U.S. SECURITIES AND EXCHANGE COMMISSION

REPORT NO. 580

December 20, 2023

OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

Fiscal Year 2023 Independent Evaluation of the U.S. Securities and Exchange Commission's Implementation of the Federal Information Security Modernization Act of 2014

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

REDACTED FOR PUBLIC RELEASE

OFFICE OF
INSPECTOR GENERAL

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

MEMORANDUM

December 20, 2023

TO: Kenneth Johnson, Chief Operating Officer

FROM: Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects, Office of Inspector General

SUBJECT: *Fiscal Year 2023 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014*, Report No. 580

Attached is the Independent Auditor's Report on the Fiscal Year (FY) 2023 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 Cotton & Company Assurance and Advisory, LLC (referred to as "Cotton") to conduct this independent evaluation. Cotton conducted the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.* The SEC's Office of Inspector General (OIG) monitored Cotton's work to ensure it met professional standards and contractual requirements.

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

Cotton reported that the SEC made progress in improving its information security program by developing (1) supply chain risk management policies and procedures, (2) an identity and access management strategic plan, (3) its FY 2023-2025 learning and development strategic plan, and (4) operating procedures for lessons learned. The SEC has also implemented the continuous diagnostic and mitigation dashboard as a service project. However, the agency faced challenges, to include, but not limited to, developing plans of action and milestones, updating and maintaining its vulnerability disclosure policy, and fully meeting logging requirements.

As described in the attached report, Cotton identified opportunities for improvement in key areas and made six new recommendations to strengthen these areas of the SEC's information security program. As a result, Cotton noted that the agency's information security program did not meet the *FY 2023-2024 Inspector General FISMA Reporting Metrics*' definition of "effective."

On November 20, 2023, we provided management with a draft of Cotton's report for review and comment. In its December 13, 2023, response, management concurred with Cotton's recommendations. Cotton included management's response as Appendix E 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. Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, a timeframe for completing the required actions, and a description of the actions management plans to take to address each recommendation.

We appreciate management's courtesies and cooperation during the evaluation. If you have questions, please contact me or Kelli Brown-Barnes, Audit Manager.

Attachment

cc: Gary Gensler, Chair
Amanda Fischer, Chief of Staff, Office of Chair Gensler
Heather Slavkin Corzo, Policy Director, Office of Chair 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
Ajay Sutaria, 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
Caroline A. Crenshaw, Commissioner
Malgorzata Spangenberg, Counsel, Office of Commissioner Crenshaw
Mark T. Uyeda, Commissioner
Holly Hunter-Ceci, Counsel, Office of Commissioner Uyeda
Jaime Lizárraga, Commissioner
Laura D'Allaird, Counsel, Office of Commissioner Lizárraga
Parisa Haghshenas, Counsel, Office of Commissioner Lizárraga
Megan Barbero, General Counsel
Elizabeth McFadden, Deputy General Counsel General Litigation/Managing Executive, Office of the General Counsel
Lisa Helvin, Principal Deputy General Counsel for Adjudication and Oversight, Office of the General Counsel
David Leviss, Associate General Counsel for Oversight and Investigations, Office of the General Counsel
Stephen Jung, Assistant General Counsel for Intergovernmental and Congressional Affairs, Office of the General Counsel
Shelly Luisi, Chief Risk Officer
Jim Lloyd, Audit Coordinator/Assistant Chief Risk Officer, Office of the Chief Risk Officer
David Bottom, Director/Chief Information Officer, Office of Information Technology
James Scobey, Associate Director/Chief Information Security Officer, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology
Deborah J. Jeffery, Inspector General

U.S. SECURITIES AND EXCHANGE COMMISSION

OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

Fiscal Year 2023 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014 Evaluation Report

Cotton

A SIKICH. COMPANY

Point of Contact:
Harrison Lee, Partner
333 John Carlyle Street, Suite 500
Alexandria, Virginia 22314
703.836.6701
harrison.lee@sikich.com

REDACTED FOR PUBLIC RELEASE

Abbreviations

BOD	Binding Operational Directive
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
EL	Event Logging
FISMA	The Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	U.S. Government Accountability Office
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SEC or agency	U.S. Securities and Exchange Commission
SP	Special Publication
VDP	Vulnerability Disclosure Policy

Contents

EXECUTIVE SUMMARY **1**
INTRODUCTION 1
Key Changes to the IG FISMA Metrics 1
Summary Evaluation Results 2
Management's Response and Evaluator's Comments 4
FISMA Evaluation Findings **5**
Security Function: Identify 5
1. The SEC did not consistently use POA&Ms to effectively mitigate security weaknesses. 5
Security Function: Protect 6
2. The SEC did not update and maintain its VDP in accordance with DHS BOD 20-01 6
3. The SEC did not [redacted] 8
Security Function: Detect 9
4. The SEC did not design, implement, and assess the new baseline controls for agency systems in accordance with NIST SP 800-53, Rev. 5. 9
Security Function: Respond 11
5. The SEC has not fully met logging requirements at the EL2 (intermediate) maturity level in accordance with OMB Memorandum M-21-31 11
Appendix A – Background **13**
Appendix B – Objective, Scope, and Methodology **16**
Appendix C – Prior-Year Recommendations **21**
Appendix D – Other Matters for Consideration **23**
Appendix E – Management Comments **24**

EXECUTIVE SUMMARY

INTRODUCTION

To protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation, the U.S. Securities and Exchange Commission (SEC or agency) relies on more than 100 information systems, many of which contain sensitive data. Under the Federal Information Security Modernization Act of 2014 (FISMA),[1] the SEC must undergo an annual independent evaluation of its information security program and practices, to be performed by the SEC's Office of Inspector General (OIG). The OIG contracted with the independent certified public accounting firm Cotton & Company Assurance and Advisory, LLC (Cotton), to conduct the SEC's FISMA evaluation for Fiscal Year (FY) 2023. This report presents the results of Cotton's independent evaluation of the effectiveness of the SEC's information security program and practices.

See **Appendix B** for detailed information regarding the objective, scope, and methodology for this evaluation.

KEY CHANGES TO THE IG FISMA METRICS

In FY 2022, the Office of Management and Budget (OMB) selected a group of 20 core information technology security metrics, based on administration priorities, high-impact security processes, and essential functions, by which to assess the effectiveness of agencies' security programs. Beginning in FY 2023, in addition to these core metrics, agencies must also evaluate the remainder of the standards and controls (referred to as "supplemental controls") on a 2-year cycle developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Security Agency (CISA). Therefore, in addition to the 20 core metrics from FY 2022, each agency is also required to evaluate an additional 20 supplemental metrics to conclude on the agency's overall cybersecurity posture in FY 2023. In rating each component of information security, the evaluator averages the results of the core metrics and the supplemental metrics for each of five Security Function areas—Identify, Protect, Detect, Respond, and Recover—which are further divided into nine domains.

IGs assess each domain and its Security Function on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. The five maturity model levels are Level 1: *Ad Hoc*, Level 2: *Defined*, Level 3: *Consistently Implemented*, Level 4: *Managed and Measurable*, and Level 5: *Optimized*. To be considered effective, an agency's information security program must achieve an overall rating of Level 4: *Managed and Measurable* or above.

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (December 18, 2014)

SUMMARY EVALUATION RESULTS

We assessed the overall maturity level of the SEC's information security program at Level 3: *Consistently Implemented* (as described in **Table 1** below). We therefore determined that the SEC's information security program and practices were **not effective**.

Table 1. SEC's Assessed Maturity Level for FY 2023[2]

Security Function	FY 2023 Assessed Maturity Level
Identify	Level 3: *Consistently Implemented*
Protect	Level 2: *Defined*
Detect	Level 2: *Defined*
Respond	Level 4: *Managed and Measurable*
Recover	Level 2: *Defined*
Overall Maturity	**Level 3: *Consistently Implemented***

Source: Cotton-generated based on the results of our testing.

Since FY 2022, the SEC has made improvements in its information security program and practices, including:

- Developing Supply Chain Risk Management policies and procedures.
- Developing an Identity and Access Management strategic plan and implementation plan that align with industry best practices and OMB Memorandum M-22-09, *Moving the U.S. Government toward Zero Trust Cybersecurity Principles*.
- Developing the FY 2023 – FY 2025 Learning and Development Strategic Plan.
- Developing operating procedures for lessons learned to standardize the lessons learned process and improve agency policies and procedures.
- Completing its implementation of the Continuous Diagnostic and Mitigation Dashboard as a Service project, in coordination with the Department of Homeland Security (DHS)/CISA, to better support existing ongoing control activities.

Although the SEC has shown progress in the above areas, it needs additional improvement in the following areas:

- Developing Plans of Action and Milestones (POA&Ms) to effectively mitigate security weaknesses.

[2] Although prior years' FISMA reports have presented the results for multiple years on a comparative basis, the introduction of supplemental metrics renders this year's scores not comparable with those of prior years at the function and domain levels. In addition, this year, domain scores are calculated based on the average of the domain's metrics. In prior years, the domain score was based on the mode. For this reason, we are not providing a table that shows the changes in maturity level over multiple years.

- Updating and maintaining its vulnerability disclosure policy (VDP) in accordance with DHS Binding Operational Directive (BOD) 20-01.
- [redacted]
- Designing and implementing new baseline controls for SEC systems based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5.
- Fully meeting the logging requirements at the Event Log (EL) 2 (intermediate) maturity level in accordance with the requirements of OMB Memorandum M-21-31.

These control weaknesses directly affected the maturity levels of the individual components of the SEC's information security program, as follows:

- The **Identify** function assists agencies in developing an organizational understanding to manage cybersecurity risks to their systems, assets, data, and capabilities. We determined that the maturity level of the SEC's Identify function was Level 3: *Consistently Implemented* because the SEC did not consistently use POA&Ms to effectively mitigate security weaknesses.
- The **Protect** function assists agencies in developing and implementing appropriate safeguards to ensure delivery of critical services, including limiting or containing the impact of a potential cybersecurity event. We determined that the maturity level of the SEC's Protect function was Level 2: *Defined* because the SEC:
    - Did not update and maintain its VDP to include all necessary public-facing applications in accordance with DHS BOD 20-01.
    - Did not [redacted]
- The **Detect** function assists agencies in developing and implementing appropriate activities to identify the occurrence of a cybersecurity event, including enabling timely discovery of a cybersecurity event. We determined that the maturity level of the SEC's Detect function was Level 2: *Defined*. The SEC has developed system security plans for its systems; however, it has not designed and implemented new baseline controls for these systems in accordance with NIST SP 800-53, Rev. 5. Specifically, the SEC did not design, implement, and assess all new baseline controls for the systems in accordance with NIST SP 800-53, Rev. 5.
- The **Respond** function assists agencies in developing and implementing appropriate activities to take action regarding a detected cybersecurity incident, including how to contain the impact of a potential cybersecurity incident. We determined that the maturity level of the SEC's Respond function was Level 4: *Managed and Measurable* and was therefore effective.
- The **Recover** function assists agencies in developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that have been impaired due to a cybersecurity incident. The Recover function supports a timely return to normal operations to reduce the impact of a cybersecurity incident. We determined that the maturity level of the SEC's Recover function was Level 2: *Defined* because the SEC did not address all of the

prior-year recommendations during our fieldwork phase, as shown in **Appendix C**. We did not issue any new recommendations for this function in FY 2023.

Management's Response and Evaluator's Comments

The SEC concurred with all of the recommendations included in the report and stated that it is pleased the report identified improvements to the SEC's information security program across several domains, including Risk Management, Supply Chain Risk Management, Security Training, and Implementation of Continuous Diagnostics and Monitoring Program. The SEC noted that the Office of Information Technology (OIT) will continue to focus on improving maturity throughout the SEC's information security program, even though not all metrics are evaluated and scored every year. The SEC also noted that OIT's progress toward a strong information security program can be further seen through its successful remediation of 14 prior-year FISMA evaluation recommendations in FY 2023. The SEC stated that it will continue to focus on improving its security posture and maturing program areas based on the FISMA metrics.

A summary of the SEC's comments and our evaluation of those comments are included in the FISMA Evaluation Findings section of the report. We have also reprinted the SEC's comments in **Appendix E**. Cotton will evaluate corrective actions addressing current and prior-year recommendations in future FISMA evaluations.

The attached report provides a detailed discussion of the findings, grouped by NIST Cybersecurity Framework security function. **Appendix A** provides background information on the SEC and FISMA. **Appendix B** details the objective, scope, and methodology for this evaluation. **Appendix C** contains information regarding the status of recommendations made in prior-year FISMA evaluation reports, while **Appendix D** contains information regarding observations that did not warrant a recommendation in FY 2023.

Harrison Lee, CISA, CISM, CISSP, PMP
Partner, Cotton
December 20, 2023

FISMA Evaluation Findings

This report describes the five FISMA functions and our findings and recommendations for each function based on the results of our evaluation. We organized our conclusions and ratings by function and domain to help orient the reader to deficiencies as categorized by the NIST Cybersecurity Framework.

SECURITY FUNCTION: IDENTIFY

The objective of the Identify function is to develop an organizational understanding to manage cybersecurity risks to agency systems, assets, data, and capabilities.

1. The SEC did not consistently use POA&Ms to effectively mitigate security weaknesses.

IG FISMA Function: Identify / Domain: Risk Management

Plans of Action and Milestones (POA&M) assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. Specifically, POA&Ms identify tasks that the agency must perform and detail the resources required to accomplish each element of the task, any milestones identified, and the scheduled completion dates for each milestone. If additional information regarding security weaknesses is identified during any other review performed by, for, or on behalf of the agency—including U.S. Government Accountability Office (GAO) audits, financial system audits, and critical infrastructure vulnerability assessments—the agency should either update its POA&Ms to consolidate the recommendations or ensure that the POA&Ms are accompanied by other agency plans to ensure that the agency fully addresses all of the recommendations for correcting the security weaknesses.[3]

The *FY 2023-2024 IG FISMA Reporting Metrics* measure the extent to which agencies consistently use POA&Ms to effectively mitigate security weaknesses. NIST SP 800-53, Rev. 5 states that agencies must "Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system."[4]

The SEC did not consistently use POA&Ms to effectively mitigate security weaknesses. Cotton noted that the SEC's Office of Information Technology (OIT) [redacted]. However, our analysis of the [redacted] report showed that the SEC did not prepare POA&Ms [redacted]

[3] See https://georgewbush-whitehouse.archives.gov/omb/memoranda/m02-01.html (last accessed on September 8, 2023) for more detail.

[4] Control CA-5(a).

This condition occurred because the SEC did not consistently use [redacted]

Without effectively [redacted], the SEC may not be able to [redacted] the IT security risks that may potentially impact its business operations.

Recommendation

To improve the SEC's Risk Management program, Cotton recommends that the Office of Information Technology:

1. Define and implement [redacted] Plans of Action and Milestones.

   Management's Response: Management concurred with this recommendation and noted that OIT maintains various policies and procedures documents that describe how the vulnerability management program discovers, prioritizes, and coordinates remediation of weaknesses discovered within SEC information systems. Management stated that OIT will evaluate its policy and associated procedures to consider further enhancements. We have included management's complete response in **Appendix E**.

   Cotton's Evaluation of Management's Response: Management's proposed actions are responsive. The recommendation will be closed upon completion and verification of the proposed actions.

SECURITY FUNCTION: PROTECT

The objective of the Protect function is to develop and implement appropriate safeguards to ensure delivery of critical services, including limiting or containing the impact of a potential cybersecurity event.

2. The SEC did not update and maintain its VDP in accordance with DHS[5] BOD 20-01.

IG FISMA Function: Protect / Domain: Configuration Management

Cybersecurity is a public good that is strongest when the public is given the ability to contribute. A key component to obtaining these public contributions is to establish a formal policy that describes the activities that individuals can undertake to find and report vulnerabilities in a legally authorized manner. Such policies enable federal agencies to remediate vulnerabilities before an adversary can exploit them, thereby benefiting the public immensely.

[5] DHS has the authority to coordinate government-wide cybersecurity efforts and issue binding operational directives detailing actions that federal agencies must take to improve their cybersecurity posture. Further, DHS provides operational and technical assistance to agencies and facilitates information-sharing across the federal government and the private sector.

A Vulnerability Disclosure Policy (VDP) is an essential element of an effective enterprise vulnerability management program and is critical to the security of internet-accessible federal information systems. VDPs enhance the resilience of the government's online services by encouraging meaningful collaboration between federal agencies and the public. VDPs also instruct the public where to send a report, what types of testing are authorized for which systems, and what communication to expect. When agencies integrate vulnerability reporting into their existing cybersecurity risk management activities, they can weigh and address a wider array of concerns. This helps safeguard the information the public has entrusted to the government and gives federal cybersecurity teams more data to protect their agencies. Additionally, ensuring consistent policies across the executive branch offers those who report vulnerabilities equivalent protection and a more uniform experience.

The *FY 2023-2024 IG FISMA Reporting Metrics* measure the extent to which agencies include all internet-accessible systems in the scope of their VDP. Additionally, DHS BOD 20-01, dated September 20, 2020, states: "At 2 years after the issuance of this directive, all internet-accessible systems or services must be in scope of the policy."

The SEC has developed and implemented a VDP, but the VDP does not include all internet-accessible systems and services, encompassing systems directly managed by the SEC, systems operated on the SEC's behalf, and mobile applications.[6] Specifically, Tips Complaints and Referrals Intake and Resolution 3.0, SRO Rule Tracking System/Electronic Form Filing System, External Application User Authentication, and Electronic Filing for Administrative Proceedings are operational, organization-operated, externally facing, internet-accessible systems; however, the SEC did not list these systems within its VDP at the time of our evaluation. This condition occurred because the SEC was in the process of updating its VDP.

Without a comprehensive vulnerability disclosure program in place, the SEC may fail to receive information regarding its high-risk and exploitable vulnerabilities, which may weaken the security of an SEC system, its data, or its users with regard to confidentiality, integrity, or availability.

Recommendations

To improve the SEC's Configuration Management program, Cotton recommends that the Office of Information Technology:

2. Update the Vulnerability Disclosure Policy (VDP) to include all internet-accessible systems. Once OIT has updated the VDP, the SEC should immediately report to the Cybersecurity and Infrastructure Security Agency (CISA) regarding:

    a. Any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on SEC systems that use commercial software or services that affect or are likely to affect other parties in government or industry.

    b. Vulnerability disclosure, coordination, or remediation activities that the SEC believes CISA can assist with or should be aware of, particularly as they relate to outside organizations.

[6] https://www.sec.gov/vulnerability-disclosure-policy (dated October 21, 2021), last accessed on November 3, 2023.

c. Any other situation in which the SEC deems it helpful or necessary to involve CISA.

Management's Response: Management concurred with this recommendation and stated that OIT will update and publish the VDP in accordance with DHS BOD 20-01. Although DHS BOD 20-01 does not define a threshold for "immediate" reporting, the SEC will define the time period as part of the associated VDP procedures (see Recommendation 3). We have included management's complete response in **Appendix E**.

Cotton's Evaluation of Management's Response: Management's proposed actions are responsive. The recommendation will be closed upon completion and verification of the proposed actions.

3. Develop and implement vulnerability disclosure-handling procedures that describe the SEC's process for implementing its VDP, in accordance with Department of Homeland Security Binding Operational Directive 20-01.

Management's Response: Management concurred with the recommendation and stated that OIT Security will review the vulnerability disclosure-handling procedures and make any updates necessary to support **Recommendation 2** and ensure compliance with DHS BOD 20-01. We have included management's complete response in **Appendix E**.

Cotton's Evaluation of Management's Response: Management's proposed actions are responsive. The recommendation will be closed upon completion and verification of the proposed actions.

3. The SEC did not [redacted]

IG FISMA Function: Protect / Domain: Identity, Credential, and Access Management

Organizations define privileged roles to allow individuals to perform security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme enables agencies to tailor levels of access according to the needs of a person's job responsibilities.

[redacted]

The SEC has defined and implemented an access provisioning process at the agency level. However, the SEC did not [redacted]. Specifically, the SEC:

[redacted]

- Did not [redacted]
- Did not [redacted]

This condition occurred because the SEC did not [redacted]

Without [redacted] in place, the SEC may [redacted]

Recommendation

To improve the SEC's Identity, Credential, and Access Management program, Cotton recommends that the Office of Information Technology:

4. [redacted]

   Management's Response: Management concurred with the recommendation and noted that the SEC had documented control requirements for account provisioning in its Information Security and Privacy Controls Manual. Management stated that the [redacted]. We have included management's complete response in **Appendix E**.

   Cotton's Evaluation of Management's Response: Management's proposed actions are responsive. The recommendation will be closed upon completion and verification of the proposed actions.

SECURITY FUNCTION: DETECT

The objective of the Detect function is to develop and implement appropriate activities to ensure timely discovery of a cybersecurity event.

4. The SEC did not design, implement, and assess the new baseline controls for agency systems in accordance with NIST SP 800-53, Rev. 5.

IG FISMA Function: Detect / Domain: Information Security Continuous Monitoring

To ensure that an organization maintains a cost-effective, risk-based approach to achieving adequate security organization-wide, the organization must select and implement the appropriate security controls

and assurance requirements as described in NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*. The selected set of security controls must include detection controls that align with the level of harm that a security breach of the particular system would have on the organization. NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* (October 2020), prescribes the minimum controls and assurance requirements, depending on whether the organization determines the information systems to be low-, moderate-, or high-impact systems.

Organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST SP 800-53B.

The *FY 2023-2024 IG FISMA Reporting Metrics* measure the extent to which agencies consistently develop and maintain system security plans and monitor system security controls at the appropriate risk/impact baselines prescribed by NIST. OMB Circular A-130 states that agencies are expected to meet the requirements of—and be in compliance with—NIST standards and guidelines within one year of their respective publication dates, unless otherwise directed by OMB.

The SEC did not design, implement, and assess all of the new baseline controls for all of the systems that were in scope for FY 2023. This condition occurred as a result of OIT's competing priorities in responding to various Directives, including those issued by OMB, DHS/CISA, and the Office of the President with agency requirements. In FY 2023, the SEC took steps to update the SEC Information Security and Privacy Controls Manual, as well as templates for system security and privacy plans, to adapt new and revised security and privacy controls from NIST SP 800-53, Rev 5. The SEC planned to assess the new control objectives and requirements for SEC systems after September 30, 2023.

Without designing, implementing, and assessing all required baseline controls for its systems, the SEC may not be able to identify and remediate system-level risks commensurate with their respective impacts on the SEC's mission.

Recommendation

To improve the SEC's Information Security Continuous Monitoring program, Cotton recommends that the Office of Information Technology:

5. Update the SEC's system security plans with the latest baseline controls for all FISMA-reportable systems to ensure the SEC is assessing and monitoring the controls in accordance with the level of risk associated with each information security system.

   Management's Response: Management concurred with the recommendation and stated that OIT will define a phased approach for updating its system security plans to align with the SEC's Information Security and Privacy Controls Manual, which OIT updated in FY 2023 to meet the requirements of NIST SP 800-53, Rev. 5. The SEC's Information System Owners will update the system security plans based on this multi-year phased approach. We have included management's complete response in **Appendix E**.

Cotton's Evaluation of Management's Response: Management's proposed actions are responsive. The recommendation will be closed upon completion and verification of the proposed actions.

SECURITY FUNCTION: RESPOND

The objective of the Respond function is to develop and implement appropriate activities to address a detected cybersecurity incident, including containing the impact of a potential cybersecurity incident.

5. The SEC has not fully met logging requirements at the EL2 (intermediate) maturity level in accordance with OMB Memorandum M-21-31.

IG FISMA Function: Response / Domain: Incident Response

Security events affecting government underscore the importance of increased visibility before, during, and after a cybersecurity incident. Information from logs on federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud service providers) is invaluable in the detection, investigation, and remediation of cyber threats.

On August 27, 2021, OMB published a four-tier maturity model for centralized access and visibility for the highest-level enterprise security operations centers. We have summarized these tiers in **Table 2** below.

Table 2. Summary of Event Logging (EL) Tiers

EL Tier	Rating	Description
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met
EL1	Basic	Only logging requirements of highest criticality are met
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met
EL3	Advanced	Logging requirements at all criticality levels are met

Source: Cotton-generated based on OMB M-21-31.

OMB required agencies to achieve an intermediate level of maturity (EL2) by February 27, 2023; i.e., within 18 months after issuance of OMB Memorandum M-21-31, dated August 27, 2021. The *FY 2023-2024 IG FISMA Reporting Metrics* measure the extent to which agencies are meeting logging requirements at the EL2 maturity level.

The SEC did not fully meet EL2 logging requirements by February 2023. This condition occurred because [redacted]

Without enhanced logging and monitoring capabilities in place, the SEC may lack sufficient visibility into security incidents posing intermediate risks that may impact its information security and business operations.

Recommendation

To improve the SEC's Incident Response program, Cotton recommends that the Office of Information Technology:

6. Develop and implement a log management process to:

   a. [redacted]

   b. [redacted]

   Management's Response: Management concurred with the recommendation and stated that under the SEC's Information Security and Privacy Controls Manual, Information System Owners and Business Owners are responsible for identifying the types of events that systems are able to log, as well as for coordinating with OIT Security regarding acceptable log formats. To address Part A of this recommendation, management stated that [redacted] To address Part B of this recommendation, management stated that [redacted] We have included management's complete response in **Appendix E**.

   Cotton's Evaluation of Management's Response: Management's proposed actions are responsive. The recommendation will be closed upon completion and verification of the proposed actions.

Appendix A – Background

During the peak of the Great Depression, Congress passed the Securities Act of 1933 (Securities Act)[8] and the Securities Exchange Act of 1934 (Securities Exchange Act),[9] which established the SEC. These laws were designed to regulate the financial markets and restore investor confidence in U.S. capital markets by providing investors and the markets with reliable information and clear rules to ensure honest dealings. The main purpose of these laws was to ensure the following:

- Companies that publicly offer securities for investment dollars are forthcoming and transparent about their businesses, the securities they are selling, and the risks involved with investing.
- People who sell and trade securities—brokers, dealers, and exchanges—treat investors fairly and honestly.

The SEC is responsible for overseeing the nation's securities markets and certain primary participants, including broker-dealers, investment companies, investment advisors, clearing agencies, transfer agents, credit rating agencies, and securities exchanges, as well as organizations such as the Financial Industry Regulatory Authority, the Municipal Securities Rulemaking Board, and the Public Company Accounting Oversight Board. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act),[10] the SEC's jurisdiction was expanded to include certain participants in the derivatives markets, private fund advisors, and municipal advisors.

Each year, the SEC brings hundreds of civil enforcement actions against individuals and companies for violation of securities laws. Examples of infractions include insider trading, accounting fraud, market manipulation, and providing false or misleading information about securities and/or the issuing companies.

The SEC has more than 100 FISMA-reportable systems in place to support its mission. These systems are rated as moderate- or low-impact, and about one-third of them are operated by contractors.

The Chief Information Officer directs OIT operations and assists OIT in achieving its strategic goals, which are aligned with the SEC's strategic goals and outcomes. OIT executes its mission and achieves its strategic goals through the Business Management, Operations, Solutions Delivery, Data Strategy, Operations, and Information Security organizations and their respective branches.

[8] See https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#secact1933 (last accessed on September 8, 2023) for more detail.

[9] See https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#secact1933 (last accessed on September 8, 2023) for more detail.

[10] See https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#df2010 (last accessed on September 8, 2023) for more detail.

FISMA Reporting Metrics

FISMA[11] requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA directs each agency's OIG to perform an annual evaluation of the effectiveness of the agency's information security program and practices and to report the results to the OMB.

OMB,[12] CISA,[13] the CIGIE,[14] agency Chief Information Security Officers, and other stakeholders coordinated to develop a set of metrics for IGs to use in evaluating the effectiveness of agency information security programs and practices. These metrics are referred to as "IG metrics." The IG metrics are aligned with the five function areas in the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover, as shown in **Table 3** below. The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

Table 3. IG FISMA Reporting Metrics Function Areas and Domains

Function	Domain
Identify	Risk Management
	Supply Chain Risk Management
Protect	Configuration Management
	Identity, Credential, and Access Management
	Data Protection and Privacy
	Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: Cotton-generated based on FY 2023-2024 IG FISMA Reporting Metrics.

The *FY 2023-2024 IG FISMA Reporting Metrics* is organized into nine domains that are aligned with the five function areas set forth in the NIST Cybersecurity Framework. The *FY 2023-2024 IG FISMA Reporting Metrics* represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle. In FY 2023, the *FY 2023-2024 IG FISMA Reporting Metrics* includes the 20 core metrics from FY 2022, along with 20 supplemental metrics for each review cycle.

[11] P.L. No. 113-283 (December 2014). FISMA's obligations for federal agencies and for federal IGs, as relevant to this evaluation, are codified chiefly to 44 U.S. Code §§ 3554 and 3555, respectively.

[12] OMB issues information security policies and guidelines for federal information resources pursuant to various statutory authorities.

[13] CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

[14] CIGIE is an independent entity established within the executive branch to address issues regarding integrity, economy, and effectiveness that transcend individual government agencies and aid in the establishment of a professional, well-trained, and highly skilled workforce in the OIG.

The core metrics are a selection of 20 metrics that agencies must assess annually and that represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine the effectiveness of the agency's security program. Supplemental metrics are metrics that agencies must assess at least once every 2 years. Supplemental metrics represent important activities that security programs conduct and that contribute to the overall evaluation and determination of the effectiveness of the agency's security program.

The *FY 2023-2024 IG FISMA Reporting Metrics* require IGs to assess the effectiveness of their agency's information security program and practices using a maturity model. **Table 4** describes the five levels of the maturity model: *Ad Hoc, Defined, Consistently Implemented, Managed and Measurable*, and *Optimized*. An information security program operating at Level 4: *Managed and Measurable* or above is considered to be operating at an effective level of security.

Table 4. Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: *Ad-hoc*	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measurable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2023-2024 IG FISMA Reporting Metrics.

Appendix B – Objective, Scope, and Methodology

Objective

The objective of this evaluation was to assess the effectiveness of the SEC's information security program and practices for FY 2023 in accordance with FISMA. The evaluation included assessing the effectiveness of security controls for a subset of systems. We performed this evaluation under CIGIE's *Quality Standards for Inspection and Evaluation*.

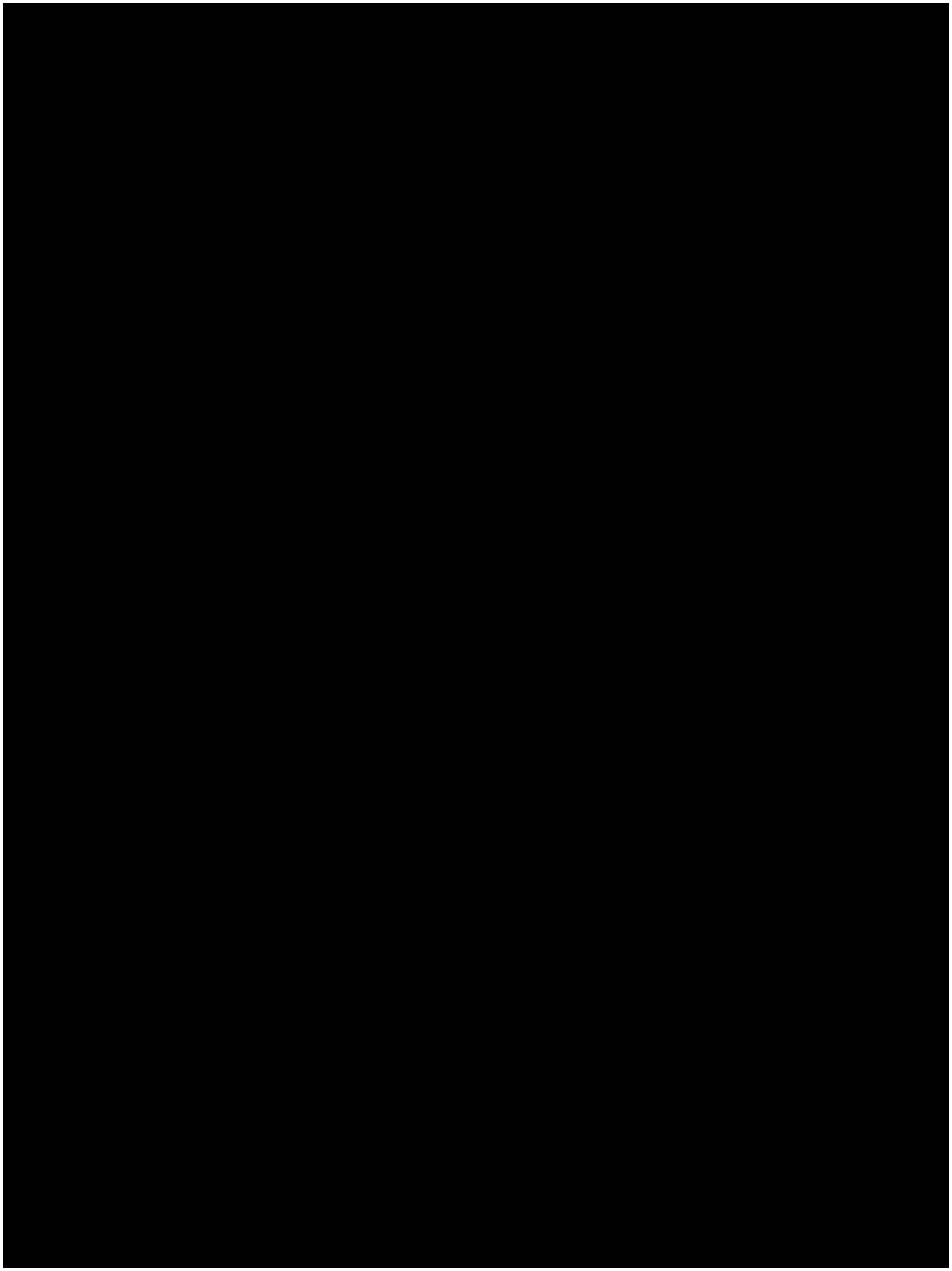
Scope

The evaluation covered the period between October 1, 2022, and May 30, 2023, and included assessing the effectiveness and maturity of the SEC's information security program, focusing on the 20 core metrics and 20 supplemental metrics spread across the 9 domains identified in the *FY 2023-2024 IG FISMA Reporting Metrics*. Cotton judgmentally selected and reviewed a non-statistical sample of 8 of the SEC's 108 FISMA-reportable information systems. This sample represents approximately 8 percent of the SEC's inventory of FISMA-reportable information systems. To select the sample, Cotton used the following criteria:

- Systems that were not tested in the prior 3 years.
- Systems that the SEC categorized as "moderate" or "high" risk under Federal Information Processing Standards Publication 199.
- Systems that contained sensitive and confidential information, including personally identifiable information.
- Systems that the SEC classified as high-value assets.

The sample consisted of the internally and externally hosted systems shown in **Table 5**. To assess system security controls, Cotton reviewed the SEC's security assessment packages, privacy program, and account management for the eight FISMA-reportable systems sampled.

[redacted]



Source: Cotton-generated based on systems extracted from OIT

Methodology

We conducted this evaluation from February 2023 to November 2023 in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objectives.

To accomplish our evaluation objectives, we:

- Interviewed key personnel, including staff from the SEC OIT's Policy and Compliance Branch and Security Engineering Branch.
- Examined documents and records that were 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.

In concluding on the effectiveness of the SEC's information security program, we leveraged guidance and definitions from the *FY 2023-2024 IG FISMA Reporting Metrics*. Relevant evaluation criteria used to draw conclusions included, but were not limited to, the following:

- SEC policies, procedures, and practices
- OMB memoranda and bulletins

- Presidential Executive Order 14028, *Improving the Nation's Cybersecurity*[15]
- NIST SPs
- DHS BODs
- SECURE Technology Act[16]
- Federal Enterprise Architecture Framework, Version 2[17]

Cotton also followed up on all prior-year recommendations that were open at the start of the FY 2023 evaluation that impacted the effectiveness of the SEC's information security program and reviewed remediation packages that the SEC submitted. See **Appendix C** for more detail.

Internal Controls: Consistent with our evaluation objectives, we did not assess OIT's overall management control structure. Instead, Cotton reviewed OIT's FY 2022 Memorandum of Unmodified Statement Assurance. Based on our review, Cotton determined that OIT conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. The assessment included an evaluation of whether the SEC's internal controls were in compliance with the underlying management principles, which incorporate GAO's *Standards for Internal Control in the Federal Government*. Based on the results of the FY 2022 assessment, OIT stated that internal controls over operations, reporting, and compliance were operating effectively through October 5, 2022.

Data Reliability: GAO's *Assessing Data Reliability* (GAO-20-283G), dated December 2019, states that reliability of data means data are applicable for audit purposes 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 a valid measure of the underlying concepts addressed in the audit's research objectives.
- "Completeness" refers to the extent to which relevant data records and fields are present and sufficiently populated.
- "Accuracy" refers to the extent to which recorded data reflect the actual underlying information.

Cotton used the SEC's enterprise governance, risk management, and compliance tool as a data source for obtaining documentation and reports related to the sampled systems and FISMA-reportable information systems inventory. Cotton tested the reliability, completeness, and accuracy of data by

[15] Executive Order 14028 can be found at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity (last accessed on September 11, 2023).

[16] The SECURE Technology Act is publicly available. See https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf (last accessed on September 11, 2023).

[17] The Federal Enterprise Architecture Framework is publicly available. See https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf (last accessed on September 11, 2023).

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 were sufficiently reliable to support our conclusions.

Prior Coverage: As of September 30, 2023, the SEC implemented corrective actions to close 14 prior-year recommendations from the FY 2018 through FY 2022 FISMA evaluations. Although OIT addressed these recommendations, as noted in this report, areas in which improvements are needed still exist. **Appendix C** lists all open OIG recommendations from prior FISMA audits and evaluations.

SEC OIG audit and evaluation reports, including prior-year FISMA reports, can be accessed at: https://www.sec.gov/oig/issued-reports

Appendix C – Prior-Year Recommendations

During FY 2023, the SEC implemented corrective actions to close 14 prior-year recommendations from the FY 2018 through FY 2022 FISMA evaluations. Another six recommendations remain open, as depicted in **Table 6**. In addition, we identified six new recommendations for FY 2023, as discussed in this report.

Table 6. Open Recommendation Status

Domain	Prior Report and Recommendation Number	Recommendation	Status as of FY 2023 Year-end
Risk Management	563-1	Develop and document a) Agency requirements for applying security and operating system updates to mobile devices in an organizationally defined timeframe; b) A software assurance process for mobile applications within the Service Delivery Framework; c) A mobile application vetting process to check for malware prior to permitting use on U.S. Securities and Exchange Commission-issued mobile devices; and d) A flaw remediation process for mobile devices.	Closed as of September 25, 2023*
	570-3	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.	Closed as of June 8, 2023
	574-1	Consistently implement its process for reviewing system interconnections listed in System Security Plans for outdated or inaccurate system interconnections as part of the agency's annual System Security Plan reviews in order to ensure the consistent maintenance of a comprehensive and accurate inventory of system interconnections.	Closed as of September 20, 2023*
	574-2	Develop, document, and implement a process for documenting the results of privacy risk assessments into the agency's cybersecurity risk register.	Closed as of September 25, 2023*
	574-3	Develop and implement a process to [redacted]	Open
	574-4	Develop and define policies and procedures to ensure adherence to its cybersecurity and supply chain risk management requirements for external providers within the agency's Supply Chain Risk Management Strategy.	Closed as of September 25, 2023*
Configuration Management	570-4	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.	Closed as of June 8, 2023
	574-5	Develop and implement a process to deploy [redacted]	Open
	574-6	Implement the defined processes for [redacted]	Open

Domain	Prior Report and Recommendation Number	Recommendation	Status as of FY 2023 Year-end
Identity, Credential, and Access Management	546-12	[redacted]	Open
	574-7	Develop and implement a process, including the timelines, [redacted]	Open
Data Protection and Privacy	574-8	Develop a process for conducting [redacted] in order to manage and measure the effectiveness of the agency's [redacted].	Open
	574-9	Document and integrate Domain Name System monitoring activities within the Information Security Continuous Monitoring strategy to ensure the agency's Domain Name System infrastructure is monitored for potential tampering.	Closed as of August 24, 2023*
	574-10	Develop a process to consistently implement encryption of data at rest for information systems, including those in isolated environments or, as applicable, assess the potential impact of not implementing encryption of data at rest for information systems and document a risk acceptance.	Closed as of August 24, 2023*
Security Training	563-6	Define and implement a process to incorporate results from the assessments of knowledge, skills, and abilities into the security training strategy.	Closed as of July 5, 2023
Information Security Continuous Monitoring	570-7	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.	Closed as of June 8, 2023
	574-11	Complete implementation of the Continuous Diagnostic and Mitigation Dashboard as a Service in coordination with Department of Homeland Security/Cybersecurity and Infrastructure Security Agency to better support existing ongoing control activities.	Closed as of March 29, 2023
Incident Response	574-12	Develop, document, and implement a formal process for consistently capturing and sharing formal lessons learned on the effectiveness of incident handling policies and procedures and make updates, as necessary.	Closed as of March 29, 2023
Contingency Planning	574-13	Develop steps to ensure that Business Impact Analyses for information systems, including information systems that have moved to a cloud service provider, are consistently completed as part of the system authorization process.	Closed as of August 24, 2023*
	570-8	Develop, document, and implement a process to consistently utilize automated testing for information system contingency plan efforts, including any identified exemptions due to system configuration requirements or limitations that would prevent such automated testing to be conducted, as necessary.	Closed as of June 8, 2023

Source: Cotton-generated based on the Open Recommendation Tracker provided by OIG and our evaluation results.

*The SEC submitted the closure package for this recommendation after the conclusion of our fieldwork phase. Cotton assessed the closure package and determined that the recommendation could be closed.

Appendix D – Other Matters for Consideration

During the FY 2023 FISMA evaluation, Cotton noted instances in which management had finalized key policies and procedures during the fieldwork phase of the evaluation but did not have sufficient time to implement the policies and procedures before the end of the fieldwork phase. We were therefore unable to proceed with testing for Maturity Level 3: *Consistently Implemented* for these instances. We did not deem it necessary to issue a recommendation for these instances simply to require management to implement the policy and procedures. Instead, we identified a proposed resolution as an action plan for future year(s) where necessary. In addition, we did not issue a recommendation if management resolved an observation during our evaluation, or if management made a risk-based decision to deviate from a requirement. **Table 7** provides information regarding the observations that impacted the CyberScope metric scores but that did not warrant a recommendation in FY 2023.

Table 7. Observations

Domain	Observations
Supply Chain Risk Management	The SEC finalized and published its Supply Chain Risk Management Acquisition Procedures document on April 20, 2023. As a result, the SEC did not have sufficient time to consistently implement the guidance for its externally provided products, services, and systems.
Configuration Management	The SEC has prepared and planned to meet requirements for the Trusted Internet Connections 3.0 initiative. However, [redacted]
Identity, Credential, and Access Management	The SEC has developed a comprehensive Identity, Credential, and Access Management policy, strategy, process, or technology solution roadmap to guide its processes and activities. However, the SEC had not fully implemented all of the requirements identified in OMB Memorandum M-19-17. Specifically, as of May 31, 2023, the SEC had begun implementing [redacted]
Identity, Credential, and Access Management	The *FY 2023-2024 IG FISMA Reporting Metrics* measure the extent to which agencies consistently implement remote access session timeouts after 30 minutes (or less) of user inactivity. The SEC did not enforce remote session timeouts after 30 minutes of inactivity for digital workspace users. The SEC implemented its defined policy of [redacted] minutes based on guidance from NIST SP 800-53, Rev. 5, which allows agencies to make an organization-defined determination for the time period allowed before a remote session times out due to inactivity. Although the implemented time period of [redacted] minutes did not meet the *FY 2023-2024 IG FISMA Reporting Metrics* criteria of 30 minutes, we determined that the SEC had used appropriate NIST guidance to determine its remote session timeout setting and that the issue therefore did not warrant an audit recommendation.
Security Training	The SEC developed its FY 2023 – FY 2025 Learning and Development Strategic Plan; however, it was unable to finalize the plan before our fieldwork phase concluded. As a result, the SEC had not yet implemented the plan during the FY 2023 FISMA evaluation.
Contingency Planning	The SEC did not conduct a tabletop exercise for one of the nine systems in our sample, in accordance with its Information Technology Contingency Planning Handbook. Once Cotton communicated this observation to the SEC, the SEC completed the tabletop exercise.

Source: Cotton-generated based on observations communicated in our CyberScope Response without recommendations.

Appendix E – Management Comments

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

MEMORANDUM

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

From: David Bottom, Chief Information Officer Bottom, David Digitally signed by Bottom, David Date: 2023.12.13 13:02:57 -05'00'

Date: December 13, 2023

Subject: Management Response to Draft OIG Report, *Fiscal Year 2023 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 (Report) on the Securities and Exchange Commission's (SEC or Agency) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year (FY) 2023. The Report evaluates the SEC's information security program in accordance with the *FY 2023-2024 Inspector General FISMA Reporting Metrics*,[1] which are designed to assess the maturity levels of controls across five functional areas of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[2]

I am pleased your Report identified improvements to SEC's information security program across several domains, such as risk management, supply chain, security training, and continuous diagnostics and monitoring. The SEC's Office of Information Technology (OIT) continues to focus on improving maturity throughout the program, even though not all metrics are evaluated and scored each year. Further demonstrating OIT's progress towards a strong information security program is the successful remediation of prior year findings, recognized by OIG concurring on the closure of 24 prior-year recommendations during FY 2023, 14 of which were FISMA-specific. The Agency will continue to focus on improving the Agency's security posture and maturing program areas based on the FISMA metrics.

We concur with your Report's six recommendations and remain committed to advancing the SEC's information security program. More details on management's responses to these recommendations are found in Appendix A.

Thank you once again for the professionalism and courtesies that OIG and your contractor, Cotton and Company, demonstrated throughout this audit. We intend to pursue corrective actions as described in Appendix A as a key priority and look forward to working with your office to confirm that our planned actions address the issues identified in your report.

cc: Kenneth Johnson, Chief Operating Officer
Shelly Luisi, Chief Risk Officer

[1]U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, February 10, 2023.
[2]U.S. Department of Commerce, NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018.

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: Define and implement [redacted] Plans of Action and Milestones.

Response: We concur. As reflected in OIT 24-04.SAC.04, *Information Technology Vulnerability Management Policy* and OIT 24-04.SAC.28, *OIT Vulnerability Management Operating Procedures* (OP), OIT describes how the vulnerability management program discovers, prioritizes, and coordinates remediation of weaknesses discovered within SEC information systems. OIT will evaluate the policy and associated procedures to consider further enhancements.

Recommendation 2: Update the Vulnerability Disclosure Policy (VDP) to include all internet-accessible systems. Once OIT has updated the VDP, the SEC should immediately report to the Cybersecurity and Infrastructure Security Agency (CISA) regarding:

a. Any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on SEC systems that use commercial software or services that affect or are likely to affect other parties in government or industry.
b. Vulnerability disclosure, coordination, or remediation activities that the SEC believes CISA can assist with or should be aware of, particularly as they relate to outside organizations.
c. Any other situation in which the SEC deems it helpful or necessary to involve CISA.

Response: We concur. OIT will update and publish the Vulnerability Disclosure Policy in accordance DHS Binding Operational Directive 20-01. Although DHS BOD 20-01 does not define a threshold for "immediate" reporting, SEC will define the time period as part of the associated VDP procedures (see Recommendation 3).

Recommendation 3: Develop and implement vulnerability disclosure-handling procedures that describe the SEC's process for implementing its VDP, in accordance with Department of Homeland Security Binding Operational Directives 20-01.

Response: We concur. OIT Security will review the vulnerability disclosure-handling procedures in Appendix D of SEC 24-04.SAC.28 *Vulnerability Management* OP and make updates, if necessary, that support Recommendation 2 and are compliant with DHS Binding Operational Directive 20-01.

Recommendation 4: [redacted]

Response: We concur. SEC had documented control requirements for account provisioning in SEC 24-04A, *Information Security and Privacy Controls Manual.* [redacted]

Recommendation 5: Update the SEC's system security plans with the latest baseline controls for all FISMA-reportable systems to ensure the SEC is assessing and monitoring the controls in accordance with the level of risk associated with each information security system.

Response: We concur. OIT will define a phased approach to complete SSP updates to align with the SEC's 24-04A, *Information Security and Privacy Controls Manual* which was updated in FY 2023 to meet NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organization*. The SEC's Information System Owners will update the SSPs according to the multi-year phased approach.

Recommendation 6: Develop and implement a log management process to ensure that:

a. [redacted]

b. [redacted]

Response: We concur. Per the SEC's 24-04A, *Information Security and Privacy Controls Manual*, Information System Owners (ISOs) and Business Owners (BOs) are responsible for identifying the types of events systems are able to log and coordinating with OIT Security about acceptable log formats. To address part a, [redacted] To address part b, [redacted]

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.

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