ensure individuals sign appropriate access agreements prior to being granted access, and individuals re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or on an organization-defined frequency. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, mandates that organizations monitor their information security training program for compliance and effectiveness and that failure to encourage IT security training puts an enterprise at 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 FY 2017, FY 2018, and FY 2019, as it has not fully implemented the recommendations identified in prior years; therefore, these conditions still exist.

Prior-Year Findings: Specifically, in the FY 2017 FISMA audit, the OIG and Kearney 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 that many of the weaknesses with the SEC's Security Training program identified during the FY 2017 FISMA audit remained present in FY 2019, as listed below:

- The SEC did not define the process for assigning specialized security training.

[15] 44 U.S.C Section 3554 (a) (4)

Kearney identified the reasons for the above control weakness. Regarding the specialized security training, OIT and the Office of Human Resources (OHR) have not documented a process for identifying each user with significant security responsibilities; therefore, OHR could not identify personnel to whom to assign specialized security training.

Kearney is not making any new recommendations in relation to the prior-year findings noted above, as the SEC is working to address the prior-year FISMA recommendations. See APPENDIX II: OPEN FISMA RECOMMENDATIONS.

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 lack of an IT Security Awareness Training Strategy.

Lack of Agency IT Security Awareness and Training Strategy: The *FY 2019 IG FISMA Reporting Metrics* require that agencies define an IT Security and Awareness Training Strategy for developing, implementing, and maintaining a security awareness and training program that is tailored to its mission and risk environment. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, describes a security awareness and training strategy as a way for the organization to develop, implement, and maintain its IT security awareness training program. An IT Security Awareness and Training Strategy leverages its organizational skills assessment and is tailored to its culture. This strategy shall include the structure of the awareness and training program priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies, frequency of training, and deployment methods in accordance with *FY 2019 IG FISMA Reporting Metrics* requirements.

During FY 2019, the SEC's OHR conducted an agency-wide competency assessment to identify proficiency gaps, including areas related to IT security. However, OIT did not define an IT Security and Awareness Training Strategy to address skill gaps identified in workforce assessment.

This occurred, in part, because OIT stated that it diverted key and significant resources to prioritize other security-related activities such as implementing enhanced processes and technologies, which led to a delay in releasing an IT Security Awareness and Training Strategy. According to OIT, the IT Security Awareness and Training Strategy document is in development with [redacted] and awaits final enhancements before its release.

Without an IT Security Awareness and Training Strategy, the SEC decreases its ability to effectively address skills and knowledge gaps identified during the agency-wide competency assessment related to information security. By not addressing gaps in information security, the

SEC leaves its networks and systems vulnerable, as key users may lack the necessary training to keep them secure.

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 and 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 9: Define and implement an Information Technology Security Awareness and Training Strategy that addresses the agency's plan to improve its security awareness and training.

> **Management's Response.** Management concurred with the recommendation. OIT is developing a Security Awareness and Training Strategy, which will describe ongoing and planned security training and awareness initiatives, discuss targeted audiences, and outline training objectives as they align to organizational objectives. The strategy document is expected to be completed in February 2020. 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 2019 IG FISMA Reporting Metrics* requires 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 POA&M, which are the three principal documents in a system's security authorization package. According to NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, organizations should take steps to establish, implement, and maintain an ISCM program, including defining an ISCM strategy, analyzing and reporting findings, and reviewing and updating the ISCM strategy and program, as necessary. In addition, OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 2013, states that agencies were required to implement continuous monitoring of security controls as part of a phased approach through FY 2017.[13]

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 improved from Level 2: *Defined* to Level 3: *Consistently Implemented* between FY 2018 and FY 2019, it has not fully implemented the recommendations identified in prior years; therefore, these 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 and did not establish procedures for reviewing and modifying all aspects of the ISCM strategy.
- Perform ongoing authorizations of its information systems and the environments in which they operate.

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

- Consistently perform [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 2019, as listed below:

- While the SEC has documented its ISCM strategy, the agency did not define the qualitative and quantitative performance measures to be collected. Additionally, the SEC did not define the procedures for reviewing and modifying all aspects of the SEC Continuous Monitoring strategy.

- SEC did not document policies and procedures for monitoring and closing POA&M as part of their ongoing authorization process for information systems.
- Although the SEC performed [redacted] on the sampled devices, the agency failed to create a Standard Operating Procedure (SOP) to establish a goal and [redacted] per the SEC's FY 2018 Corrective Action Plan (CAP).

These control weaknesses occurred, in part, because the ISCM processes did not include procedures for reviewing and modifying all aspects of the ISCM strategy. However, OIT has defined a new Ongoing Authorization Methodology within 2019, which is still in implementation stages. Once fully implemented, the Ongoing Authorization Methodology will contain all necessary documented components of the ISCM program. Additionally, according to OIT, the agency implemented a rigorous POA&M closure process, which requires a critical analysis of closure requests performed by an independent team prior to closing a particular POA&M. Furthermore, it is determined that OIT has implemented an adequate POA&M process; however, its dependencies on the assigned POA&M owners cause delays closing POA&M timely. Lastly, the SEC did not complete all tasks related to the FY 2018 CAP, specifically the documentation of an SOP related to their [redacted] Overall, the above weaknesses occurred, in part, because the current ISCM processes did not include an effective oversight function to review ISCM strategy, ongoing authorization processes, and the [redacted]

Kearney is not making any new recommendations in this area, as the SEC is working to address the prior-year FISMA recommendations. See APPENDIX II: OPEN FISMA RECOMMENDATIONS.

Domain #7: Incident Response

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*, August 2012, key phases in the incident response process are: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

Kearney assessed the SEC's incident response program and determined that the program's assessed maturity level is Level 3: *Consistently Implemented*, meaning the SEC formalized and consistently implemented its incident response policies, procedures, and strategies for responding to incidents, 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 FY 2018 and FY 2019, it has not fully implemented the recommendations identified in prior years; therefore, these conditions still exist.

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

- Maintain up-to date and comprehensive incident response plans, policies, procedures, and strategies.
- Timely report incidents to the United States Computer Emergency Readiness Team (US-CERT).

Similarly, Kearney determined that many of the weaknesses with the SEC's incident response program identified during the FY 2017 FISMA audit remained present in FY 2018 and in FY 2019, as listed below:

- The SEC has defined its plan, policies, procedures, and strategies for responding to incidents; however, the SEC did not consistently maintain and execute its incident response policies and procedures. Kearney reviewed the SEC's incident response plan, policies, procedures, and strategies and determined that the SEC did not identify and define performance metrics that will be used to measure and track the effectiveness of its incident response program. The [redacted] mentioned training at a high level and did not detail the type of training or frequency of training requirements for incident response personnel.
- According to policy, the SEC is required to report incidents to US-CERT within one hour of identification; however, according to records from the Security Operations Center (SOC), the agency failed to timely report 75 of 289 incidents (about 26%) to US-CERT within one hour. In 11 of 75 cases, the SOC did not report the incidents to US-CERT for five or more days. See ***Exhibit 4*** for a breakdown of the SEC's timeliness of incident reporting to US-CERT.

Exhibit 4: Timeliness of Incident Reporting to US-CERT

Timeframe Reported to US-CERT	Number of Incidents
Total Reported within 1 hour (compliant)	**214 (about 74%)**
1-24 hours	61
1-5 days	3
5+ days	11
Total Reported after 1 hour (non-compliant)	**75 (about 26%)**
Total FY 2019 Incidents	**289 (100%)**

Source: Kearney analysis of SOC-reported incidents between October 1, 2018 and May 31, 2019.

These control weaknesses continued to occur, in part, because the incident response processes did not include reviews and updates to all aspects of the [redacted] according to FY 2017 OIG recommendations related to incident response. Although the SEC has partially completed updates to the [redacted], per OIG recommendation, there are still key points within the plan, including performance measures and training, which require updates. Additionally, the SEC has taken the initiative to report all incidents, including incidents identified as low-impact and/or low risk, to encourage information sharing between the SEC and DHS in order to promote a secure environment. The SEC stated that these low-impact incidents were not a priority for the SEC, which resulted in untimely reporting of incidents to US-CERT, as the SEC directed its focus on the communication of other high-impact related incidents.

Kearney is not making any new recommendations in this area, 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 #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.[16] Because information system resources are essential to an organization's success, it is critical that systems are able to operate effectively without excessive interruption. Business Impact Analyses (BIAs) help organizations identify and prioritize information systems and components critical to supporting the organization's operations. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and efficiently as possible following a disaster. NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, states that contingency planning activities include developing the planning policy, creating contingency strategies, maintaining contingency plans, conducting BIAs, testing contingency plans, and conducting exercises. In addition, NIST SP 800-53, Rev. 4, (CP-4), *Contingency Plan Testing and Exercises*, requires organizations to perform periodic testing of contingency plans to determine effectiveness and organizational readiness to execute the plan.

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 effectively manages and measures its Contingency Planning program. The SEC improved from Level 2: *Defined* in FY 2018. Specifically, during FY 2019, the SEC improved five of seven contingency planning metrics, including Contingency Planning Policies and Procedures, BIAs, Maintaining Information System Contingency Plans (ISCP), ISCP Testing, and Planning and Performance of Recovery Activities, to achieve an effective level of security.[17] In addition, the agency has closed all prior-year recommendations, which related to the annual testing of the EDRP and updating contingency planning documentation.

During FY 2019, the SEC performed a test of the agency's EDRP in accordance with its policy. In addition, the SEC documented an After Action Report that included milestones performed, findings, recommendations, key performance indicators, and a list of participants.

Additionally, OIT updated and maintained contingency planning documentation in accordance with SEC policies and procedures in FY 2019. Specifically, OIT made updates to its EDRP, ISCP application template, ISCP infrastructure template, and BIA application template. Additionally, in accordance with the [redacted] and the EDRP, all eight sampled systems (about 100%) had appropriate BIAs and ISCPs and were updated within the appropriate period.

As the SEC reached an effective level of security for the Contingency Planning domain in FY 2019, and Kearney did not identify any new control weaknesses that prevented the SEC from reaching an effective level of security, Kearney is not offering any new recommendations related contingency planning.

[16] 44 U.S.C Section 3554 (b) (8)
[17] According to the *FY 2019 IG FISMA Reporting Metrics*, Level 4: *Managed and Measurable*, is considered to be an effective level of security at the domain, function, and overall program level.

OVERALL CONCLUSION

Overall, the SEC improved aspects of its information security program. For example, the SEC improved its ISCM, Incident Response, and Contingency Planning Programs. Further, there were improvements in individual metrics, including information security architecture, security awareness training, ISCM performance measures, use of incident response technology, planning and performance of recovery activities, and BIA. However, Kearney noted that the SEC's information security program did not meet the *FY 2019 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 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 Incident Response. 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.

Develop a Supply Chain Risk Strategy: The *FY19 FISMA Reporting Metrics* requires 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 SECURE Technology Act. The SEC did not establish policies and procedures regarding supply chain risk management and the integration of supply chain concepts into its enterprise architecture. 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 the SEC is awaiting further direction on the SECURE Technology Act, as it was released in December 2018 without additional guidance. OIT stated that it was waiting for the Council established by the SECURE Technology Act 2018 to release the standards, guidance, and practices for agencies to self-assess against in accordance with the SECURE Technology Act 2018. Without necessary policies and procedures to address supply chain risks, the SEC is unable to recognize the risks involved with the agency's supply chain, including: 1) reducing the likelihood of unauthorized modifications at each stage in the supply chain and 2) protecting information systems and information system components prior to taking delivery of such systems/components. Therefore, the agency is less likely to be able to respond effectively to supply chain risks.

Kearney encourages the SEC to develop an action plan, as well as establish policies and procedures regarding supply chain risk management that align with the SECURE Technology Act, upon the release of the standards, guidance, and practices in accordance with said Act.

Management's Response. The agency's response can be found in APPENDIX IV: MANAGEMENT COMMENTS.

[redacted]

[redacted]

Management's Response. The agency's response can be found in APPENDIX IV: MANAGEMENT COMMENTS.

Implement an Automated Risk Designation Tool: The *FY 2019 IG FISMA Reporting Metrics* require that agencies employ automation to centrally document, track, and share personnel risk designations and screening information with necessary parties. The SEC has ensured that all personnel are assigned a risk designation, appropriately screened prior to being granted system access, and rescreened periodically. However, 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 the Office of Support Operations recently recognized the increased need for an automated risk designation tool, but has not yet implemented the tool in FY 2019. Without an automated tool to centrally document, track, and share risk designations, manual processes are necessary to perform these actions. Risk designations are more likely to be appropriately assigned with automated controls, as automated controls tend to be 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 with necessary parties.

Management's Response. The agency's response can be found in APPENDIX IV: MANAGEMENT COMMENTS.

Implement ICAM Strategy: The *FY 2019 IG FISMA Reporting Metrics* require agencies to transition to its 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 (FICAM) segment architecture to reach Level 4: *Managed and Measurable*. The SEC developed an ICAM Strategy and set target initiatives. However, 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 FICAM segment architecture. Of the [redacted] initiatives outlined in the ICAM Strategy, OIT has completed [redacted] of these. The [redacted] remaining

target initiatives that have not been accomplished relate to leveraging [redacted], implementing ICAM policies and procedures, [redacted], and developing a Risk Management Plan that defines the way ICAM risks are measured. This occurred, in part, because the SEC has recently developed its ICAM strategy and was in the process of transitioning to its "to-be" ICAM architecture during FY 2019. Of the [redacted] incomplete initiatives, [redacted] was not completed yet, as the agency was in the process of evaluating the ICAM risk measurements in relation to the SEC's enterprise architecture during FY 2019. The other [redacted] were planned to be completed during the [redacted] program implementation, which is targeted for [redacted]. Without transitioning to its desired or "to-be" ICAM architecture, the SEC may not timely remediate risks associated with [redacted] 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.

Define Breach Response Metrics: The *FY 2019 IG FISMA Reporting Metrics* require agencies to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Breach Response Plan. The SEC performed a Table-Top Exercise (TTX) in accordance with its Breach Response Plan and documented lessons learned resulting from the TTX; however, 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 functions as intended or evaluated the continuous improvement or program performance. This occurred, in part, because the activities performed in the SEC's most recent TTX, performed in accordance with the Breach Response Plan, 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 improve the response program; specifically, the SEC cannot improve the effectiveness with which it is able to lessen the impact of 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.

Define Data Exfiltration Metrics: The *FY 2019 IG FISMA Reporting Metrics* require agencies to analyze qualitative and quantitative measures on the performance of its data exfiltration and

enhanced network defenses. The SEC performed an exercise to determine attempts at data exfiltration in accordance with DHS; however, the SEC did not track quantitative metrics on the performance of its data exfiltration exercise and enhanced network defenses. This occurred, in part, because the SEC performed data exfiltration exercises according to DHS's schedule, which decreases the ability to collect reproducible supporting metrics. Further, the SEC self-identified that it was in the process of fully implementing advanced incident response technologies for analysis of trends and performance against benchmarks and adjusting security measures using quantitative metrics accordingly. Without qualitative and quantitative metrics on the performance of its data exfiltration and enhanced network defenses, the SEC cannot measure its data incident responses effectively. Further, the SEC cannot continuously improve the effectiveness of its data incident response performance, leading to the decreased impact of incidents.

Kearney encourages the SEC to track quantitative and qualitative metrics on the performance of its data exfiltration exercise and enhance network defenses by fully implementing advanced incident response technologies for analysis trends and performance against benchmarks and adjusting security measures using qualitative and quantitative metrics accordingly.

Management's Response. The agency's response can be found in APPENDIX IV: MANAGEMENT COMMENTS.

[redacted]

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 CIGIE *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 2019 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.

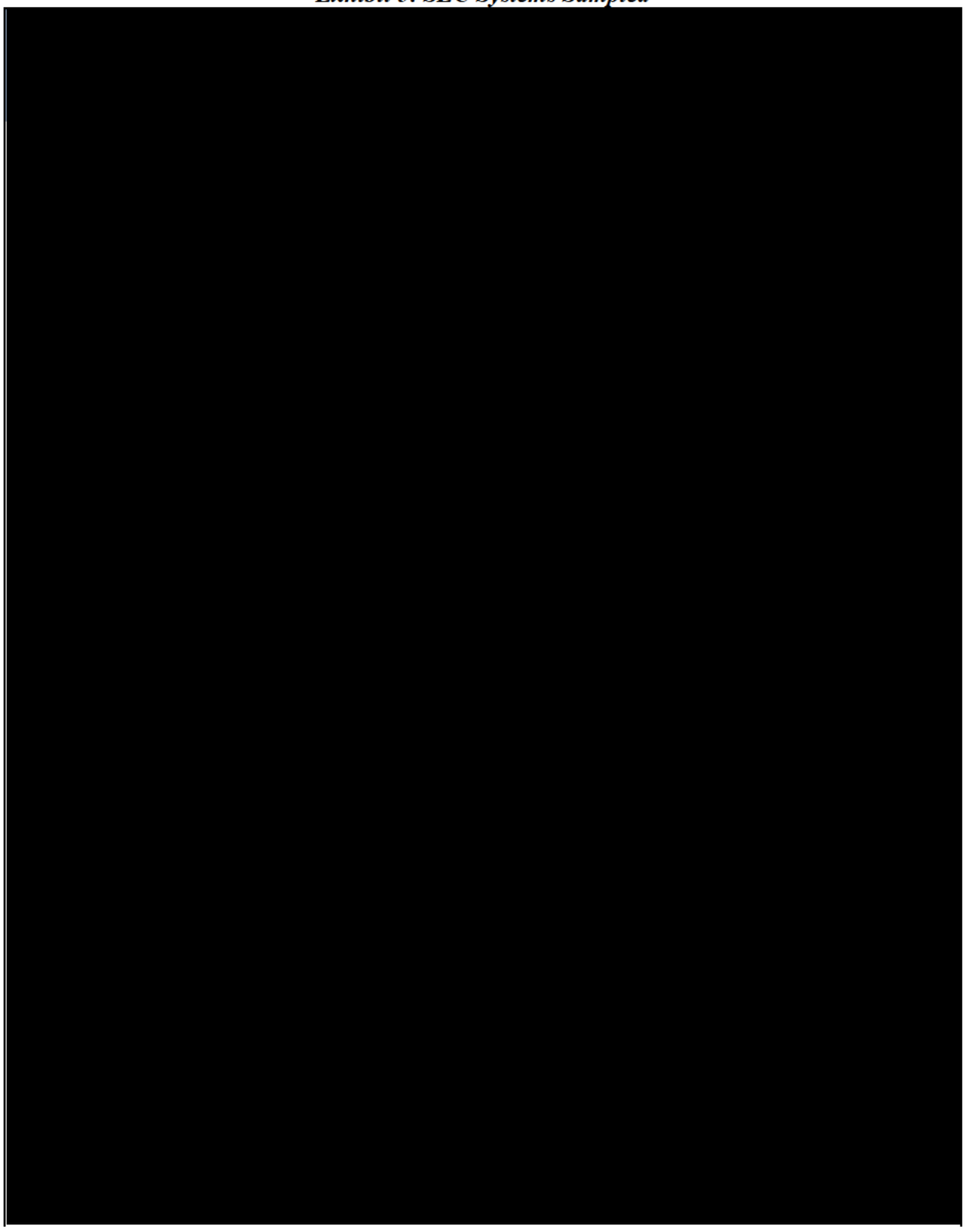
The evaluation covered the period between October 1, 2018 and July 19, 2019 and addressed the following eight domains specified in DHS's reporting instructions for FY 2019:

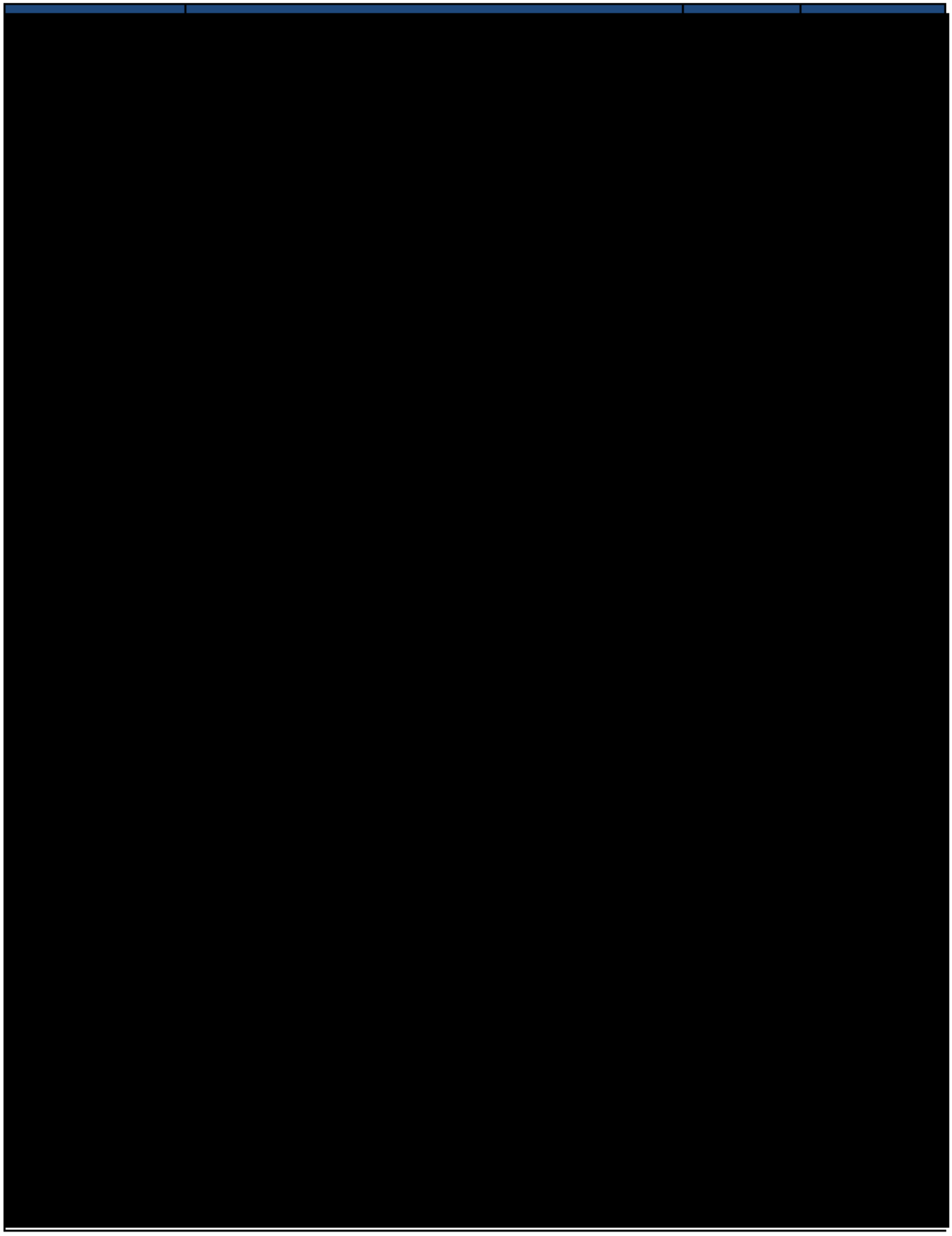
- Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- ISCM
- Incident Response
- Contingency Planning.

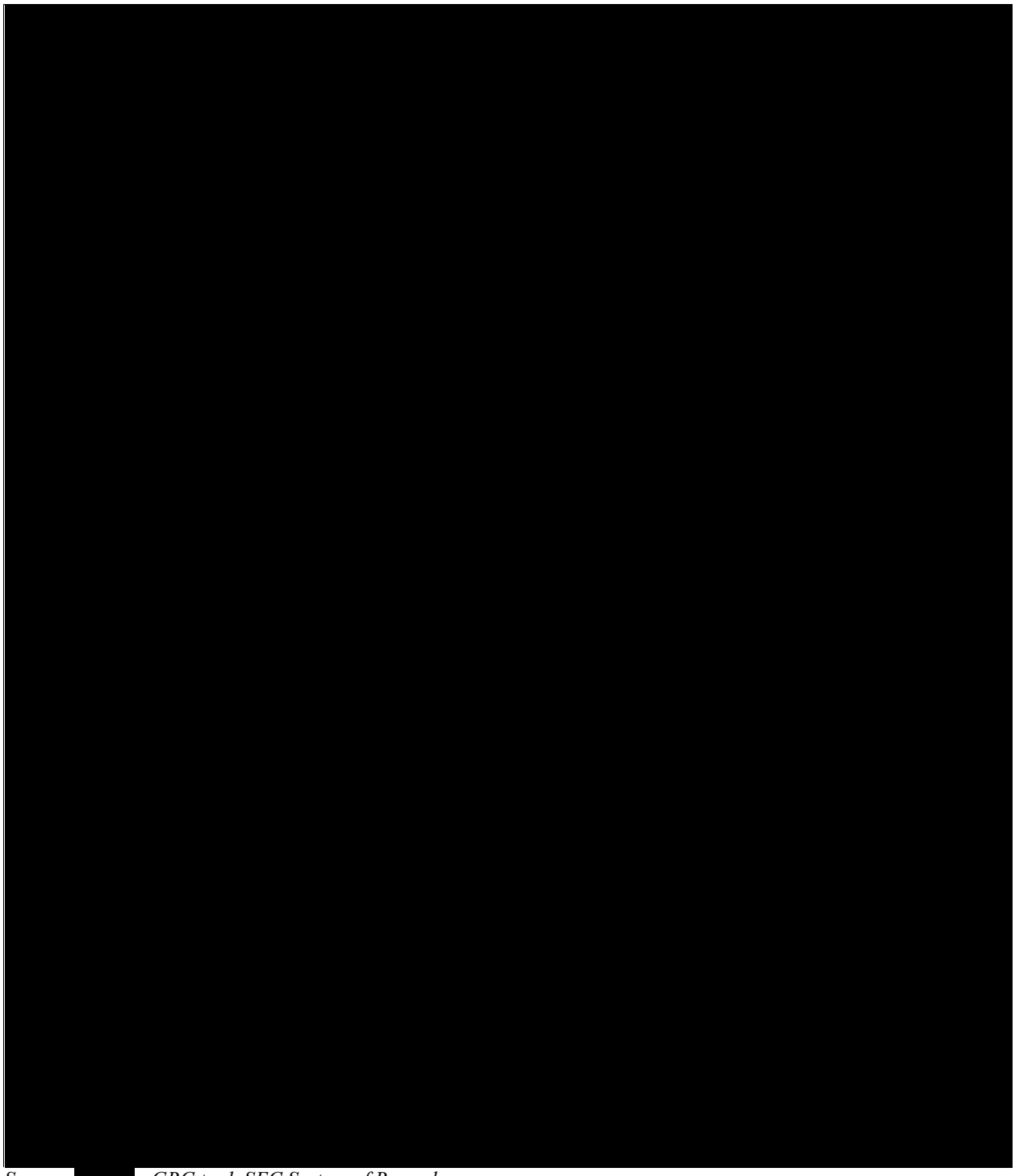
Methodology: We conducted an evaluation of the SEC's information security posture sufficient to address our objective. Specifically, to assess system security controls, Kearney reviewed the security assessment packages for a non-statistical, judgmentally selected sample of 8 of the SEC's 80 FISMA-reportable systems (about 10%). The sample consisted of the internally and externally hosted systems shown in ***Exhibit 5***: SEC Systems Sampled.[18] In addition, to address the requirements of the *FY 2019 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.

[18] We selected information systems based on the SEC's inventory of FISMA-reportable systems maintained in OIT's system of record as of April 29, 2019. The inventory included 80 FISMA-reportable information systems (i.e., 47 SEC-operated, and 33 contractor-operated). We selected eight FISMA-reportable information systems, factoring in: 1) whether the system was included in prior FISMA audits or covered in audits conducted by the OIG in the past three years; 2) whether the system contained sensitive and confidential information, including PII; 3) system risk categorization; and 4) the system's ATO status, among other criteria. We also solicited OIT's input for our sample selection.

Exhibit 5: SEC Systems Sampled







Source: [redacted] *eGRC 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, 2018 and May 31, 2019
- Were confirmed as having compromised the confidentiality, integrity, or availability of information
- Were from all nine US-CERT threat taxonomies where a confirmed incident occurred
- Were representative of each incident priority type (i.e., high, medium, or low) as classified by OIT.

According to OIT's records, 608 incidents occurred between October 1, 2018 and May 31, 2019. Based on our established criteria, we selected and reviewed a random sample of 45 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 2019 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 Memorandum 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 2019 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: GAO's *Assessing the Reliability of Computer-Processed Data*, July 2009, (GAO-09-680G) states: "data reliability refers to the accuracy and completeness of computer-processed data, given the uses they are intended for. Computer-processed data may be data (1) entered into a computer system or (2) resulting from computer processing."

Furthermore, GAO-09-680G defines reliability, completeness, and accuracy as follows:

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

Kearney used the SEC's eGRC 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 ISOs 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: Prior to the start of the FY 2019 FISMA evaluation and throughout FY 2019, the SEC closed the remaining two of 21 recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2016[19] (FY 2016 FISMA audit). As of October 1, 2019, the SEC also closed 8 of 20 recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2017[20] (FY 2017 FISMA audit), dated March 30, 2018, and 2 of 11 recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2018[21] (FY 2018 FISMA evaluation), dated December 12, 2018. Although OIT addressed these recommendations, as we noted in this report, areas for improvement still exist. APPENDIX II: OPEN FISMA RECOMMENDATIONS lists all open OIG recommendations from prior FISMA audits.

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

[19] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016*, Report No. 539; March 7, 2017.
[20] 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.
[21] 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.

APPENDIX II: OPEN FISMA RECOMMENDATIONS

Exhibit 6 lists all FISMA recommendations that remain open from prior FISMA audits as of October 1, 2019.

Exhibit 6: Open FISMA Recommendations

Domain	Open Recommendations
FY 2017	
Risk Management (Identify)	**Recommendation 1:** Define and implement a process that includes clear roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of agency information systems [redacted]
	Recommendation 3: 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, [redacted]
	Recommendation 5: (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.
	Recommendation 7: 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)	**Recommendation 8:** Develop, review, and approve secure baselines for all systems included in the [redacted]
	Recommendation 9: 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

Domain	Open Recommendations
	address the [redacted], including those issues and vulnerabilities identified as unmitigated at the time of our audit.
Identity and Access Management (Protect)	**Recommendation 12:** [redacted]
	Recommendation 13: [redacted]
Security Training (Protect)	**Recommendation 15:** 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)	**Recommendation 16:** 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)	**Recommendation 17:** 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.
	Recommendation 20: Perform an assessment of existing incident response reporting mechanisms, and develop a process to periodically measure and ensure the timely reporting of incidents to agency officials and external stakeholders.
FY 2018	
Configuration Management (Protect)	**Recommendation 1:** Update configuration management procedures to require that [redacted] are approved.
	Recommendation 2: Update configuration management procedures to require [redacted]

Domain	Open Recommendations
Data Protection and Privacy (Protect)	**Recommendation 3:** Complete initiatives to implement [redacted]
	Recommendation 4: Complete initiatives to implement [redacted]
	Recommendation 5: Update procedures for the [redacted]
Security Training (Protect)	**Recommendation 6:** Define and implement a control to detect instances where contractor personnel received network accounts but were not assigned privacy and information security awareness training, nor tracked within system reporting tools.
Information Security Continuous Monitoring (Detect)	**Recommendation 7:** [redacted] Additionally, Office of Information Technology should develop procedures [redacted] Accordingly, Office of Information Technology should update policies and procedures to [redacted]
	Recommendation 8: [redacted]
	Recommendation 9: Establish a process to improve coordination and communication among the various Office of Information Technology teams [redacted].

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

APPENDIX III: SUMMARY OF ASSESSED FISMA RATINGS, FY 2018 & FY 2019

The table below lists the individual The *FY 2019 IG FISMA Reporting Metrics* metric ratings for the SEC in FY 2018 and FY 2019, and the determination of effective or not effective for each metric in FY 2019. Individual metrics are colored to highlight where the SEC improved or regressed between FY 2018 and FY 2019. See the key below.

Exhibit 7: Summary of Assessed FISMA Ratings between FY 2018 and FY 2019

Red: Indicates the assessed rating went down from FY 2018 to FY 2019
Green: Indicates the assessed rating went up from FY 2018 to FY 2019

	Domain	#	Metric Title	2018 Assessed Rating	2019 Assessed Rating	2019 Effective/Not Effective
Identify	Risk Management (RM)	1	Inventory of Information Systems and System Interconnections	Defined	Defined	Not Effective
		2	Inventory of Hardware Assets	Managed and Measureable	Consistently Implemented	Not Effective
		3	Inventory of Software Assets	Ad-Hoc	Ad-Hoc	Not Effective
		4	Security Categorization and HVAs	Consistently Implemented	Defined	Not Effective
		5	RM Policies, Procedure, Strategy	Managed and Measureable	Defined	Not Effective
		6	Information Security Architecture	Defined	Consistently Implemented	Not Effective
		7	RM Roles and Responsibilities	Managed and Measureable	Defined	Not Effective
		8	POA&M Maintenance	Defined	Defined	Not Effective
		9	Risk Assessments	Defined	Defined	Not Effective
		10	Risk Communication	Defined	Defined	Not Effective
		11	Risk Mitigation of Contractor Systems	Defined	Defined	Not Effective
		12	Enterprise-Wide View of Risks	Defined	Consistently Implemented	Not Effective
	Overall	**13**	**Assessed Conclusion**	**Defined**	**Defined**	**Not Effective**
Protect	Configuration Management (CM)	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

	Domain	#	Metric Title	2018 Assessed Rating	2019 Assessed Rating	2019 Effective/Not Effective
		19	Flaw Remediation	Defined	Defined	Not Effective
		20	TIC Adoption	Consistently Implemented	Consistently Implemented	Effective
		21	Configuration Change Control	Defined	Defined	Not Effective
	Overall	**22**	**Assessed Conclusion**	**Defined**	**Defined**	**Not Effective**
	Identity and Access Management (IA)	23	IA Roles and Responsibilities	Defined	Defined	Not Effective
		24	IA Strategy	Defined	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	Defined	Managed and Measureable	Effective
		28	Strong Authentication- Non-Privileged	Consistently Implemented	Defined	Not Effective
		29	Strong Authentication - Privileged	Consistently Implemented	Defined	Not Effective
		30	Privileged Account Management	Defined	Defined	Not Effective
		31	Remote Access Configurations	Defined	Defined	Not Effective
	Overall	**32**	**Assessed Conclusion**	**Defined**	**Defined**	**Not Effective**
	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	Defined	Consistently Implemented	Not Effective
		36	Data Breach Response Plan	Consistently Implemented	Consistently Implemented	Not Effective
		37	Privacy Awareness Training	Managed and Measurable	Managed and Measurable	Effective
	Overall	**38**	**Assessed Conclusion**	**Consistently Implemented**	**Consistently Implemented**	**Not Effective**
	Security Training (ST)	39	ST Roles and Responsibilities	Defined	Defined	Not Effective
		40	Assessment of Cybersecurity Workforce	Ad-Hoc	Defined	Not Effective
		41	ST Strategy	Defined	Ad-Hoc	Not Effective
		42	ST Policies and Procedures	Ad-Hoc	Ad-Hoc	Not Effective
		43	Security Awareness Training	Defined	Managed and Measureable	Effective

	Domain	#	Metric Title	2018 Assessed Rating	2019 Assessed Rating	2019 Effective/Not Effective
		44	Specialized Security Training	Defined	Ad-Hoc	Not Effective
	Overall	**45**	**Assessed Conclusion**	**Defined**	**Defined**	**Not Effective**
Detect	ISCM	46	ISCM Strategy	Defined	Consistently Implemented	Not Effective
		47	ISCM Policies and Procedures	Defined	Defined	Not Effective
		48	ISCM Roles and Responsibilities	Defined	Defined	Not Effective
		49	Ongoing Assessments	Consistently Implemented	Consistently Implemented	Not Effective
		50	ISCM Performance Measures	Consistently Implemented	Managed and Measurable	Effective
	Overall	**51**	**Assessed Conclusion**	**Defined**	**Consistently Implemented**	**Not Effective**
Respond	Incident Response (IR)	52	IR Policies and Procedures	Defined	Defined	Not Effective
		53	IR Roles and Responsibilities	Defined	Defined	Not Effective
		54	Incident Detection and Analysis	Defined	Consistently Implemented	Not Effective
		55	IR Handling Processes	Defined	Optimized	Effective
		56	Sharing IR Information	Defined	Defined	Not Effective
		57	Collaboration with DHS and Other Parties	Consistently Implemented	Managed and Measurable	Effective
		58	IR Technologies Used	Defined	Managed and Measurable	Effective
	Overall	**59**	**Assessed Conclusion**	**Defined**	**Consistently Implemented**	**Not Effective**
Recover	Contingency Planning (CP)	60	CP Roles and Responsibilities	Consistently Implemented	Consistently Implemented	Not Effective
		61	CP Policies, Procedures, and Strategies	Defined	Consistently Implemented	Not Effective
		62	Business Impact Analysis	Defined	Consistently Implemented	Effective
		63	Maintain Information Systems CPs	Defined	Managed and Measurable	Effective
		64	System CP Testing/ Exercises	Defined	Managed and Measurable	Effective
		65	Information System Backup and Storage	Consistently Implemented	Consistently Implemented	Effective
		66	Planning and Performance of Recovery Activities	Defined	Managed and Measurable	Effective
	Overall	**67**	**Assessed Conclusion**	**Defined**	**Managed and Measurable**	**Effective**

Source: Kearney-generated based on FY 2018 and FY 2019 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: 2019.12.10 16:24:29 -05'00'

Date: December 10, 2019

Subject: Management Response to Draft Report No. 558, *"Fiscal Year 2019 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) 2019 (Report No. 558). The report evaluates the SEC's Information Security Program in accordance with the FY2019 Inspector General FISMA Reporting Metrics,[1] which are designed to assist Inspectors General in assessing 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).[2]

While more work remains to be done, it is encouraging that your report found that the SEC's information security program has increased its maturity rating for three of the five CSF functional areas (Detect, Respond and Recover) and in 18 individual metric categories including access agreements, security awareness training, Information Security Continuous Monitoring (ISCM) strategy, incident detection and analysis, and planning and performance of recovery activities.

Continuing to mature our cyber risk posture is a key priority for the SEC. During FY19, SEC staff closed 28 OIG IT-related recommendations and three GAO recommendations. Indeed, in order to continue to make progress to close outstanding recommendations and support ongoing audit activity, the Office of Information Technology (OIT) established a Cyber Risk and Governance Branch (CRG). Among other things, the CRG leads the development of enterprise information security policies and works with agency stakeholders to identify, analyze, and coordinate mitigation strategies for information technology risks identified by internal and external audits and reviews. In FY 2020, the agency plans to hire additional CRG staff in order

[1] U.S. Department of Homeland Security, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, April 9, 2019.
[2] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018

1

to support forthcoming audits and to prioritize and address recommendations made by both the OIG and the GAO.

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

Your report contains nine recommendations with which we concur. Below, we have outlined the steps we have already taken or intend to take to mature our program in these areas.

Recommendation 1: 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.

Response: We concur. The SEC will update its existing procedures to add a semi-annual review of FISMA reportable systems and their Federal Information Processing Standards Publication 199 security categorizations. The SEC will also update [redacted]. OIT will perform a comprehensive review of existing FISMA-reportable systems to validate each has a documented system categorization and correct any deficiencies. Additionally, the SEC will update its [redacted] of systems under their purview.

Recommendation 2: Complete all relevant components of the [redacted] including [redacted] expiration and review date, according to [redacted].

Response: We concur. The SEC will complete an analysis of existing system security plans to ensure the [redacted] is complete and is supported by the required documentation.

Recommendation 3: Define and communicate Information System Owner and Information System Security Officer roles and responsibilities.

Response: We concur. The SEC will formally define the roles of agency Information System Owner (ISO) and Information System Security Officer (ISSO) and communicate that information to individuals in these roles.

Recommendation 4: Develop and document a [redacted]

Response: We concur. In September 2018, the SEC purchased a new solution for [redacted] The SEC has developed a [redacted] and has acquired a new [redacted] tool that will provide the capability to ensure the [redacted] are being applied. Once this capability has been implemented, the SEC will perform analysis and data normalization to [redacted]

Recommendation 5: 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 (SSP) templates to ensure control tailoring justification corresponds to the methodology covered in part a).

Response: We concur. Although SEC had created control mappings, they were not explicitly trackable in the SSP templates. SEC is developing a new methodology that will update the control mapping source documents and the SSP templates to ensure consistency and completeness. In November 2019, the SEC updated its SSP template for [redacted] to more clearly identify the controls that are fully inherited from other systems, SEC program-level controls, and the controls that are tailored for inclusion or exclusion. During FY2020, system security plans for all [redacted] will be updated.

Recommendation 6: 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.

Response: We concur. OIT will update the SEC's user recertification procedures to document how the formal recertification process will be conducted for the [redacted] Additionally, OIT will perform an account recertification for each group of [redacted]

Recommendation 7: 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]

Response: We concur. The SEC will develop and document a formal process to prevent the creation of [redacted]. Additionally, instructions will be distributed to stakeholders involved in the [redacted] to reaffirm existing guidance and standard operating procedures regarding [redacted]. Lastly, SEC will perform a formal review of [redacted] and correct any deviations from the [redacted]

Recommendation 8: a) Determine 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 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 Commission has publically posted the required information in accordance with Section 208 of the E-Government Act.
Response: We concur. The SEC will update its policy to require the Senior Agency Official for Privacy to review the results of a privacy impact assessment prior to authorizing the use of a system to collect, process, or store personally identifiable information. The SEC will also review the status of privacy assessment worksheets (PAW) and privacy impact assessment (PIA) documentation for existing systems to ensure that required documents are accurate and accessible for review in accordance with Section 208 of the E-Government Act. Based on the review, the SEC will develop a timetable to correct noted deficiencies.

Recommendation 9: Define and implement an IT Security Awareness and Training Strategy that addresses the agency's plan to improve its security awareness and training.
Response: We concur. In July 2019, OIT Security began to develop a Security Awareness and Training Strategy. The strategy document describes ongoing and planned security training and awareness initiatives, discusses targeted audiences, and outlines training objectives as they align to organizational objectives. The strategy document is expected to be completed in February 2020.

With regards to the Other Matters of Interest identified, 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, as well as establish policies and procedures regarding supply chain risk management that align with the SECURE Technology Act, upon the release of the standards, guidance, and practices in accordance with said Act.
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 leadership plans to meet with stakeholders to discuss certain actions that may be able to be taken prior to the release of the FASC materials.

[redacted]

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 with necessary parties.

Response: The SEC's Office of Security Services, Personnel Security Operations (PSO) office is required, in accordance with Federal requirements,[4] to establish the risk and sensitivity level of all positions within the SEC and utilize the [redacted] to arrive at all risk and sensitivity designations. At the SEC, the [redacted] has been utilized since 2012 to designate the risk and sensitivity level of all new SEC positions. PSO maintains all position descriptions and results of the [redacted] in a library on a shared network drive that may be accessed only by individuals in PSO. In addition, PSO maintains an [redacted] that serves as the automated record which centrally documents, tracks, and is available to share risk designations and screening information with necessary parties. However, OSO plans to consider further opportunities to leverage automation in the managing and tracking of position risk designations as determined by the [redacted] and we look forward to sharing this process with OIG during the FY20 FISMA evaluation.

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,[5] and we will map the Strategy to the new requirements

[redacted]

[4] Parts 1400 and 731 of Title 5, Code of Federal Regulations

[5] [redacted]

identified in OMB Memorandum 19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*[6] and identify target implementation dates.

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 will update its Breach Response Plan to include metrics to evaluate the effectiveness of its plan and processes. The metrics will 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.

Define Data Exfiltration Metrics: Kearney encourages the SEC to track quantitative and qualitative metrics on the performance of its data exfiltration exercise and enhance network defenses by fully implementing advanced incident response technologies for analysis trends and performance against benchmarks and adjusting security measures using qualitative and quantitative metrics accordingly.
Response: The SEC is in the process of defining metrics goals and reporting frequency for its Data Loss Prevention capability and maturing the use of its incident response technology for analysis trends and benchmarks.

cc: Charles Riddle, Acting 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

[6] OMB Memorandum 19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019

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

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

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

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

Comments and Suggestions

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