

REPORT NO. 570
DECEMBER 21, 2021

OFFICE OF
**INSPECTOR
GENERAL**

OFFICE OF AUDITS

**Fiscal Year 2021 Independent
Evaluation of the SEC's
Implementation of the Federal
Information Security
Modernization Act of 2014**

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



OFFICE OF
INSPECTOR GENERAL

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

M E M O R A N D U M

December 21, 2021

TO: Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

A handwritten signature in blue ink, reading "Carl W. Hoecker".

SUBJECT: *Fiscal Year 2021 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014, Report No. 570*

Attached is the Independent Auditor's Report on the Fiscal Year 2021 Independent Evaluation of the U.S. Securities and Exchange Commission's (SEC or agency) Implementation of the Federal Information Security Modernization Act of 2014 (FISMA). We contracted with Kearney and Company, P.C. (referred to as "Kearney"), to conduct this independent evaluation. The 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 its information security program. Among other actions taken, the SEC made progress in improving its information security program by refining its management of security training roles and responsibilities, enhancing its security training strategy, implementing the agency's policy for specialized security training, improving its [REDACTED], optimizing a Vulnerability Disclosure Policy, refining its configuration management processes related to reconciliation of software code in production, improving its incident response information-sharing capabilities, and improving its Contingency Planning Capabilities. These improvements occurred despite facing challenges presented by the ongoing Coronavirus Disease 2019 pandemic, which included a significant increase in telework.

However, as described in the attached report, Kearney identified opportunities for improvement in key areas and made eight 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 2021 Inspector General FISMA Reporting Metrics' definition of "effective."

REDACTED FOR PUBLIC RELEASE

On November 16, 2021, we provided management with a draft of Kearny' report for review and comment. In the agency's December 10, 2021 response, management concurred with Kearney's recommendations. Kearney included management's response as Appendix IV of this report.

To improve the SEC's information security program, we urge management to take action to address areas of potential risk identified in this report. Please provide the OIG with a written corrective action plan within the next 45 days that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how the SEC will address the recommendations.

We appreciate management's courtesies and cooperation during the evaluation. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits Evaluations, and Special Reports.

Attachment

cc: Gary Gensler, Chairman
Prashant Yerramalli, Chief of Staff, Office of Chairman Gensler
Heather Slavkin Corzo, Policy Director, Office of Chairman Gensler
Kevin Burris, Counselor to the Chair and Director of Legislative and Intergovernmental Affairs
Scott Schneider, Counselor to the Chair and Director of Public Affairs
Lisa Helvin, Legal Counsel, Office of Chair Gensler
Philipp Havenstein, Operations Counsel, Office of Chair Gensler
Hester M. Peirce, Commissioner
Benjamin Vetter, Counsel, Office of Commissioner Peirce
Elad L. Roisman, Commissioner
Matthew Estabrook, Counsel, Office of Commissioner Roisman
Allison Herren Lee, Commissioner
Frank Buda, Counsel, Office of Commissioner Lee
Andrew Feller, Counsel, Office of Commissioner Lee
Caroline A Crenshaw, Commissioner
David Hirsch, Counsel, Office of Commissioner Crenshaw
Dan Berkovitz, General Counsel
Caryn Kauffman, Director/Chief Financial Officer and Acting Chief Risk Officer
Matthew Keeler, Management and Program Analyst, Office of Chief Risk Officer
David Bottom, Director/Chief Information Officer, Office of Information Technology
Andrew Krug, Chief Information Security Officer, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology

***Fiscal Year 2021 Independent Evaluation
of the U.S. Securities and Exchange
Commission's Implementation of the
Federal Information Security
Modernization Act of 2014***

December 21, 2021



*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 1SJI4

COVER LETTER

December 21, 2021

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 each Federal agency Inspector General or a contracted independent external auditor to conduct an annual independent evaluation to determine the effectiveness of its information security program and practices. Kearney conducted this independent evaluation of the SEC's information security program and practices in support of the SEC Office of Inspector General (OIG) in accordance with the Council of Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Kearney's evaluation included inquiries, observations, and inspection of SEC documents and records, as well as direct testing of controls. We are pleased to provide our report, entitled *Fiscal Year 2021 Independent Evaluation of the Securities and Exchange Commission'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 *Fiscal Year (FY) 2021 Inspector General (IG) FISMA Reporting Metrics, Version 1.1 (FY 2021 IG FISMA Reporting Metrics)*, dated May 12, 2021. Kearney's methodology for the FY 2021 FISMA evaluation included testing the effectiveness of selected security controls the SEC has implemented in eight sampled information systems for compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013. The *FY 2021 IG FISMA Reporting Metrics* utilize a maturity model and request that IGs evaluate and rate the effectiveness of security controls for each of the five NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) Functions (i.e., Identify, Protect, Detect, Respond, and Recover). To achieve an effective level of information security under the maturity model, agencies must reach Level 4: *Managed and Measurable*.

Since FY 2020, the SEC’s Office of Information Technology (OIT) improved aspects of its information security program. Among other actions taken, OIT made progress in improving its information security program by refining its management of security training roles and responsibilities, enhancing its security training strategy, implementing the agency’s policy for specialized security training, improving its [REDACTED], optimizing a Vulnerability Disclosure Policy, refining its configuration management processes related to reconciliation of software code in production, improving its incident response information-sharing capabilities, and improving its Contingency Planning Capabilities. These improvements occurred despite facing challenges presented by the ongoing Coronavirus Disease 2019 pandemic, which included a significant increase in telework.

Although the SEC has strengthened its program since the last FISMA evaluation, Kearney noted that the agency’s information security program did not meet the *FY 2021 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 **Exhibit 1** below, the SEC’s assessed maturity level for security training increased from Level 2: *Defined* to Level 5: *Optimized*. While the agency’s program, as a whole, did not reach the level of an effective information security program, the SEC has shown significant improvements at the domain levels.

Exhibit 1: Summary of SEC FISMA Ratings

Domain	Assessed Rating By Fiscal Year (FY)	
	2021	2020
Risk Management	Level 3: <i>Consistently Implemented</i>	Level 3: <i>Consistently Implemented</i>
Supply Chain Risk Management	Level 1: <i>Ad Hoc</i>	Not applicable (N/A)
Configuration Management	Level 2: <i>Defined</i>	Level 2: <i>Defined</i>
Identity and Access Management	Level 2: <i>Defined</i>	Level 2: <i>Defined</i>
Data Protection and Privacy	Level 3: <i>Consistently Implemented</i>	Level 3: <i>Consistently Implemented</i>
Security Training	Level 5: <i>Optimized</i>	Level 2: <i>Defined</i>
Information Security Continuous Monitoring	Level 3: <i>Consistently Implemented</i>	Level 3: <i>Consistently Implemented</i>
Incident Response	Level 4: <i>Managed and Measurable</i>	Level 4: <i>Managed and Measurable</i>
Contingency Planning	Level 4: <i>Managed and Measurable</i>	Level 4: <i>Managed and Measurable</i>

Source: Kearney-generated based on FYs 2020 and 2021 CyberScope Metric responses

Our report includes eight new recommendations to strengthen the SEC's information security program. As our report highlights, while the agency made improvements within five of the nine¹ *FY 2021 IG FISMA Reporting Metrics* domains, opportunities exist for the SEC to improve its performance in all nine *FY 2021 IG FISMA Reporting Metrics* areas.² Significant opportunities for improvement remain in key areas such as developing a supply chain management action plan, fully implementing a [REDACTED], completing Federal Information Processing Standards Publication 199 categorization worksheets for [REDACTED], consistently capturing and sharing lessons learned on cybersecurity Risk Management practices, documenting and utilizing lessons learned for configuration baseline policies and procedures, [REDACTED], documenting processes for maintaining an inventory for the collection and use of Personally Identifiable Information, implementing lessons learned for the effectiveness of Information Security Continuous Monitoring policies, and utilizing automation to test contingency plans for information systems. 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 21, 2021

¹ One of the nine domains, (i.e., the Supply Chain Risk Management domain) is a new domain for FY 2021 and was not present in prior years.

² The SEC made metric-level improvements in Risk Management, Identity and Access Management, Security Training, Incident Response, and Contingency Planning. However, metric-level improvements can still be made related to current-year and prior-year recommendations.


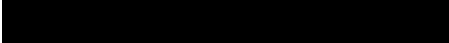


TABLE OF CONTENTS

	<u>Page #</u>
COVER LETTER.....	i
TABLE OF CONTENTS	iv
TABLE OF EXHIBITS	v
ABBREVIATIONS	v
BACKGROUND AND OBJECTIVES	1
Background	1
Objectives.....	4
RESULTS	6
Domain #1: Risk Management	6
Domain #2: SCRM.....	11
Domain #3: Configuration Management	11
Domain #4: Identity and Access Management.....	16
Domain #5: Data Protection and Privacy	18
Domain #6: Security Training	21
Domain #7: ISCM	22
Domain #8: Incident Response	23
Domain #9: Contingency Planning.....	24
OVERALL CONCLUSION.....	27
OTHER MATTERS OF INTEREST.....	28
APPENDIX I: SCOPE AND METHODOLOGY	30
APPENDIX II: OPEN FISMA RECOMMENDATIONS.....	35
APPENDIX III: SUMMARY OF ASSESSED FISMA RATINGS, FY 2020 & FY 2021	38
APPENDIX IV: MANAGEMENT COMMENTS.....	41

TABLE OF EXHIBITS

	<u>Page #</u>
Exhibit 1: Summary of SEC FISMA Ratings.....	ii
Exhibit 2: Cybersecurity Framework Functions Mapped to FY 2021 IG FISMA Reporting Metrics Assessment Domains	2
Exhibit 3: IG Assessment Maturity Levels.....	3
Exhibit 4: Security-Focused Configuration Management Phases.....	11
Exhibit 5: SEC Systems Sampled	31
Exhibit 6: Open FISMA Recommendations.....	35
Exhibit 7: Summary of Assessed FISMA Ratings between FY 2020 and FY 2021	38

ABBREVIATIONS

Cybersecurity Framework	National Institute of Standards and Technology's <i>Framework for Improving Critical Infrastructure of Cybersecurity</i>
DHS	Department of Homeland Security
	
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
ICT	Information and Communications Technology
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
Kearney	Kearney & Company, P.C.
	
M	Memorandum
NIST	National Institute of Standards and Technology

[REDACTED]

OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PL	Public Law
POA&M	Plans of Action & Milestones
PUB	Publication
Rev.	Revision
SA&A	Security Assessment and Authorization
SCRM	Supply Chain Risk Management
SEC	U.S. Securities and Exchange Commission
SP	Special Publication
SSP	System Security Plan
U.S.C.	United States Code

BACKGROUND AND OBJECTIVES

Background

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law [PL] 113-283). 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 information 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 may 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 issued guidance to IGs on FISMA reporting for fiscal year (FY) 2021.³

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 2021 IG FISMA Reporting Metrics*. The results of these efforts supported the Office of Inspector General’s (OIG) FY 2021 CyberScope submission to OMB and DHS.⁴

As *Exhibit 2* illustrates, the *FY 2021 IG FISMA Reporting Metrics* include nine 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).⁵

³ *Fiscal Year 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.1, dated May 12, 2021 (hereafter referred to as “*FY 2021 IG FISMA Reporting Metrics*”)

⁴ CyberScope is the platform that Chief Information Officers, Privacy Officers, and IGs use to meet FISMA reporting requirements. The SEC OIG completed its FY 2021 CyberScope submission to DHS and OMB on October 28, 2021.

⁵ The Cybersecurity Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today.

Exhibit 2: Cybersecurity Framework Functions Mapped to FY 2021 IG FISMA Reporting Metrics Assessment Domains

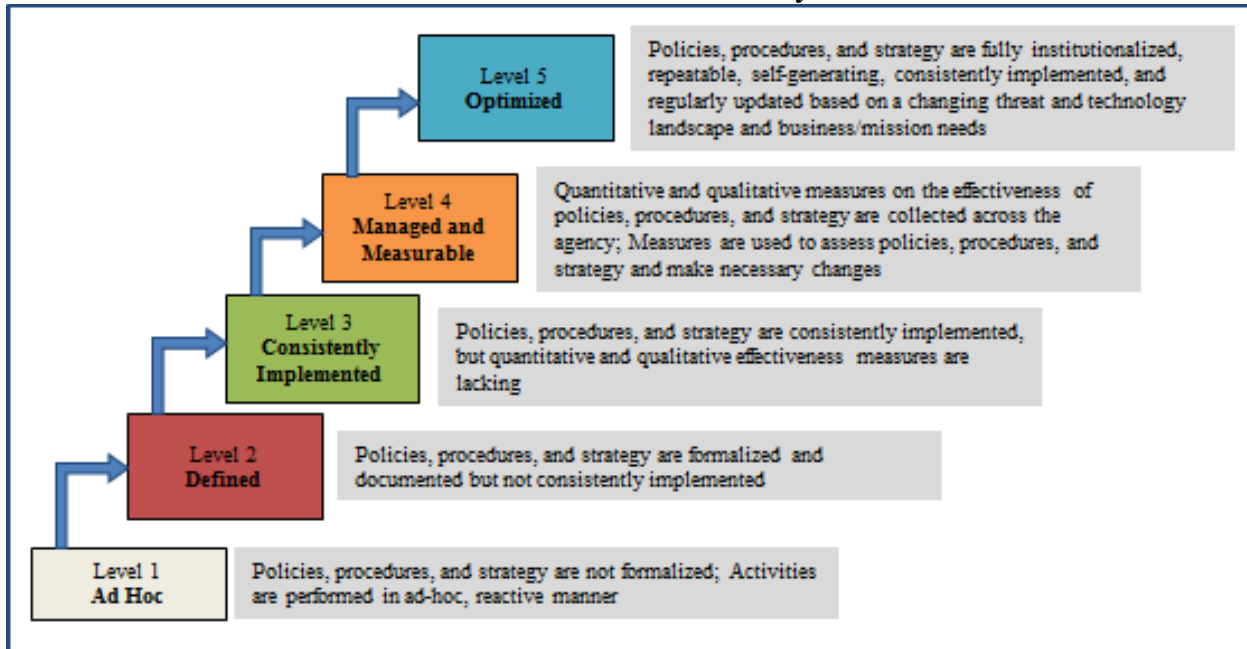
Cybersecurity Framework Functions	FY 2021 IG FISMA Reporting Metrics Assessment Domains
Identify	Risk Management
	Supply Chain Risk Management (SCRM)
Protect	Configuration Management
	Identity and Access Management
	Data Protection and Privacy,
	Security Training
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Source: Kearney-generated from FY 2021 IG FISMA Reporting Metrics

Change in Metrics and Assessment Methodology: In FY 2018, the *IG FISMA Reporting Metrics* expanded to include an eighth domain (i.e., Data Protection and Privacy). In FY 2019, the *IG FISMA Reporting Metrics* remained largely stable with slight revisions to the attributes for *Defined*, *Consistently Implemented*, and *Managed and Measureable* to address new requirements for SCRM in the Risk Management domain and for security of domain name systems in the Data Protection and Privacy and Identity and Access Management domains. In FY 2020, the *IG FISMA Reporting Metrics* were revised to address mobile device management, enterprise mobility management, and updated guidance on the Trusted Internet Connection (TIC) initiative. In FY 2021, the *IG FISMA Reporting Metrics* introduced a new domain (i.e., SCRM) within the Identify function, implemented structural changes related to policies and procedures metrics, and introduced requirements for a Vulnerability Disclosure Program. Lastly, Kearney utilized NIST Special Publication (SP) 800-53, Revision (Rev.) 4 as criteria for the FY 2021 FISMA evaluation; NIST SP 800-53, Rev. 5 did not go into effect until September 2021 and, therefore, was not used during the FY 2021 FISMA evaluation of the SEC.

As shown in *Exhibit 3*, the foundation levels of the maturity model ensure that agencies develop sound policies and procedures, whereas the advanced levels capture the extent to which agencies institutionalize those policies and procedures (Level 3), establish performance measures (Level 4), and aim to improve and optimize performance against established goals (Level 5).

Exhibit 3: IG Assessment Maturity Levels



Source: Kearney-generated based on the FY 2021 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 annual FISMA reviews. Within the context of the maturity model, Level 4: *Managed and Measurable* represents an effective level of security at the domain, function, and overall program levels.

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

Prior Audits and Evaluations: The SEC took corrective action sufficient to close 14 recommendations from prior-year FISMA reports within FY 2021. Specifically, within FY 2021, the SEC took actions to close five of nine open recommendations from the OIG's audit of the SEC's compliance with FISMA for FY 2017⁶ (FY 2017 FISMA audit), dated March 30, 2018; three of six recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2018⁷ (FY 2018 FISMA evaluation), dated December 12, 2018; four of eight recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2019⁸ (FY 2019 FISMA evaluation), dated December 18, 2019; and two of seven recommendations from Kearney's evaluation of the SEC's compliance with FISMA for FY 2020⁹ (FY 2020 FISMA evaluation), dated December 21, 2020. To close these recommendations, among other improvements, OIT made progress in developing its processes for maintaining up-to-date hardware and [REDACTED], implementing specialized training for individuals with significant security responsibilities, updating its Configuration Management procedures to require periodic reconciliations between the software code deployed and the agency's software repository, and developing and documenting a formal process for maintaining a comprehensive inventory of information systems. In total, as of September 27, 2021, the SEC has remediated 16 of the 20 recommendations from the FY 2017 FISMA audit, eight of the 11 recommendations from the FY 2018 FISMA evaluation, five of the nine recommendations from the FY 2019 FISMA evaluation, and two of seven recommendations from the FY 2020 FISMA evaluation.

Objectives

Our overall objective was to evaluate the SEC's implementation of FISMA for FY 2021 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 nine domains in accordance with the *FY 2021 IG FISMA Reporting Metrics*:

- Risk Management
- SCRM
- Configuration Management
- Identity and Access Management

⁶ 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").

⁷ 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").

⁸ U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 558; December 18, 2019 (hereafter referred to as "FY 2019 FISMA evaluation").

⁹ U.S. Securities and Exchange Commission, Office of Inspector General, *Fiscal Year 2020 Independent Evaluation of SEC's Implementation of the Federal Information Security*, Report No. 563; December 21, 2020 (hereafter referred to as "FY 2020 FISMA evaluation").

- Data Protection and Privacy
- Security Training
- ISCM
- Incident Response
- Contingency Planning.

To assess the effectiveness and maturity of security controls identified in the *FY 2021 IG FISMA Reporting Metrics*, Kearney judgmentally selected and reviewed a non-statistical sample of eight information systems from the SEC's March 29, 2021 inventory of 87 FISMA-reportable information systems. 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.

RESULTS

Domain #1: Risk Management

The *FY 2021 IG FISMA Reporting Metrics*, in accordance with the NIST Cybersecurity Framework, consider Risk Management as the ongoing process of identifying, assessing, and responding to risk. Risk Management practices include establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, dated March 2011, states that in order to integrate the Risk Management process throughout the organization, a three-tiered approach is employed that addresses risk at the following levels: organizational (Tier 1), mission/business processes (Tier 2), and information systems (Tier 3).

Kearney assessed the SEC's Risk Management program and determined that the program's assessed maturity level is Level 3: *Consistently Implemented*, meaning the SEC consistently implemented its continuous monitoring policies, procedures, and strategies for its Risk Management processes, but quantitative and qualitative effectiveness measures were lacking. While the agency's assessed maturity remained at Level 3: *Consistently Implemented* between FYs 2020 and 2021, it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

Prior-Year Findings: Specifically, in the FY 2019 FISMA evaluation, Kearney determined that the SEC did not:

- Complete all relevant components [REDACTED] according to [REDACTED].
- Develop and document a standard [REDACTED].

Specifically, in the FY 2020 FISMA evaluation, Kearney determined that the SEC did not:

- Sufficiently integrate mobile device management controls into its Risk Management program.

Similarly, Kearney determined that many of the weaknesses within the SEC's Risk Management program identified during the FY 2019 and FY 2020 FISMA evaluations remained present in FY 2021, as listed below:

- While the SEC organized an inventory of its Interconnection Security Agreements and Memorandums of Understanding, the SEC did not complete all relevant components [REDACTED] in accordance with [REDACTED].

- While the SEC has developed a naming convention guide for its server infrastructure, the naming convention did not include other hardware assets, [REDACTED].
- [REDACTED]

These control weaknesses occurred for a variety of reasons. OIT was working to update its processes for capturing the required information for its [REDACTED] in line with [REDACTED]. Further, OIT was still working to improve its documentation related to the naming convention for its hardware assets. Lastly, OIT was in the process of developing [REDACTED]

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

Current-Year Findings: Kearney has identified additional opportunities for the agency to mature its 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 [REDACTED], security categorization, and lessons learned for cybersecurity Risk Management processes.

OIT did not consistently implement its process to include [REDACTED] and [REDACTED] into its [REDACTED]: The *FY 2021 IG FISMA Reporting Metrics* measure the extent to which agencies develop and maintain [REDACTED]. Additionally,

[REDACTED]

Finally, the SEC's [REDACTED]. This includes maintaining an accurate and complete inventory of [REDACTED] used within the agency's environment.

The SEC has defined policies, procedures, and processes to develop and maintain an up-to-date inventory of its [REDACTED] to include detailed information necessary for tracking. Specifically, the agency uses an [REDACTED], which is a centrally managed [REDACTED] information. However,

the agency did not consistently [REDACTED].

This occurred, in part, because the SEC OIT manages its [REDACTED]. Additionally, the agency's separate [REDACTED] was not yet fully mature. Further, the SEC faced [REDACTED].

Without the consistent implementation of [REDACTED] the agency will be unable to [REDACTED]. Therefore, without the effective use of [REDACTED], the agency risks [REDACTED].

The SEC did not consistently complete and maintain Federal Information Processing Standards (FIPS) Publication (PUB) 199 categorization worksheets: The *FY 2021 IG FISMA Reporting Metrics* require agencies to consistently implement their policies, procedures, and processes for system categorization, review, and communication, including for high-value assets. Additionally, the SEC OIT's *Security Assessment and Authorization Operating Procedures* require that: "After the Information System Owner approves the FIPS 199 form, the Security Assessment and Authorization [SA&A] team inputs the selected information types and impact levels into the *Security Category* tab within [REDACTED]. The SA&A Team also uploads the FIPS 199 form to [REDACTED]."

The SEC consistently implemented most of its policies, procedures, and processes for system categorization, review, and communication, including for high value assets; considered potential adverse impacts to SEC operations, organizational assets, individuals, other organizations, and the nation in its security categorizations; and used system categorization levels to guide Risk Management decisions. Additionally the SEC input security categorization information types and impact levels into [REDACTED]. However, the SEC did not complete FIPS 199 categorization worksheets (i.e. forms) for two of the eight sample systems (or 25 percent), [REDACTED] and [REDACTED], or upload the worksheets to [REDACTED] in accordance with established policies and procedures.

This occurred, in part, because the SEC did not develop or define requirements for consistently completing and maintaining FIPS 199 categorization worksheets for all system types.

Without consistently completing and maintaining FIPS 199 categorization worksheets for [REDACTED], the SEC may not consider agency-specific security risks included with the introduction of a [REDACTED]. Additionally, without a complete security categorization process, the SEC risks not considering all potential adverse impacts to the agency's confidentiality, integrity, and availability.

The SEC did not consistently capture, document, and share lessons learned for the effectiveness of cybersecurity Risk Management activities: The *FY 2021 IG FISMA Reporting Metrics* require agencies to consistently capture and share lessons learned on the effectiveness of cybersecurity Risk Management processes, as well as update the program accordingly. Additionally, NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations*, states: “Incorporating lessons learned facilitates the consistent progression of the continuous monitoring and ongoing authorization implementation...” Furthermore, the Cybersecurity Framework states that: “The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators.”

The SEC defined and communicated the policies, procedures, and processes it utilizes for managing cybersecurity risks associated with operating and maintaining its information systems. In addition, the SEC ensured its policies, procedures, and processes cover cybersecurity risk management at the organizational, mission, business process, and information system levels and address risk framing, assessment, response, and monitoring. However, the SEC did not consistently capture, document, and share lessons learned on the effectiveness of its cybersecurity risk management processes.

This occurred, in part, because the SEC is still in the process of documenting formal procedures for consistently capturing, documenting, and sharing lessons learned for the agency’s effectiveness of cybersecurity Risk Management activities.

Without a formal process for consistently capturing, documenting, and sharing lessons learned, the agency risks not adapting its cybersecurity Risk Management program based on previous and current cybersecurity activities or the ever-evolving cybersecurity landscape.

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

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

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

Recommendation 1: Develop, document, and implement a process for consistently implementing [REDACTED] within the agency’s [REDACTED].

Management Response. We concur. Our work in further enhancing the agency’s [REDACTED] continues, including in response to OIG’s prior recommendations in Report 562. As part of this ongoing work, OIT is in the process of

incorporating reviews of [REDACTED] into the Service Delivery Framework (SDF) lifecycle processes. As part of the remediation activity associated with CAP 562-06, SDF phases will include processes to add approved [REDACTED] to the [REDACTED] and [REDACTED] in the SEC's [REDACTED]. This effort will be documented in OIT operating procedures. Management's complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

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

Recommendation 2: Develop, document, and implement a process to clearly define requirements for consistently completing and maintaining Federal Information Processing Standards Publication 199 categorization worksheets for all system types.

Management Response. We concur. OIT will further develop, document, and implement requirements for consistently completing and maintaining Federal Information Processing Standards Publication (FIPS) 199 categorization worksheets for all system types. In particular, the requirements will indicate when an SEC-specific FIPS 199 categorization form is required, and when it is acceptable to accept and maintain a FIPS 199 categorization from an appropriate Federal government agency or partner organization. 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: Develop, document, and implement a formal process to consistently capture and share lessons learned on the effectiveness of its cybersecurity Risk Management program and make updates, as necessary.

Management Response. We concur. OIT will develop, document, and implement such a process with respect to its cybersecurity Risk Management program and make updates, as necessary. 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.

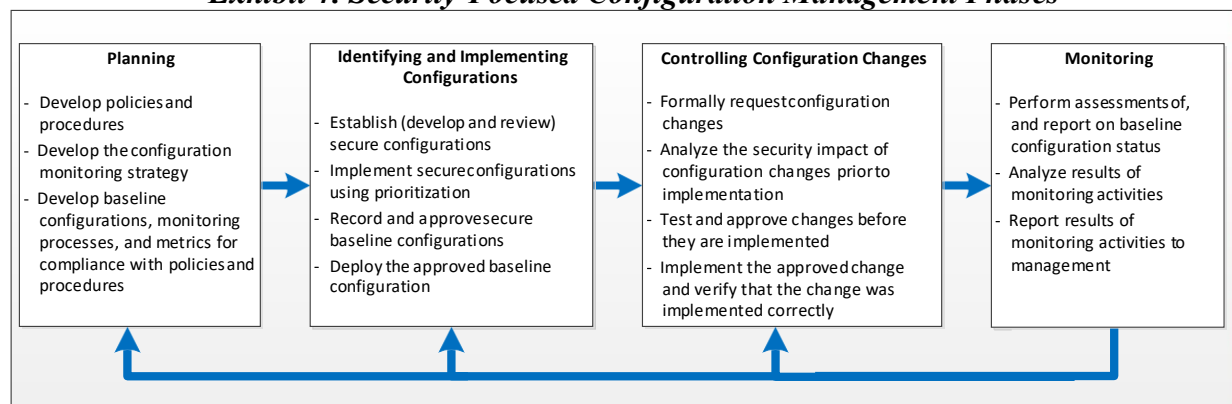
Domain #2: SCRM

The *FY 2021 IG FISMA Reporting Metrics* excludes the SCRM domain from being considered for the Identify function rating. Observations within FY 2021 related to the SCRM domain are summarized in the **Other Matters of Interest** section.

Domain #3: Configuration Management

The *FY 2021 IG FISMA Reporting Metrics*, in accordance with NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, dated August 2011, consider Configuration Management an important process for establishing and maintaining secure information system configurations, in addition to providing important support for managing security risks in information systems. Configuration management activities include developing baseline configurations,¹⁰ establishing a configuration change control process, implementing a configuration monitoring and reporting process, and implementing a Vulnerability Disclosure Policy. 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 represent the most secure state consistent with operational requirements and constraints. In addition, NIST SP 800-53, Rev. 4, CM-3 (f), “Configuration Change Control,” states that organizations should audit and review activities associated with configuration-controlled changes to the information system. Further, NIST SP 800-53, Rev. 4, SI-2, “Flaw Remediation,” states that organizations should identify, report, and correct information system flaws. Finally, as described in *Exhibit 4*, security-focused Configuration Management of information systems involves a set of activities that can be organized into the following four major phases: 1) Planning; 2) Identifying and Implementing Configurations; 3) Controlling Configuration Changes; and 4) Monitoring.

Exhibit 4: Security-Focused Configuration Management Phases



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

¹⁰ 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.

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 it did not consistently implement them. The SEC's assessed maturity remained at Level 2: *Defined* between FYs 2020 and 2021, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

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

- Fully define [REDACTED] or review and update system security plans ([REDACTED]) at least annually or within established schedules.
- Adequately implement [REDACTED].

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

- [REDACTED]

Further, in the FY 2020 FISMA evaluation, Kearney determined that the SEC did not:

- [REDACTED] as required by OMB M-19-26.

Similarly, Kearney determined that many of the weaknesses within the SEC's Configuration Management program identified during the FY 2017 FISMA audit and the FYs 2018 and 2020 FISMA evaluations remained present in FY 2021, as listed below:

- The SEC did not consistently implement its [REDACTED].
- The SEC has not developed, documented, and disseminated its policies and procedures for [REDACTED].
- The SEC did not [REDACTED].
- The SEC did not [REDACTED].

within the defined timeframes listed in the agency's Vulnerability Management Policy.

- The SEC did not define a performance measure for an acceptable target level of [REDACTED].
- The SEC was [REDACTED] one of eight sampled systems (about 13 percent).
- The SEC did not create [REDACTED] and [REDACTED] in accordance with SEC policy 24.04.04. Specifically, [REDACTED] for [REDACTED] had associated [REDACTED] for [REDACTED] had an associated [REDACTED].
- The SEC did not update its Configuration Management procedures to require that [REDACTED].
- The SEC did not define its processes to develop, maintain, and report an accurate [REDACTED].

The above weaknesses occurred because SEC management had not fully addressed management challenges identified in FYs 2017, 2018, and 2020. While the SEC continued to increase its [REDACTED] for all SEC systems. In addition, the SEC is still in the process of updating [REDACTED]. Further, while the SEC has made improvements to its vulnerability management documentation and capabilities, the agency is still working [REDACTED]. Additionally, OIT was working to update its POA&M requirements in the agency's [REDACTED]. Further, the SEC is also in the process of updating [REDACTED] policies and procedures to define a performance measure for an acceptable target level of approved [REDACTED] across the agency. Also, while the SEC made updates to its Configuration Management procedures regarding [REDACTED]. Finally, OIT's Network Engineering Branch is developing an operating procedure to define [REDACTED].

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

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

In addition to the prior-year findings, Kearney identified new weaknesses related to the SEC's documentation of lessons learned and [REDACTED].

The SEC did not consistently capture and share lessons learned to improve its configuration baseline policies and procedures: The *FY 2021 IG FISMA Reporting Metrics* require agencies to utilize lessons learned in implementation to make improvements to its baseline configuration policies and procedures. Additionally, the NIST Cybersecurity Framework states: "The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators."

The SEC defined, developed, and disseminated its baseline configuration and component inventory policies and procedures. However, the SEC did not consistently capture and share lessons learned to assess the effectiveness of its baseline configuration policies and procedures and make configuration baseline program updates, as appropriate.

This occurred, in part, because while the SEC held discussions for its Configuration Management program where issues and concerns are addressed, the agency has not defined a formal process to consistently capture and share lessons learned related to baseline configuration activities.

Without a formal process for consistently capturing and sharing lessons learned, the agency risks not adapting its configuration baseline program based on previous and current Configuration Management activities or the ever-evolving cybersecurity landscape.

The SEC OIT did not consistently [REDACTED]: To achieve the consistently implemented maturity level, the *FY 2021 IG FISMA Reporting Metrics* require agencies to consistently implement its change control policies, procedures, and processes, including explicit consideration of security impacts prior to implementing changes. Additionally, NIST SP 800-53, Rev. 4, CM-3, "Configuration Change Control," states: "Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems." Further, NIST SP 800-53, Rev. 4, CM-3 (2), states: "The organization tests, validates, and documents changes to the information system before implementing the changes on the operating system."

The SEC defined, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures addressed, at a minimum, the necessary configuration change control-related activities. However, the SEC did not consistently

This occurred, in part, because the SEC has not defined in its Configuration Management or related policies and procedures which proposed change types

Without the consistent completion of , the agency risks implementing changes with unforeseen adverse effects or changes to information system operations.

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

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

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

Recommendation 4: Develop, document, and implement a formal process to consistently capture and share lessons learned on the effectiveness of its configuration baseline program and make updates, as necessary.

Management Response. We concur. OIT will develop, document, and implement such a process regarding the agency's configuration baseline program and make updates, as necessary. 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: Develop, document, and implement a formal process that clearly defines requirements for all configuration change types at the SEC or configuration changes

Management Response. We concur. OIT will review the existing change management documentation and update, as necessary, the process and definitions for configuration change types and associated [REDACTED], to ensure the [REDACTED]

[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: Identity and Access Management

The *FY 2021 IG FISMA Reporting Metrics*, in accordance with the NIST Cybersecurity Framework, require agencies to establish an Identity and Access Management program that limits access to physical and logical assets and associated facilities to authorized users, processes, and devices, and it is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. NIST SP 800-53, Rev. 4, AC-1, "Access Control Policy and Procedures," and IA-1, "Identification and Authentication Policy and Procedures," require organizations to develop, document, and disseminate an access control policy and 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 it did not consistently implement them. While the agency continued to make improvements, the SEC's assessed maturity remained at Level 2: *Defined* between FYs 2020 and 2021, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

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

- [REDACTED]

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

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

Further, in the FY 2020 FISMA evaluation, Kearney determined that the SEC did not:

- Implement or document processes and procedures for performing risk-based reviews [REDACTED].

Similarly, Kearney determined that many of the weaknesses within the SEC's Identity and Access Management program identified during the FY 2017 FISMA audit and FY 2019 and FY 2020 FISMA evaluations remained present in FY 2021, as listed below:

- The SEC had not completed the implementation of [REDACTED].
- The SEC did not develop policies and procedures for enforcing [REDACTED].
- The SEC had not consistently implemented the Identity Credential and Access Management policy for performing [REDACTED] on a [REDACTED] basis. The SEC had not documented all completed [REDACTED] for three of eight sampled systems, including [REDACTED] and its subcomponents, and [REDACTED].
- Kearney observed 32 out of 42 (about 76 percent) active accounts that had [REDACTED] in the description, yet did not follow the defined [REDACTED].
- The SEC did not define or document the process for performing risk-based reviews [REDACTED].

These control weaknesses occurred, in part, because the SEC was in the process of remediating its [REDACTED]; however, the agency

was targeting [REDACTED]. Further, the OIT was in the process of updating the [REDACTED]

[REDACTED] Also, while the SEC had defined a [REDACTED], the agency did not have an established process for performing [REDACTED]

[REDACTED] Finally, while the agency stated that its corrective action plan for defining a process for risk-based reviews [REDACTED] was complete, the agency's updated documentation did not evidence that the agency had defined or documented a process for performing risk-based reviews [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 #5: Data Protection and Privacy

The NIST Cybersecurity Framework requires agencies to manage information and records (data) consistent with the organization's risk strategy to protect the confidentiality,¹¹ 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.

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 its quantitative and qualitative effectiveness measures were lacking. The SEC's assessed maturity for Data Protection and Privacy remained at Level 3: *Consistently Implemented* between FYs 2020 and 2021, as it has not fully implemented the recommendations identified in prior years; therefore, certain previously identified conditions still exist.

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

¹¹ According to 44 United States Code (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."

- Implement security controls to protect [REDACTED]

Additionally, in the FY 2020 FISMA evaluation, Kearney determined that the SEC did not:

- [REDACTED]

Similarly, Kearney determined that many of the weaknesses within the SEC's Data Protection and Privacy program identified during the FYs 2018 and 2020 FISMA evaluations remained present in FY 2021, as listed below:

- The SEC did not consistently implement [REDACTED]

- [REDACTED]

These control weaknesses occurred for a variety of different reasons. OIT stated that it was still in the process of addressing its [REDACTED] related to a prior OIG recommendation. Further, OIT stated that it did not perform [REDACTED]

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

Current-Year Finding: Kearney has identified additional opportunities for the agency to mature its Data Protection and Privacy program. See the finding detailed below.

In addition to the prior-year findings, Kearney identified new weaknesses related to its PII inventory.

OIT did not clearly document or maintain its process for maintaining a complete inventory of the collection and use of PII: The *FY 2021 IG FISMA Reporting Metrics* require agencies to maintain an inventory of the collection and use of PII. Additionally, NIST SP 800-53, Rev. 4, Appendix J, SE-1, states that the organization establishes, maintains, and updates an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

The SEC consistently implemented its privacy program by dedicating appropriate resources to the program, maintaining an inventory of the collection and use of PII, conducting and maintaining privacy impact analyses, and removing unnecessary PII on a regular basis. However, while the SEC maintained an inventory of the collection and use of PII, the agency did not clearly document or maintain a complete PII inventory that contains a listing of all programs and information systems. Specifically, the [REDACTED] inventory fields were inconsistent with the Privacy Analysis Worksheets for two of the eight sampled systems (i.e., [REDACTED] and [REDACTED]).

This occurred, in part, because the SEC is still in the process of fully updating its Governance Risk and Compliance tool to include its PII inventory capabilities.

Without a clearly documented process for maintaining a complete inventory of the collection and use of PII for all programs and information systems, the agency risks the possibility of unintended PII exposure for its systems or programs that collect or utilize PII.

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

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

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

Recommendation 6: Develop and document a process for maintaining a complete inventory of the collection and use of Personally Identifiable Information that includes a listing of all programs and information systems.

Management Response. We concur. OIT will review, update, and document, as necessary, the Privacy and Information Assurance team's process for maintaining a complete inventory of the collection and use of Personally Identifiable Information (PII) that includes a listing of all programs and information systems. 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: Security Training

FISMA requires agencies to establish an information security program that includes security awareness training.¹² 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 Cybersecurity Workforce Framework*, dated August 2017, provides guidance on a superset of cybersecurity knowledge, skills, and abilities and tasks for each work role. The *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* supports consistent organizational and sector communication for cybersecurity education, training, and workforce development. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, dated October 2003, mandates that organizations monitor their Information Security Training program for compliance and effectiveness and that failure to encourage IT security training puts an agency 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 5: *Optimized*, meaning the SEC’s policies, procedures, and strategies for Security Training are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs. The SEC’s assessed maturity increased drastically from Level 2: *Defined* in FY 2020 to Level 5: *Optimized* in FY 2021.

Prior-Year Findings: Specifically, in the FY 2020 FISMA evaluation, the OIG determined that the SEC did not:

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

Similarly, Kearney determined that the weaknesses with the SEC’s Security Training program identified during the FY 2020 FISMA evaluation remained present in FY 2021 as listed below:

- The SEC did not utilize its results from the assessments of knowledge, skills, and abilities to update the agency’s Security Training strategy.

Kearney identified the reasons for the above control weakness. The agency is in the process of updating its OIT Security Learning and Development Strategic Plan, which will include

¹² 44 U.S.C. Section 3554 (a) (4)

guidance regarding the utilization of results from the assessments of knowledge, skills, and abilities to address gaps within the agency's Security Training program.

Kearney is not making any new recommendations in this area, as the SEC is still working to resolve all prior-year FISMA recommendations and achieved Level 5: *Optimized*. See [APPENDIX II: OPEN FISMA RECOMMENDATIONS](#).

Domain #7: ISCM

The *FY 2021 IG FISMA Reporting Metrics* require agencies to establish an information security program that includes ISCM. ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational Risk Management decisions. The output of a strategically designed and well-managed organization-wide ISCM program can be used to maintain a system's authorization to operate and keep required system information and data up to date on an ongoing basis. According to NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, dated September 2011, organizations should take steps to establish, implement, and maintain an ISCM program, including defining an ISCM strategy, analyzing and reporting findings, and reviewing and updating the ISCM strategy and program, as necessary. In addition, OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, dated November 2013, states that agencies were required to implement continuous monitoring of security controls as part of a phased approach through FY 2017.

Kearney assessed the SEC's ISCM program and determined that the program's assessed maturity level was Level 3: *Consistently Implemented*, consistent with FY 2020, meaning the SEC formalized and consistently implemented its continuous monitoring policies, procedures, and strategies for ongoing authorization, but its quantitative and qualitative effectiveness measures were lacking.

Current-Year Finding: Kearney has identified additional opportunities for the agency to mature its ISCM program. See the finding detailed below.

OIT did not consistently capture and share formal lessons learned to improve the effectiveness of ISCM policies and strategy: The *FY 2021 IG FISMA Reporting Metrics* require agencies to consistently capture lessons learned to improve the effectiveness of its ISCM policies and strategy. Additionally, the NIST Cybersecurity Framework states: "the organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators."

The SEC consistently implemented its ISCM policies and strategy at the organization/business process level and information systems levels and discussed improvements towards its ISCM program. However, the SEC did not consistently capture and share formal lessons learned to improve the effectiveness of its ISCM policies and strategy.

This occurred, in part, because while the SEC continually evaluates its ISCM policies and strategy for improvements, the agency had not developed a formal process for consistently capturing and sharing lessons learned on the effectiveness of its ISCM policies and strategy.

Without a formal process for consistently capturing and sharing lessons learned, the agency risks not adapting its ISCM program based on previous and current ISCM activities or the ever-evolving cybersecurity landscape.

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

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

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

Recommendation 7: Develop, document, and implement a formal process to consistently capture and share lessons learned to improve the effectiveness of its Information Security Continuous Monitoring policies and strategy and make updates, as necessary.

Management Response. We concur. OIT will develop, document, and implement such a process for its Information Security Continuous Monitoring policies and strategy and make updates, as necessary. 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 #8: 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*, dated 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 4: *Managed and Measurable*, meaning the SEC formalized strategies for collecting quantitative and qualitative effectiveness measures to promote continuous improvement. The agency's assessed maturity remained consistent at Level 4:

Managed and Measurable between FYs 2020 and 2021. While the agency's Incident Response program is effective, the SEC did not fully implement a recommendation identified in a prior year.

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

- Review and update Incident Response plans, policies, procedures, and strategies to:
1) address all common threat and attack vectors and the characteristics of each particular situation; 2) identify and define performance metrics that will be used to measure and track the effectiveness of the agency's Incident Response program; 3) 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; 4) define Incident Response communication protocols and incident handlers' training requirements; and 5) remove outdated terminology and references.

Similarly, Kearney determined that the weaknesses with the SEC's Incident Response program identified during the FY 2017 FISMA audit remained present in FY 2021 as listed below:

- While the SEC has a defined Incident Response Plan, the SEC did not define metrics for measuring the effectiveness of its Incident Response capabilities or defined procedures for incident handler training.

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

Kearney is not making any new recommendations in this area, as the SEC is working to address the prior-year FISMA recommendation. Additionally, Kearney determined that the SEC's Incident Response program achieved Level 4: *Managed and Measurable* and, therefore, is effective. See [APPENDIX II: OPEN FISMA RECOMMENDATIONS](#).

Domain #9: 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.¹³ Because information system resources are essential to an organization's success, it is critical that systems are able to operate effectively without excessive interruption. Contingency Planning supports this requirement by establishing thorough plans, procedures, and

¹³ 44 U.S.C. Section 3554 (b) (8)

technical measures that can enable a system to be recovered as quickly and efficiently as possible following a disaster. NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010, states that Contingency Planning activities include developing the planning policy, creating contingency strategies, maintaining contingency plans, conducting Business Impact Analyses, testing contingency plans, and conducting exercises. In addition, NIST SP 800-53, Rev. 4, CP-4, “Contingency Plan Testing and Exercises,” requires organizations to perform periodic testing of contingency plans to determine the effectiveness and organizational readiness to execute the plan. Additionally, NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, CP-1, “Contingency Planning Policies and Procedures, Supplemental Information and Communications Technology (ICT) Supply Chain Risk Management Guidance,” dated April 2015, states that organizations should integrate ICT supply chain concerns into the Contingency Planning policy.

Kearney assessed the SEC’s Contingency Planning program and determined that the program’s maturity level is Level 4: *Managed and Measureable*, meaning the SEC formalized strategies for collecting quantitative and qualitative effectiveness measures to promote continuous improvement. The SEC maintained this rating from FYs 2020 to 2021.

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

- Consistently implement information system Contingency Planning policies, procedures, and strategies for information system Contingency Planning, as the SEC did not integrate ICT supply chain concerns and risks into its Contingency Planning policies and procedures.

Similarly, Kearney determined that the weakness with the SEC’s Contingency Planning program identified during the FY 2017 FISMA audit remained present in FY 2021, as listed below:

- The SEC has not defined an SCRM strategy which addresses the agency’s Information and Communications Technology Supply Chain risks with respect to Contingency Planning activities.

This control weakness occurred, in part, because SCRM requirements were introduced with NIST SP 800-53, Rev. 5 at the beginning of FY 2021 and will not take effect until September 2021; thus, the agency is still working to identify gaps and remediate any issues related to the newly introduced standard.

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

Kearney identified a new weakness regarding the SEC’s information system contingency plan testing:

OIT did not consistently utilize automation to test its information system contingency plans: The *FY 2021 IG FISMA Reporting Metrics* require agencies to employ automated mechanisms to test system contingency plans more thoroughly and effectively. Additionally, NIST SP 800-53 Rev.4, CP-4 (3), “Automated Testing,” states: “the organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.”

The SEC consistently implemented information system contingency plan testing and exercises and integrated information system contingency plan testing and exercises with testing of related plans as well as coordinating information system contingency plan testing with external stakeholders. However, the SEC did not consistently utilize automation for all systems to conduct thorough and effective testing of its information system contingency plans.

This occurred, in part, because while the SEC has implemented automated testing mechanisms for some of its information systems, the agency has been unable to consistently utilize automated testing to all systems due to [REDACTED].

Without the consistent utilization of automation for testing information system contingency plans, the SEC lacks thorough and effective testing, as automated testing mechanisms provide more complete coverage of contingency issues, more realistic scenarios and environments for testing, and more effective stressing of information systems and supported missions.

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

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

Recommendation 8: Develop, document, and implement a process to consistently utilize automated testing for information system contingency plan efforts, [REDACTED].

Management Response. We concur. OIT will evaluate the ability to utilize automated testing as part of contingency planning efforts to include conferring with other agencies and performing market research of potential vendor solutions. As applicable, OIT will use the results of its evaluation to update its Enterprise Disaster Recovery Plan. Management’s complete response is reprinted in [APPENDIX IV: MANAGEMENT COMMENTS](#).

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

OVERALL CONCLUSION

Overall, the SEC has made progress in improving its information security program by refining its management of security training roles and responsibilities, enhancing its security training strategy, implementing the agency's policy for specialized security training, [REDACTED], [REDACTED], optimizing a Vulnerability Disclosure Policy, refining its configuration management processes related to reconciliation of software code in production, improving its incident response information sharing capabilities, and improving its Contingency Planning capabilities. These improvements occurred despite the agency facing challenges presented by the ongoing Coronavirus Disease 2019 pandemic, which included a significant increase in telework. While the SEC made program improvements and achieved Level 4: *Managed and Measurable* in two of the nine *FY 2021 IG FISMA Reporting Metrics* areas and Level 5: *Optimized* in one of the nine metrics areas, Kearney noted that the SEC's information security program did not meet the *FY 2021 IG FISMA Reporting Metrics*' definition of "effective" because the program's overall maturity did not reach Level 4: *Managed and Measurable*. Specifically, the agency faced challenges with developing a Supply Chain Risk Management program, managing its FIPS PUB 199 documentation for its information systems, [REDACTED], and utilizing lessons learned in its Information Security Continuous Monitoring practices. Finally, fully addressing the remaining OIG FY 2017 recommendations, as well as implementing Kearney's FYs 2018, 2019, 2020 and 2021 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 to 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 SCRM domain. These include opportunities that will increase the agency's ability to strengthen its security and privacy controls, but they did not rise to the significance of a formal finding as the requirements for the SCRM domain were outlined in NIST SP 800-53, Rev. 5, which took effect in September 2021.

The SEC did not completely define and develop its SCRM program: The *FY 2021 IG FISMA Reporting Metrics* require agencies to: develop an organization-wide SCRM strategy; develop policies and procedures for managing SCRM activities at all organizational tiers; ensure that systems, system components, and services are consistent with the agency's supply chain requirements; [REDACTED]

[REDACTED]. Additionally, NIST SP 800-53, Rev. 5, PM-30, "Supply Chain Risk Management Strategy," states that organizations should develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. Additionally, NIST SP 800-53, Rev. 5, SR-1, "Supply Chain Risk Management Policy and Procedures" notes that the organization should develop, document, and disseminate an SCRM policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Further, NIST SP 800-53, Rev. 5, SR-3, "Supply Chain Controls and Processes" states that organizations should establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes.

[REDACTED]

While the SEC initiated the process for defining an SCRM policy and strategy, the strategy was incomplete, as it did not define SCRM strategies and controls, processes for monitoring and communicating the SCRM strategy, processes for monitoring supply chain risk, and an SCRM risk appetite. Additionally, the SEC did not define formal SCRM policies and procedures that included roles and responsibilities for SCRM processes. Further, the SEC did not define policies and procedures to ensure that organizationally defined products, systems, and services adhere to SCRM requirements. [REDACTED]

[REDACTED]

This occurred, in part, because SCRM requirements were introduced with NIST SP 800-53, Rev. 5, at the beginning of FY 2021 and agencies are expected to meet the requirements of, and be in compliance with this publication within one year from the publication date; thus, the agency is still working to identify gaps and remediate any issues related to the newly introduced standard.

Without an SCRM strategy, the agency may be unable to effectively implement and manage controls for maintaining an acceptable level of risk for supply chain activities. Without SCRM policies and procedures, the SEC may not have documented processes for responding to, monitoring, and assigning responsibility for supply chain risks. Additionally, without ensuring systems, system components, and services are consistent with the agency's supply chain requirements, the SEC may introduce systems, services, or system components into the agency that cause adverse or harmful effects to its infrastructure. [REDACTED]

Kearney encourages the SEC to develop and document SCRM policies and procedures that include processes for responding to and monitoring supply chain risk; a process for ensuring systems, system components, and services are consistent with SEC supply chain requirements; and a process for [REDACTED]. Additionally, Kearney encourages the SEC to develop a SCRM strategy that guides the SEC in maintaining an acceptable level of risk for supply chain activities.

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

APPENDIX I: SCOPE AND METHODOLOGY

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

Scope: Our overall objective was to assess the SEC's implementation of FISMA and respond to the *FY 2021 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, 2020 and September 27, 2021 and addressed the following nine domains specified in DHS's reporting instructions for FY 2021:

- Risk Management
- SCRM
- 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 a sample of eight of the SEC's 87 FISMA-reportable systems (about 9 percent). The sample consisted of internally and externally hosted systems shown in *Exhibit 5*.¹⁴ In addition, to address the requirements of the *FY 2021 IG FISMA Reporting Metrics* for the Identity and Access Management, Security Training, Configuration Management, and Incident Response domains, we judgmentally selected and reviewed a non-statistical sample of controls related to those domains. This included a random sample of 25 of 638 (about 4 percent) contractors onboarded during FY 2021 to evaluate the SEC's implementation of access agreements and security awareness training, a random sample of 10 of 101 (about 10 percent) configuration management changes to assess the agency's change control process, and a random sample of 25 of 1,207 (about 2 percent) security incidents to assess the incident response process. Because sampled items were non-statistical, Kearney did not project our results and conclusions to the total user population or measure overall prevalence.

¹⁴ We selected information systems based on the SEC's inventory of FISMA-reportable systems maintained in OIT's system of record as of April 12, 2021. The inventory included 87 FISMA-reportable information systems (i.e., 54 SEC-operated and 33 contractor-operated). We selected eight FISMA-reportable information systems, factoring in: 1) systems that were not previously tested in the prior three years; 2) systems that were categorized as "moderate" or "high" under FIPS PUB 199; and 3) systems that contain sensitive and confidential information, including PII data. We also solicited OIT's input for our sample selection.

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Source: [REDACTED] enterprise Governance Risk and Compliance tool, SEC System of Record

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

- Occurred between January 1, 2020 and April 9, 2021.
- Were confirmed as having compromised the confidentiality, integrity, or availability of information.

According to OIT’s records, 1,207 incidents occurred between January 1, 2020 and April 9, 2021. Based on our established criteria, we selected and reviewed a random sample of 25 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 2021 IG FISMA Reporting Metrics*. We interviewed key personnel, including staff from OIT's Policy and Compliance Branch and Security Engineering Branch. Kearney also examined documents and records relevant to the SEC's information security program, including applicable Federal laws and guidance; SEC administrative regulations, policies, and procedures; system-level documents; and reports. As discussed throughout this report, these included, but were not limited to, the following:

- Federal Information Security Modernization Act of 2014, PL 113-283
- E-Government Act of 2002, PL 107-347
- Applicable OMB guidance, including OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 2016, and OMB M-16-04, *Cybersecurity Strategy and Implementation Plan 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 2021 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.

Data Reliability: The Government Accountability Office's (GAO) *Assessing Data Reliability* (GAO-20-283G, December 2019) states reliability of data means that data are applicable for audit purpose and are sufficiently complete and accurate. Data primarily pertains to information that is entered, processed, or maintained in a data system and is generally organized in, or derived from, structured computer files. Furthermore, GAO-20-283G defines "applicability for audit purpose," "completeness," and "accuracy" as follows:

- "Applicability for audit purpose" refers to whether the data, as collected, are valid measures of the underlying concepts being addressed in the audit's research objectives
- "Completeness" refers to the extent that relevant data records and fields are present and sufficiently populated

- “Accuracy” refers to the extent that recorded data reflect the actual underlying information.

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

Prior Coverage: The SEC took corrective action sufficient to close 14 total recommendations from prior-year FISMA reports within FY 2021. Specifically, within FY 2021, the SEC took action to close five of nine open recommendations from the OIG’s audit of the SEC’s compliance with FISMA for FY 2017 (FY 2017 FISMA audit), dated March 30, 2018; three of six recommendations from Kearney’s evaluation of the SEC’s compliance with FISMA for FY 2018 (FY 2018 FISMA evaluation), dated December 12, 2018; four of eight recommendations from Kearney’s evaluation of the SEC’s compliance with FISMA for FY 2019 (FY 2019 FISMA evaluation), dated December 18, 2019; and two of seven recommendations from Kearney’s evaluation of the SEC’s compliance with FISMA for FY 2020 (FY 2020 FISMA evaluation), dated December 21, 2020. 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 and evaluations.

SEC OIG audit and evaluation reports, including the FYs 2017, 2018, 2019, 2020, and 2021 FISMA reports, can be accessed at: <https://www.sec.gov/oig>.

APPENDIX II: OPEN FISMA RECOMMENDATIONS

Exhibit 6 lists all FISMA recommendations that remain open from prior FISMA audits and evaluations as of September 27, 2021.

Exhibit 6: Open FISMA Recommendations

Domain	Open Recommendations
FY 2017	
Configuration Management (Identify)	<p>Recommendation 8: Develop, review, and approve secure baselines for all systems included in the SEC's [REDACTED]</p> <p>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 address [REDACTED], including those issues and vulnerabilities identified as unmitigated at the time of our audit.</p>
Information Access Management (Identify)	<p>Recommendation 12: [REDACTED]</p>
Incident Response (Respond)	<p>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.</p>
FY 2018	
Configuration Management (Identify)	<p>Recommendation 1: Update configuration management procedures to require that [REDACTED]</p>
Data Protection and Privacy (Protect)	<p>Recommendation 3: Complete initiatives to implement an [REDACTED]</p> <p>Recommendation 4: Complete initiatives to implement [REDACTED]</p>

Domain	Open Recommendations
FY 2019	
Risk Management (Identify)	<p>Recommendation 2: Complete all relevant components of the [REDACTED], including [REDACTED] expiration and review date, according to [REDACTED].</p> <p>Recommendation 4: Develop and document a [REDACTED].</p> <p>Recommendation 5: a) Develop a methodology to demonstrate the control assignments from NIST SP 800-53, Rev. 4, including control tailoring and inheritance and b) update the SEC's SSP templates to ensure control tailoring justification corresponds to the methodology covered in Recommendation a).</p>
Information Access Management (Identify)	<p>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 SEC [REDACTED].</p>
FY 2020	
Risk Management (Identify)	<p>Recommendation 1: Develop and document: a) agency requirements for applying security and operating system updates to mobile devices in an organizationally defined timeframe; [REDACTED].</p>
Configuration Management (Identify)	<p>Recommendation 2: Develop and document a process to consistently [REDACTED].</p>
Information Access Management (Identify)	<p>Recommendation 3: Develop and document processes for performing risk-based reviews [REDACTED] on an organizationally defined frequency.</p>
Security Training (Protect)	<p>Recommendation 6: Define and implement a process to incorporate results from the assessments of knowledge, skills, and abilities into the security training strategy.</p>

Domain	Open Recommendations
Contingency Planning (Recover)	<p>Recommendation 7: a) Identify and define the SEC's information and communications technology supply chain risks; b) develop and define a supply chain risk management strategy which addresses the agency's information and communications technology supply chain risks with respect to Contingency Planning activities; and c) incorporate the supply chain risk management strategy into Contingency Planning policies and procedures.</p>

Source: Kearney-generated based on OIG analysis of open and closed recommendations from SEC OIG Reports No. 546, No. 552, No. 558, and No. 563

APPENDIX III: SUMMARY OF ASSESSED FISMA RATINGS, FY 2020 & FY 2021

Exhibit 7 lists the individual *FY 2021 IG FISMA Reporting Metrics* metric ratings for the SEC in FYs 2020 and 2021, as well as the determination of “effective” or “not effective” for each metric in FY 2021. Individual metrics are colored to highlight where the SEC improved or regressed between FYs 2020 and 2021. See the key below.

Exhibit 7: Summary of Assessed FISMA Ratings between FY 2020 and FY 2021

Green: Indicates the assessed rating went up from FY 2020 to FY 2021
Red: Indicates the assessed rating went down from FY 2020 to FY 2021

Domain	#	Metric Title	2020 Assessed Rating	2021 Assessed Rating	2021 Effective/Not Effective	
Identify	Risk Management	1	Inventory of Information Systems and System Interconnections	Defined	Defined	Not Effective
		2	Inventory of Hardware Assets	Consistently Implemented	Consistently Implemented	Not Effective
		3	Inventory of Software Assets	Ad Hoc	Defined	Not Effective
		4	Security Categorization and High Value Assets	Managed and Measurable	Consistently Implemented	Not Effective
		5	Risk Management Policies, Procedure, Strategy	Defined	Defined	Not Effective
		6	Information System Security Risk Management	Defined	Defined	Not Effective
		7	Risk Management Roles and Responsibilities	Defined	Optimized	Effective
		8	POA&M Maintenance	Consistently Implemented	Consistently Implemented	Not Effective
		9	Risk Communication	Managed and Measurable	Managed and Measurable	Effective
		10	Enterprise-Wide View of Risks	Managed and Measurable	Managed and Measurable	Effective
	Overall 11	Assessed Conclusion	Consistently Implemented	Consistently Implemented	Not Effective	
	SCRM	12	SCRM Strategy	Not applicable (N/A)	Ad-Hoc	Not Effective
		13	SCRM Policies and Procedures	N/A	Ad-Hoc	Not Effective
		14	Acquisition and Assessment Processes for Third-Party Providers	N/A	Ad-Hoc	Not Effective
		15	Counterfeit Components Handling	N/A	Ad-Hoc	Not Effective
	Overall 16	Assessed Conclusion	N/A	Ad-Hoc	Not Effective	
Configuration Management		17	Configuration Management Roles and Responsibilities	Defined	Defined	Not Effective
		18	Enterprise-Wide Configuration Management Plan	Defined	Defined	Not Effective
		19	Baseline Configuration	Defined	Defined	Not Effective

Domain	#	Metric Title	2020 Assessed Rating	2021 Assessed Rating	2021 Effective/Not Effective
	20	Configuration Settings	Defined	Defined	Not Effective
	21	Flaw Remediation	Defined	Defined	Not Effective
	22	Trusted Internet Connection Adoption	Defined	Consistently Implemented	Not Effective
	23	Configuration Change Control	Defined	Defined	Not Effective
	24	Vulnerability Disclosure Policy	N/A	Optimized	Effective
Overall	25	Assessed Conclusion	Defined	Defined	Not Effective
Identity and Access Management	26	Identity and Access Management Roles and Responsibilities	Consistently Implemented	Defined	Not Effective
	27	Identity Credential and Access Management Policies and Strategy	Consistently Implemented	Consistently Implemented	Not Effective
	28	Personnel Risk Designations	Consistently Implemented	Managed and Measurable	Effective
	29	Access Agreements	Optimized	Optimized	Effective
	30	Strong Authentication – Non-Privileged	Defined	Defined	Not Effective
	31	Strong Authentication – Privileged	Defined	Defined	Not Effective
	32	Privileged Account Management	Defined	Defined	Not Effective
	33	Remote Access Configurations	Defined	Defined	Not Effective
Overall	34	Assessed Conclusion	Defined	Defined	Not Effective
Data Protection and Privacy	35	Privacy Program	Consistently Implemented	Consistently Implemented	Not Effective
	36	Protection of PII and Sensitive Data	Defined	Defined	Not Effective
	37	Data Exfiltration Prevention	Consistently Implemented	Consistently Implemented	Not Effective
	38	Data Breach Response Plan	Consistently Implemented	Consistently Implemented	Not Effective
	39	Privacy Awareness Training	Optimized	Optimized	Effective
Overall	40	Assessed Conclusion	Consistently Implemented	Consistently Implemented	Not Effective
Security Training	41	Security Training Roles and Responsibilities	Defined	Managed and Measurable	Effective
	42	Assessment of Cybersecurity Workforce	Defined	Defined	Not Effective
	43	Security Training Strategy	Defined	Optimized	Effective
	44	Security Awareness Training	Optimized	Optimized	Effective

	Domain #	Metric Title	2020 Assessed Rating	2021 Assessed Rating	2021 Effective/Not Effective	
	45	Specialized Security Training	Ad-Hoc	Optimized	Effective	
	Overall 46	Assessed Conclusion	Defined	Optimized	Effective	
Detect	ISCM	47	ISCM Policies and Strategy	Consistently Implemented	Consistently Implemented	Not Effective
		48	ISCM Roles and Responsibilities	Defined	Defined	Not Effective
		49	Ongoing Assessments	Consistently Implemented	Consistently Implemented	Not Effective
		50	ISCM Performance Measures	Managed and Measurable	Managed and Measurable	Effective
	Overall 51	Assessed Conclusion	Consistently Implemented	Consistently Implemented	Not Effective	
Respond	Incident Response	52	Incident Response Plan, Policies, and Procedures	Defined	Defined	Not Effective
		53	Incident Response Roles and Responsibilities	Consistently Implemented	Consistently Implemented	Not Effective
		54	Incident Detection and Analysis	Managed and Measurable	Managed and Measurable	Effective
		55	Incident Response Handling Processes	Optimized	Optimized	Effective
		56	Sharing Incident Response Information	Consistently Implemented	Managed and Measurable	Effective
		57	Collaboration with DHS and Other Parties	Managed and Measurable	Managed and Measurable	Effective
		58	Incident Response Technologies Used	Managed and Measurable	Managed and Measurable	Effective
Overall 59	Assessed Conclusion	Managed and Measurable	Managed and Measurable	Effective		
Recover	Contingency Planning	60	Contingency Planning Roles and Responsibilities	Consistently Implemented	Optimized	Effective
		61	Business Impact Analysis	Consistently Implemented	Managed and Measurable	Effective
		62	Maintain Information Systems Contingency Plans	Managed and Measurable	Optimized	Effective
		63	System Contingency Planning Testing/Exercises	Consistently Implemented	Consistently Implemented	Not Effective
		64	Information System Backup and Storage	Consistently Implemented	Consistently Implemented	Not Effective
		65	Planning and Performance of Recovery Activities	Managed and Measurable	Managed and Measurable	Effective
Overall 66	Assessed Conclusion	Managed and Measurable	Managed and Measurable	Effective		

Source: Kearney-generated based on FY 2020 and FY 2021 SEC CyberScope results

APPENDIX IV: MANAGEMENT COMMENTSUNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549**MEMORANDUM**

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

From: David Bottom, Chief Information Officer *David Bottom*

Date: December 10, 2021

Subject: Management Response to Draft OIG Report, *Fiscal Year 2021 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) 2021. The report evaluates the SEC's information security program in accordance with the FY 2021 Inspector General FISMA Reporting Metrics,¹ which are designed to assess the maturity levels of controls across the five functional areas of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF).²

I am pleased your report found the SEC's information security program has improved since FY 2020. Although the metrics upon which the assessment was based were only finalized in May 2021, the SEC is very pleased that our efforts over the past year were recognized, both in the overall scoring of the Security Training domain as Optimized (Level 5) and in maturity improvements noted in 15 specific metric areas.

We remain committed to bolstering information security, including with respect to your report's eight recommendations, with which we concur. More details on management's responses to these recommendations, as well as the Other Matters of Interest cited in your report, are found in Appendix A.

Thank you once again for the professionalism and courtesies that OIG and its contractor, Kearney and Company (Kearney), demonstrated throughout this audit. We intend to pursue corrective

¹ U.S. Department of Homeland Security, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021.

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

actions as described in Appendix A as a key priority, and look forward to working with your office to confirm that our planned actions fully address the issues identified in your report.

cc: Kenneth Johnson, Chief Operating Officer
Caryn Kauffman, Acting Chief Risk Officer

Appendix A: Management's Responses to OIG's Recommendations

The following are management's responses to each of the recommendations provided in the OIG report.

Recommendation 1: Develop, document, and implement a process for consistently implementing [REDACTED] within the agency's [REDACTED]

Response: We concur. Our work in further enhancing the agency's [REDACTED] continues, including in response to OIG's prior recommendations in Report 562. As part of this ongoing work, OIT is in the process of incorporating reviews of [REDACTED] into the Service Delivery Framework (SDF) lifecycle processes. As part of the remediation activity associated with CAP 562-06, SDF phases will include processes to add approved [REDACTED] to the [REDACTED] and [REDACTED] in the SEC's [REDACTED]. This effort will be documented in OIT operating procedures.

Recommendation 2: Develop, document, and implement a process to clearly define requirements for consistently completing and maintaining Federal Information Processing Standards Publication 199 categorization worksheets for all system types.

Response: We concur. OIT will further develop, document, and implement requirements for consistently completing and maintaining Federal Information Processing Standards Publication (FIPS) 199 categorization worksheets for all system types. In particular, the requirements will indicate when an SEC-specific FIPS 199 categorization form is required, and when it is acceptable to accept and maintain a FIPS 199 categorization from an appropriate Federal government agency or partner organization.

Recommendation 3: Develop, document, and implement a formal process to consistently capture and share lessons learned on the effectiveness of its cybersecurity Risk Management program and make updates, as necessary.

Response: We concur. OIT will develop, document, and implement such a process with respect to its cybersecurity Risk Management program and make updates, as necessary.

Recommendation 4: Develop, document, and implement a formal process to consistently capture and share lessons learned on the effectiveness of its configuration baseline program and make updates, as necessary.

Response: We concur. OIT will develop, document, and implement such a process regarding the agency's configuration baseline program and make updates, as necessary.

Recommendation 5: Develop, document, and implement a formal process that clearly defines [REDACTED] requirements for all configuration change types at the SEC or configuration changes [REDACTED]

Response: We concur. OIT will review the existing change management documentation and update, as necessary, the process and definitions for configuration change types and associated [REDACTED] to ensure the [REDACTED]

Recommendation 6: Develop and document a process for maintaining a complete inventory of the collection and use of Personally Identifiable Information that includes a listing of all programs and information systems.

Response: We concur. OIT will review, update, and document, as necessary, the Privacy and Information Assurance team's process for maintaining a complete inventory of the collection and use of Personally Identifiable Information (PII) that includes a listing of all programs and information systems.

Recommendation 7: Develop, document, and implement a formal process to consistently capture and share lessons learned to improve the effectiveness of its Information Security Continuous Monitoring policies and strategy and make updates, as necessary.

Response: We concur. OIT will develop, document, and implement such a process for its Information Security Continuous Monitoring policies and strategy and make updates, as necessary.

Recommendation 8: Develop, document, and implement a process to consistently utilize automated testing for information system contingency plan efforts, [REDACTED]

Response: We concur. OIT will evaluate the ability to utilize automated testing as part of contingency planning efforts to include conferring with other agencies and performing market research of potential vendor solutions. As applicable, OIT will use the results of its evaluation to update its Enterprise Disaster Recovery Plan.

Other Matters of Interest

With regards to the Other Matters of Interest identified in the OIG report, the SEC appreciates the information and input provided in this section. We are committed to continued improvements in these areas, and believe that the efforts underway will further support higher maturity ratings in future audits.

Develop Supply Chain Risk Strategy, Policies, and Procedures: Kearney encourages the SEC to develop and document SCRM policies and procedures that include processes for responding to and monitoring supply chain risk; a process for ensuring systems, system components, and services are consistent with SEC supply chain requirements; and a process for [REDACTED]. Additionally, Kearney encourages the SEC to develop a SCRM strategy that guides the SEC in maintaining an acceptable level of risk for supply chain activities.

Response: We concur. As noted in the OIG's report, the SEC initiated the process for defining an SCRM strategy in FY21. In response to OIG Report 563, CAP 563-07, the SEC approved its Information Communications Technology (ICT) Supply Chain and Vendor Risk Management (SCVRM) Strategy on September 12, 2021. The ICT SCVRM Strategy provides a strategic roadmap for implementing effective ICT SCVRM capabilities, practices, processes, and tools within the SEC. Execution of the strategy is governed by the SEC's ICT SCVRM Executive Committee, a formally chartered body responsible for setting overall objectives and strategy for ICT SCVRM activities. The ICT SCVRM Executive Committee Charter, which was approved on April 8, 2021, identifies roles and responsibilities, outlines the structure of the ICT SCVRM Executive Committee, and describes other requirements. OIT will submit a closure request that demonstrates remediation activities related to CAP 563-07 and will continue its work to develop and implement SCRM processes and procedures in accordance with the ICT SCVRM Strategy.

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.

TO REPORT

fraud, waste, and abuse

Involving SEC programs, operations, employees,
or contractors

FILE A COMPLAINT ONLINE AT

www.sec.gov/oig

CALL THE 24/7 TOLL-FREE OIG HOTLINE

833-SEC-OIG1

CONTACT US BY MAIL AT

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

