

REPORT NO. 584

November 25, 2024

OFFICE OF
**INSPECTOR
GENERAL**

OFFICE OF AUDITS

Fiscal Year 2024 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



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

M E M O R A N D U M

November 25, 2024

TO: Kenneth Johnson, Chief Operating Officer

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

SUBJECT: *Fiscal Year 2024 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA), Report No. 584*

Attached is the subject independent auditor's report. To conduct this evaluation, we contracted with Sikich CPA LLC (Sikich). Sikich planned and performed its work in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* and is wholly responsible for the attached report and the conclusions expressed therein. We monitored Sikich's performance throughout the evaluation to ensure compliance with professional standards and contract requirements.

Sikich reported that the SEC can further mature its information security program by designing and implementing new baseline controls, reviewing and approving elevated removable media access, enforcing recurring privileged user training requirements, performing information system business impact analyses, and handling certain incidents in a timely manner. As a result, Sikich concluded that the SEC's information security program did not meet the *Fiscal Year 2023-2024 Inspector General FISMA Reporting Metrics'* definition of "effective" and made 10 new recommendations for corrective action.

On October 10, 2024, we provided management with a draft of Sikich's report for review and comment. In its November 1, 2024, response, management concurred with Sikich's recommendations. Sikich included management's response as Appendix D of the attached report.

Within the next 45 days, please provide 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 description of the actions management plans to take to address each recommendation, and a timeframe for completing those actions.

We appreciate the courtesies and cooperation extended to us and Sikich 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
Corey Klemmer, 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, 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
Jason Tant, Acting 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 2024 Independent Evaluation of the SEC's
Implementation of the Federal Information Security
Modernization Act of 2014 (FISMA) Evaluation Report***



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

Abbreviations

	
DHS	U.S. Department of Homeland Security
EDR	Endpoint Detection and Response
FOIA	Freedom of Information Act
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
MEF	Mission-Essential Function
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
RTO	Recovery Time Objective
SEC, Commission, or agency	U.S. Securities and Exchange Commission
SP	Special Publication

Contents

EXECUTIVE SUMMARY	3
Introduction	3
Key Changes to the IG FISMA Metrics	3
Summary Evaluation Results.....	4
Management’s Response and Evaluator’s Comments.....	6
FISMA Evaluation Findings	7
Security Function: Identify	7
Finding 1: The SEC’s Risk Management Strategy is Three Years Out of Date.....	7
Security Function: Protect.....	8
Finding 2: The SEC Did Not Consistently Justify Elevated Removable Media Access in Sufficient Detail.....	9
Finding 3: The SEC’s [REDACTED]	10
Finding 4: The SEC Does Not Have [REDACTED]	12
Finding 5: The SEC Had Not Addressed the Results of a Workforce Study	13
Finding 6: The SEC Has Not Enforced Recurring Privileged User Training Requirements .	14
Security Function: Respond.....	15
Finding 7: The SEC Did Not Timely Inform the Security Operations Center of an Inadvertent and Unauthorized Spill of Personally Identifiable Information Event.....	15
Security Function: Recover.....	16
Finding 8: The SEC Conducted Its System Business Impact Analyses Using an Incomplete List of Mission-Essential Functions (MEFs).....	17
Finding 9: The SEC Disaster Recovery Test Did Not Test the Recovery Time Objectives (RTOs) of Individual Systems.....	18
Appendix A – Background	20
Appendix B – Objective, Scope, and Methodology	23
Appendix C – Prior-Year Recommendations	28
Appendix D – Management Comments	30

EXECUTIVE SUMMARY

INTRODUCTION

To protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation, the U.S. Securities and Exchange Commission (SEC, Commission, or agency) relies on more than 100 information systems. 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, Sikich CPA LLC (Sikich), to conduct the SEC's FISMA evaluation for Fiscal Year (FY) 2024. This report presents the results of Sikich'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 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' information 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 metrics") on a 2-year cycle based on a calendar agreed upon by the Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Security Agency. Therefore, in addition to the 20 core metrics, each agency is also required to evaluate an additional 17 supplemental metrics to conclude on the agency's overall cybersecurity posture in FY 2024. 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.

Inspectors General (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 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. The SEC's Assessed Maturity Level for FY 2024

Security Function	FY 2024 Assessed Maturity Level
Identify	Level 3: <i>Consistently Implemented</i>
Protect	Level 3: <i>Consistently Implemented</i>
Detect	Level 2: <i>Defined</i>
Respond	Level 4: <i>Managed and Measurable</i>
Recover	Level 3: <i>Consistently Implemented</i>
Overall Maturity	Level 3: <i>Consistently Implemented</i>

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

Since FY 2023, the SEC has made improvements in its information security program and practices, including:

- Continuing to develop Supply Chain Risk Management policies and procedures.
- Developing a process for conducting data exfiltration exercises.
- Implementing a process for reviewing hardware asset information in system security plans to identify any outdated hardware listings and maintain an up-to-date inventory of hardware assets connected to the SEC's network.
- Implementing a process to deploy configuration settings that include strong cryptographic controls on SEC workstations.
- Implementing strong authentication for all non-privileged users and, in accordance with Federal best practices, considering taking steps to ensure that users with local administrator privileges do not use the same credentials to perform privileged and non-privileged functions.

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

- [REDACTED]
- [REDACTED]
- Designing and implementing new baseline controls for agency systems based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.
- Implementing supply chain requirements.

- Maintaining its Risk Management documentation in accordance with agency policy.
- Reviewing and approving elevated removable media access in accordance with agency policy.
- Fully implementing [REDACTED]
- Enforcing recurring privileged user training requirements.
- Performing information system business impact analyses using accurate information.
- Comprehensively testing system recovery capabilities.
- Handling certain incidents in a timely manner.

These new 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 maintain its risk management strategy in accordance with agency policy.
- 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 3: *Consistently Implemented* because the SEC:
 - Did not appropriately manage its approvals for individuals granted elevated access to portable storage devices.
 - Did not effectively implement [REDACTED]
 - Did not have a [REDACTED]
 - Did not address the results of the most recent workforce study.
 - Did not enforce recurring privileged user training requirements.
- 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* because the SEC did not address all the prior-year recommendations related to this function during our evaluation's fieldwork phase, as shown in **Appendix C**. We did not issue any new recommendations for this function in FY 2024.
- 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. However, we did identify a control weakness involving an inadvertent disclosure of personally identifiable information was not routed to the Security Operations Center in a timely manner.

- 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 3: *Consistently Implemented* because the SEC:
 - Performed system business impact analyses based on an incomplete set of Mission-Essential Functions.
 - Did not test the recovery time objectives of individual systems.

MANAGEMENT'S RESPONSE AND EVALUATOR'S COMMENTS

The SEC concurred with all of the recommendations included in the report and stated it is pleased the report identified improvements to the SEC's information security programs across several domains, including Risk Management, Supply Chain Risk Management, Configuration Management, and Identity and Access Management. The SEC noted that the Office of Information Technology (OIT) remains committed to advancing the information security program's maturity, recognizing that not all metrics are assessed and scored annually. The SEC also noted that OIT's progress toward a strong information security program can be further seen through its successful remediation of 6 prior-year FISMA evaluation recommendations in FY 2024.

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 D**. Sikich 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.



Harrison Lee, CISA, CISM, CISSP, PMP
Principal, Sikich
November 25, 2024

FISMA Evaluation Findings

This report describes the five FISMA functions and our findings and provides recommendations 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 National Institute of Standards and Technology (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.

Finding 1: The SEC's Risk Management Strategy is Three Years Out of Date

Fiscal Year (FY) 2024 IG FISMA Function: Identify / Domain: Risk Management

Effective risk management requires that organizations operate in highly complex, interconnected environments using state-of-the-art and legacy information systems to accomplish their missions and to conduct important business-related functions. A risk management strategy should address how the organization intends to assess, respond to, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions.

NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, control PM-9: Risk Management Strategy states that organizations should develop and implement a comprehensive strategy to manage security and privacy risks, and review and update the strategy to address organizational changes. NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*, provides tasks and expected outcomes for agencies when executing the Risk Management Framework. Task P-2 of the Framework is to “Establish a risk management strategy for the organization that includes a determination of risk tolerance.” Further, NIST SP 800-39, *Managing Information Security Risk*, states that it is imperative for leaders and managers at all levels to understand their responsibilities and be held accountable for managing information security risk (i.e., the risk associated with the operation and use of information systems that support the missions and business functions of their organizations).

The *FY 2023 – 2024 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* measure the extent to which an organization adequately manages risk at the organizational, mission/business process, and information system levels. The SEC has implemented a risk management strategy pursuant to NIST SP 800-39 that defines its strategy for managing risks across these levels.

However, the SEC did not maintain its risk management strategy in accordance with SEC Administrative Regulation 24-04, *Information Technology Security Program*, dated November 14, 2018. Although this SEC Administrative Regulation states that the SEC should update its risk management strategy every

three years, or as required, the Office of Information Security within the Office of Information Technology (OIT) last updated the strategy document on March 6, 2018.

OIT stated that this issue occurred because OIT and the Office of the Chief Operating Officer did not coordinate to align their activities and documentation. OIT is responsible for maintaining SEC Administrative Regulation 24-04.

On September 25, 2024,² the Chief Operating Officer signed a memorandum concurring with the Chief Risk Officer's recommendation to retire the Risk Management Strategy. In the memorandum, the Chief Risk Officer acknowledges that the Risk Management Strategy is out of date and no longer reflects current SEC risk management activities. Accordingly, the SEC will create a new SEC Administrative Regulation addressing enterprise risk management at the agency, and among other things, require a 4-year review cycle.

Without routinely updating its risk management strategy, the SEC has reduced assurance that organization-level mechanisms used to manage and monitor risks continue to be aligned with the SEC's mission, goals, and current business environment.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's Risk Management program, we recommend that the Office of the Chief Operating Officer, in collaboration with agency stakeholders, to include the Office of Information Technology:

1. Complete efforts to document and implement an enterprise-wide risk management strategy that incorporates the review and approval processes set forth in agency policy.

Management's Response: Management concurred with the recommendation and stated that agency staff will develop an administrative regulation addressing enterprise risk management at the agency. We have included management's complete response in **Appendix D**.

Sikich'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 Following the conclusion of our fieldwork period on June 14, 2024.

Finding 2: The SEC Did Not Consistently Justify Elevated Removable Media Access in Sufficient Detail

FY 2024 IG FISMA Function: Protect / Domain: Data Protection and Privacy

A portable storage device is a system component that can communicate with and be added to—or removed from—a system or network and that is limited to data storage (text, video, audio, or image data) as its primary function. Examples of portable storage devices include optical discs, removable hard drives, and flash memory devices. Although these devices give users more convenient access to data, they also increase the risk of data loss and data exposure. Organizations should therefore restrict portable storage device use to authorized personnel.

The *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations limit the transfer of data to removable media. NIST SP 800-53, Revision 5, states that agencies must restrict access to organization-defined types of digital and/or non-digital media to organization-defined personnel or roles.

The SEC did not appropriately manage its approvals for individuals granted elevated access to portable storage devices. Specifically, we noted that the SEC defined four access levels (0 through 3) in its File and Removable Media Policy:

- Level 0: No access
- Level 1: Read-only
- Level 2: Ability to save to removable media with encryption
- Level 3: Ability to save to removable media without encryption

Users who need access at levels 2 and 3 must formally request approval, which includes a written justification from the user's supervisor or the contracting officer's representative. We compared the list of 279 individuals who had elevated access to portable storage devices to the corresponding approvals and noted the following:

- Two individuals did not have a written justification indicating why they needed the exception.
- The SEC determined that one individual no longer needed elevated access in 2023. However, the individual retained that access in 2024.

Supervisors did not consistently provide detailed business justifications for elevated access. Although some justifications included the exact task for which the exception was needed, other justifications were more generic; in some cases, the supervisor did not provide a justification at all. OIT Security approved the generic justifications despite their non-compliance with the policy.

Without an effective process for managing use of portable storage devices, individuals without a business need may employ those devices, increasing the risk of SEC data loss and exposure.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's Data Protection and Privacy program, we recommend that the Office of Information Technology:

2. Update the approval process to require that File and Removable Media Policy exception justifications contain a specific business or technical need for the elevated access.

Management's Response: Management concurred with the recommendation and stated that OIT will review and update the existing categories in the Justification field of the [REDACTED] Removable Media Exception workflow to align to typical exception reasons more closely. In addition, OIT will provide additional guidance on the Additional Information field, which is a required field when the Justification of "Reason not listed" is selected. We have included management's complete response in **Appendix D**.

Sikich'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.

Finding 3: The SEC's [REDACTED]

FY 2024 IG FISMA Function: Protect / Domain: Data Protection and Privacy

Organizations such as the SEC hold sensitive data that stakeholders expect them to protect. Data loss could substantially harm not only an organization's mission, but also its reputation. To limit the risk of data loss, organizations should take measures to understand the sensitive data they hold, how they control that data, and how to prevent individuals from removing the data without authorization.

The *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations develop and implement procedures for data exfiltration. NIST SP 800-53, Revision 5, states that agencies must take measures to prevent the exfiltration of information.

[REDACTED]

[REDACTED]

[REDACTED]

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's Data Protection and Privacy program, we recommend that the Office of Information Technology, together with the Office of the Chief Data Officer:

- 3. [REDACTED]

Management's Response: Management concurred with the recommendation and stated [REDACTED]

[REDACTED] We have included management's complete response in **Appendix D**.

Sikich'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.

- 4. [REDACTED]

Management's Response: Management concurred with the recommendation and stated [REDACTED]

[REDACTED] We have included management's complete response in **Appendix D**.

Sikich'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.

Finding 4: The SEC Does Not Have [REDACTED]

FY 2024 IG FISMA Function: Protect / Domain: Data Protection and Privacy

Protecting “endpoints,” the physical devices connected to a network, such as mobile phones, virtual machines, laptops, and workstations, can identify and isolate threats before they spread throughout the network. An Endpoint Detection and Response (EDR) solution continuously monitors network endpoints and automatically takes action to mitigate threats.

The *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations use EDR capabilities to support host-level visibility, attribution, and response for its information systems. EDR implementation is also an administration priority. Office of Management and Budget (OMB) Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, requires agencies to coordinate with the Cybersecurity and Infrastructure Security Agency to implement EDR solutions.

The SEC demonstrated that its EDR solution was able to detect suspicious activity and integrate observations into the agency’s incident detection processes. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

RECOMMENDATION, MANAGEMENT’S RESPONSE, AND EVALUATION OF MANAGEMENT’S RESPONSE

To improve the SEC’s Data Protection and Privacy program, we recommend that the Office of Information Technology:

5. [REDACTED]

Management’s Response: Management concurred with the recommendation and stated [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] We have included management’s complete response in **Appendix D.**

Sikich'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.

Finding 5: The SEC Had Not Addressed the Results of a Workforce Study

FY 2024 IG FISMA Function: Protect / Domain: Security Training

In an ever-changing cybersecurity landscape, an organization must ensure that its IT professionals not only possess the necessary skills but also maintain familiarity with emerging technologies and potential threats. Organizations do this by conducting periodic workforce skills assessments and addressing any identified gaps in knowledge, skills, and abilities, either through training or through talent acquisition.

For this reason, the *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations perform workforce assessments and take actions based on skill gaps identified. NIST SP 800-53, Revision 5, states that agencies must establish a security and privacy workforce development and improvement program.

The SEC Information Technology Security Program requires OIT and the SEC's Office of Human Resources to conduct competency assessments every other year to identify knowledge and skills gaps for users with significant security and privacy responsibilities. However, because of the level of effort involved, the SEC has only conducted these assessments every five years. The most recent study was completed in 2018; another study was in progress during our evaluation.

To conduct an assessment, the SEC first identifies relevant job functions (e.g., cybersecurity) and works with subject matter experts to build competency models that delineate the qualities and skills needed. Job function supervisors then complete surveys based on the competency models. The competency study team analyzes the results and shares the results with Divisions and Offices to take appropriate follow up action to guide training and future hiring.

When our testing concluded, the SEC received the study results but had not developed and implemented a responsive action plan. Given the amount of time that had passed since the last workforce assessment (more than five years), we concluded that the SEC has not taken actions to address its knowledge and skills gaps.

If the SEC does not address its identified skills gaps in a timely manner, its personnel may not be equipped to adapt to emerging technologies or respond to newer threats. This increases the risk that the SEC may not be able to effectively implement controls meant to protect SEC systems and data.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's Security Training program, we recommend that the Office of Information Technology:

6. Develop a plan to address the findings of the cybersecurity competency study.

Management's Response: Management concurred with the recommendation and stated that it will utilize the competency study results to develop a human capital plan to improve the skills, knowledge, and abilities of its cybersecurity workforce. We have included management's complete response in **Appendix D**.

Sikich'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.

Finding 6: The SEC Has Not Enforced Recurring Privileged User Training Requirements

FY 2024 IG FISMA Function: Protect / Domain: Security Training

Organizations like the SEC rely on key personnel—such as security engineers, configuration managers, and system, network, and database administrators—to ensure that their information technology operations are secure. Their job responsibilities include administering and making modifications to the SEC's information systems. They are known as "privileged users" because their jobs involve a level of access beyond that of ordinary users. Privileged access to information systems and data carries elevated security risks, so privileged users require appropriate role-based training. This role-based training is different from general security awareness training that organizations provide to all of their system users.

The *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations develop and administer role-based training for individuals who have significant security responsibilities and access. NIST SP 800-53, Revision 5, states that agencies must provide role-based security and privacy training to these privileged users.

The SEC developed multiple role-based and tool-specific trainings for individuals who have key security responsibilities, including privileged users. Among other topics, trainings for these users cover general privileged user responsibilities, privileged user restrictions and prohibitions, and consequences of improper use of privileged access rights.

As part of the account approval process, the SEC requires prospective privileged users to demonstrate that they have completed the trainings before it grants them access to their privileged roles. Further, the SEC's written procedures require that privileged users complete role-based annually. However, the SEC could not demonstrate that its privileged users completed the annual training and did not have a mechanism for reducing their access if they failed to do so.

Without recurring privileged user training, the SEC has less assurance that users are aware of the security responsibilities that accompany their elevated roles. This decreased awareness increases the risk of key security control deficiencies that occur as a result of human error.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's Security Training program, we recommend that the Office of Information Technology:

7. Develop and implement a mechanism to enforce recurring privileged user training for applicable personnel.

Management's Response: Management concurred with the recommendation and stated that it will review and enforce its privileged user training procedures for assigning, managing, and reporting compliance for applicable personnel. We have included management's complete response in **Appendix D**.

Sikich'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.

Finding 7: The SEC Did Not Timely Inform the Security Operations Center of an Inadvertent and Unauthorized Spill of Personally Identifiable Information Event

FY 2024 IG FISMA Function: Respond / Domain: Incident Response

Computer security incident response is an important component of information technology programs. Because responding to incidents effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential. It is also vital to build relationships and establish suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement).

The *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations can detect and respond to incidents. NIST SP 800-53, Revision 5, states that agencies must require personnel to report suspected incidents to the organization's incident response unit within a reasonable period.

We noted an event in which an IT component failed to timely inform the response team of an information spill, leading to a delayed response. On March 22, 2024, a user self-reported to the Vulnerability Dispute Approver team that they had inadvertently sent to another government entity an unencrypted file that included social security numbers and other personally identifiable information for more than 5,000 individuals. The Vulnerability Dispute Approver team did not forward this notification to the Security

Operations Center in a timely manner. As a result, the Security Operations Center did not classify and respond to the event until May 2, 2024. This communication breakdown occurred because the Vulnerability Dispute Approver team was unfamiliar with the incident response process and lacked training and experience as to who should be notified of an incident.

Without ensuring that personnel timely communicate information regarding potential incidents to the unit charged with incident response, the SEC may fail to timely identify and address security issues, which increases the threat to SEC systems and data and risks reputational harm and diminished public trust.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

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

8. Identify a list of SEC teams that operate in capacities relevant to the agency's incident response capability and provide those teams with training to ensure that they correctly report potential incidents in a timely manner.

Management's Response: Management concurred with the recommendation and stated that the recipient (at another federal agency) was authorized to receive the information and the email in question had been encrypted, and therefore no breach occurred. The team that was noted as having received the report from the user does not work with incident tickets, and therefore had no reason to regularly check for this type of ticket assignment. Once the ticket was discovered, the team forwarded it to the Security Operations Center. To address this recommendation, OIT will identify teams that manage [REDACTED] workflows and provide an additional communication to remind individuals to re-route any misreported incidents to the correct party. We have included management's complete response in **Appendix D**.

Sikich'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: RECOVER

The objective of the Recover function is to develop 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.

Finding 8: The SEC Conducted Its System Business Impact Analyses Using an Incomplete List of Mission-Essential Functions (MEFs)

FY 2024 IG FISMA Function: Recover / Domain: Contingency Planning

According to Federal Continuity Directive 2, the U.S. Federal Government is responsible for eight national essential functions that it must sustain before, during, and in the aftermath of a catastrophic emergency. The SEC directly supports national essential function 7, *Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems*, by conducting its primary MEF, *Regulatory Oversight: Monitor Financial Markets and Provide Crisis Management*. The SEC also performs a series of other MEFs that are related to the mission set forth in its statutory or executive charter. The SEC must use its people, processes, and technology to ensure that, even in an emergency, it can perform its primary and other MEFs.

In accordance with Federal Continuity Directive 2, federal agencies, including the SEC, are required to complete an organization-wide biennial Business Process Analysis/Business Impact Analysis to confirm their readiness and ability to perform their primary MEF and other MEFs. Separately, the SEC also conducts business impact analyses for individual systems to determine the systems' recovery priority should an event disrupt their operation. Generally, systems that directly support an MEF must become operable relatively quickly to avoid unacceptable business consequences.

The *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations use business impact analyses as part of their contingency planning efforts.

The SEC conducted an organizational Business Process Analysis/Business Impact Analyses in March 2023 that identified 22 MEFs, consistent with prior years. However, for the system-level Business Impact Analysis, the SEC used a template that only lists four MEFs. As a result, the criticality analysis was incomplete, leaving the SEC without adequate assurance that the recovery measures for each system are commensurate with the impact of their loss. The SEC acknowledged this oversight and will update the business impact analysis template to reflect the full set of 22 MEFs.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's Contingency Planning program, we recommend that the Office of Information Technology:

9. Update its business impact analysis template to ensure that the SEC assesses all systems using a correct and comprehensive set of mission-essential functions.

Management's Response: Management concurred with the recommendation and stated that it will update the business impact analysis template to align with the SEC's mission-essential functions defined in the SEC's Continuity Plan. We have included management's complete response in **Appendix D**.

Sikich'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.

Finding 9: The SEC Disaster Recovery Test Did Not Test the Recovery Time Objectives (RTOs) of Individual Systems

FY 2024 IG FISMA Function: Recover / Domain: Contingency Planning

The SEC relies on individual systems to support its organizational operations. These systems vary in their importance to the SEC's mission. Some systems would irrevocably harm the SEC's capabilities if they were inoperable for several hours, while other systems might be inoperable for days without significant consequences. The exact length of time a system can be inoperable is captured in a measure called the RTO, described by NIST as "the overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes." The RTO of a particular system drives the design and testing its of recovery mechanism.

The *FY 2023 – 2024 IG FISMA Reporting Metrics* measure the extent to which organizations can demonstrate that their recovery mechanisms can meet the RTO for each system. NIST SP 800-53, Revision 5, states that agencies must provide for the recovery and reconstitution of systems to a known state within the RTO after a disruption, compromise, or failure.

At the time of our fieldwork, the SEC's most recent disaster recovery exercise—conducted beginning in the second half of calendar year 2022³—did not test the RTOs of individual systems. Instead, the exercise focused primarily on whether the SEC's backup data center could sustain primary data center operations for an extended period of time. To perform this test, the SEC failed over⁴ its systems to the backup data center over a two-day period, operated from the backup data center for three months, and failed back. This procedure could not and did not demonstrate whether the SEC's highest priority information systems—those with an RTO of less than four hours—could in fact be recovered within that timeframe. The exercise's after-action report acknowledged this limitation, stating that the exercise did not evaluate the SEC's ability to meet the RTOs of the information systems.

Without confirming through testing that its systems can be recovered in accordance with their RTOs, the SEC will not have reasonable assurance that its recovery measures are sufficient to restore critical systems before they are inoperable for an intolerable time period.

³ The SEC published an after-action report for the May 2024 disaster recovery exercise on June 18, 2024, four calendar days after the conclusion of our fieldwork period. As such, we did not consider this report in our results. We did inspect the 2024 report following the conclusion of the fieldwork period and confirmed that condition persisted (i.e., the SEC did not perform RTO assessments).

⁴ Failover is the capability to switch over to a redundant or standby information system upon the failure or abnormal termination of the previously active system. See <https://csrc.nist.gov/glossary/term/failover> (last accessed August 28, 2024) for more detail.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's Contingency Planning program, we recommend that the Office of Information Technology:

10. Incorporate assessments of system recovery time objectives into future disaster recovery exercises.

Management's Response: Management concurred with the recommendation and stated that OIT will coordinate with the SEC Continuity team to establish RTOs for SEC systems that support agency continuity operations. Once the RTOs are updated, the SEC will incorporate timeframe-based testing of the RTOs into future disaster recovery exercises. We have included management's complete response in **Appendix D**.

Sikich'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)⁵ and the Securities Exchange Act of 1934 (Securities Exchange Act),⁶ 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),⁷ 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 109 FISMA-reportable systems in place to support its mission. These systems are rated as low- and moderate-impact, and contractors operate more than one-third of them.

OIT is led by the SEC Chief Information Officer and supports the SEC's mission and its related strategic objectives by aligning its activities to the Commission's objectives and strategic goals. OIT plays a critical role in the SEC's performance by providing strategic direction and leadership that promotes sound investment in technologies that provide the tools required to collect, analyze, and act upon the enormous volume of financial data and other information required to protect investors; maintain fair, orderly, and

⁵ See <https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#secact1933> (last accessed on July 30, 2024) for more detail.

⁶ See <https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#secact1934> (last accessed on July 30, 2024) for more detail.

⁷ See <https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#df2010> (last accessed on July 30, 2024) for more detail.

efficient markets; and facilitate capital formation. OIT missions, functions, and strategic goals are aligned with SEC strategic goals and outcomes.

FISMA and U.S. Department of Homeland Security (DHS) Reporting Metrics

FISMA⁸ 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 Office of inspector General (OIG) to perform an annual evaluation of the effectiveness of the agency's information security program and practices and to report the results to OMB.

OMB,⁹ the Cybersecurity and Infrastructure Security Agency,¹⁰ the Council of the Inspectors General on Integrity and Efficiency,¹¹ the agency Chief Information Security Officer council, 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 2** 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 2. FY 2023 – 2024 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: Sikich-generated based on FY 2023 – 2024 IG FISMA Reporting Metrics.

⁸ Public Law No. 113-283 (December 2014). FISMA's obligations for federal agencies and for federal IGs, as relevant to this evaluation, are codified chiefly in 44 U.S. Code §§ 3554 and 3555, respectively.

⁹ OMB issues information security policies and guidelines for federal information resources pursuant to various statutory authorities.

¹⁰ The Cybersecurity and Infrastructure Security Agency is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

¹¹ The Council of the Inspectors General on Integrity and Efficiency 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.

DHS¹² organized the *FY 2023-2024 IG FISMA Reporting Metrics* 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 DHS transitioned the IG metrics reporting process to a multi-year cycle. In FY 2023, DHS updated the *FY 2023-2024 IG FISMA Reporting Metrics* to include the 20 core metrics from FY 2022, along with 17 supplemental metrics for the FY 2024 review cycle.

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 two 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 3** 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 3. Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: <i>Ad-hoc</i>	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: <i>Defined</i>	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: <i>Consistently Implemented</i>	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: <i>Managed and Measurable</i>	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: <i>Optimized</i>	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*.

¹² 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. It also serves as the operational lead for federal cybersecurity.

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 2024 in accordance with FISMA. The evaluation included assessing the effectiveness of security controls for a subset of systems. We performed this evaluation under the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

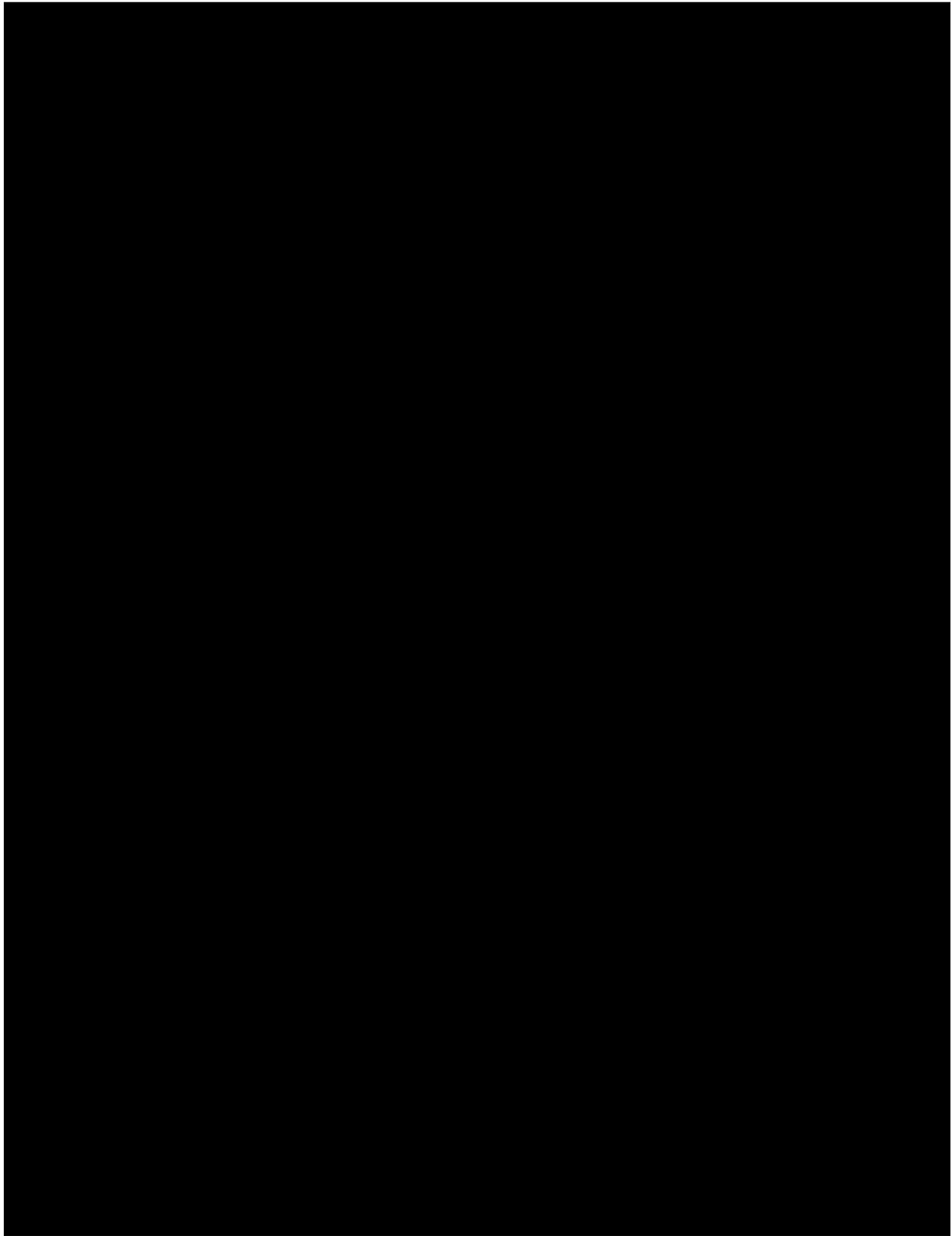
Scope

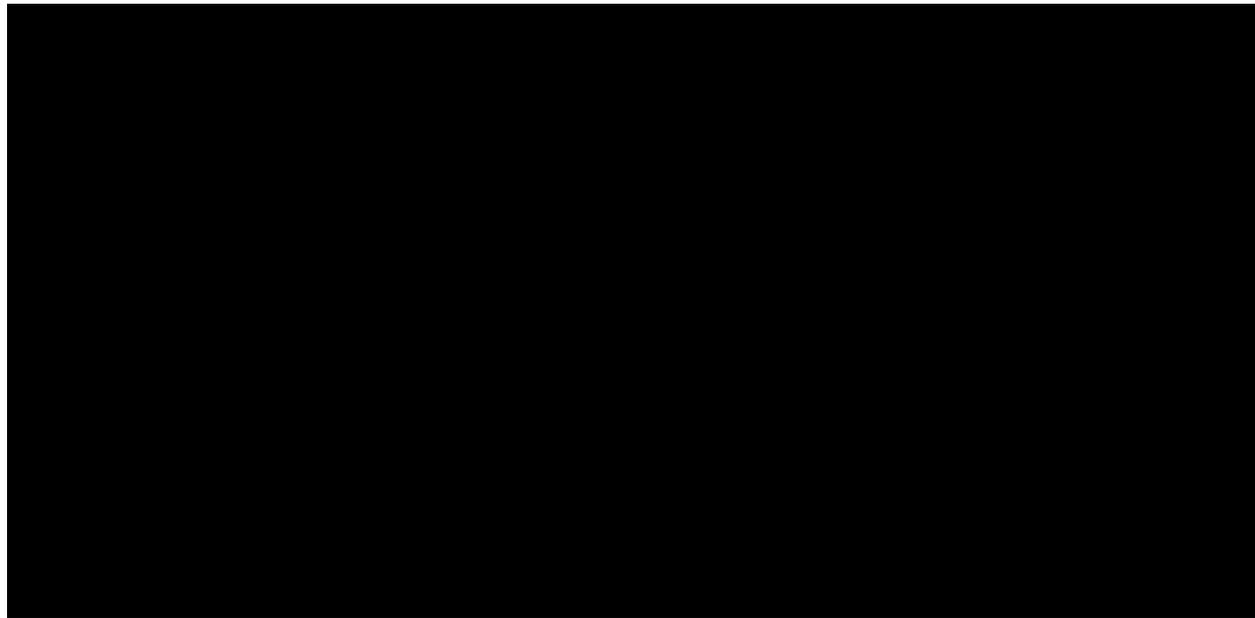
The evaluation covered the period between October 1, 2023, and June 14, 2024, and included assessing the effectiveness and maturity of the SEC's information security program, focusing on the 20 core metrics and 17 supplemental metrics spread across the nine domains identified in the *FY 2023-2024 IG FISMA Reporting Metrics*. Sikich judgmentally selected and reviewed a non-statistical sample of eight of the SEC's 109 FISMA-reportable information systems. This sample represents approximately seven percent of the SEC's inventory of FISMA-reportable information systems. To select the sample, Sikich used the following criteria:

- Systems that were not tested in the prior three 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.

The sample consisted of the internally and externally hosted systems shown in **Table 4**. To assess system security controls, Sikich reviewed the SEC's security assessment packages, privacy program, and account management for the eight FISMA-reportable systems sampled.







Source: Sikich-generated based on systems report extracted from OIT [REDACTED].

Methodology

We conducted this evaluation from February to November 2024 in accordance with the Council of the Inspectors General on Integrity and Efficiency'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 objective. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objective.

To accomplish the evaluation objective, 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 the guidance and definitions from the *FY 2023-2024 IG FISMA Reporting Metrics*. Relevant evaluation criteria that we 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*¹³
- NIST SPs
- DHS Binding Operational Directives
- SECURE Technology Act¹⁴
- Federal Enterprise Architecture Framework, Version 2¹⁵

Sikich also followed up on all prior-year recommendations that were open at the start of the FY 2024 evaluation and that impact the effectiveness of the SEC's information security program. Additionally, we reviewed remediation packages that the SEC submitted. See **Appendix C** for more detail.

Internal Controls: Consistent with our evaluation objective, we did not assess the OIT's overall management control structure. Instead, Sikich reviewed the OIT's Memorandum of Unmodified Statement Assurance. Based on our review, Sikich determined that SEC 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 internal controls were in compliance with underlying management principles, which incorporate the Government Accountability Office's *Standards for Internal Control in the Federal Government*. Based on the results of the assessment, the SEC OIT stated that internal control over operations, reporting, and compliance were operating effectively through September 30, 2023.

Data Reliability: The Government Accountability Office's *Assessing Data Reliability* (GAO-20-283G), dated December 2019, states that 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 measure 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 reflects the actual underlying information.

¹³ Executive Order 14028 can be found at <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity> (last accessed on July 31, 2024).

¹⁴ The SECURE Technology Act is publicly available. Please see <https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf> (last accessed on July 31, 2024).

¹⁵ The Federal Enterprise Architecture is publicly available. Please see https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf (last accessed on July 31, 2024).

Sikich 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 the FISMA-reportable information systems inventory. Sikich performed data reliability, completeness, and accuracy testing 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 were sufficiently reliable to support our conclusions.

Prior Coverage: As of July 31, 2024, the SEC implemented corrective actions to close six prior-year recommendations in FY 2024 from the FY 2017 through FY 2023 FISMA evaluations. Although OIT addressed these recommendations, as noted in this report, areas requiring improvement 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

The SEC implemented corrective actions to close seven prior-year recommendations from the FY 2017 through FY 2023 FISMA evaluations. Another five recommendations remain open, as depicted in **Table 5**. In addition, we identified 10 new recommendations for FY 2024, as discussed in this report.

Table 5. Recommendation Status

Domain	Prior Report and Recommendation Number	Recommendation	Status
Risk Management	574-3	Develop and implement a process to review hardware asset information listed in System Security Plans for outdated or inaccurate hardware listings as part of the annual System Security Plan reviews in order to consistently maintain an up-to-date inventory of hardware assets connected to the agency's network.	Closed as of January 17, 2024
	574-5	Develop and implement a process to deploy configuration settings on agency workstations that include the agency's strong cryptographic controls to ensure the consistent implementation and maintenance of security configurations for agency workstations.	Closed as of January 30, 2024
Configuration Management	574-6	Implement the defined processes for [REDACTED]	Open
	580-1	Define and implement [REDACTED] Plans of Action and Milestones.	Open
	580-2	Update the Vulnerability Disclosure Policy to include all internet-accessible systems. Once OIT has updated the Vulnerability Disclosure Policy, the SEC should immediately report to the Cybersecurity and Infrastructure Security Agency regarding: <ul style="list-style-type: none"> 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 Cybersecurity and Infrastructure Security Agency 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 Cybersecurity and Infrastructure Security Agency. 	Closed as of August 20, 2024*
	580-3	Develop and implement vulnerability disclosure-handling procedures that describe the SEC's process for implementing its Vulnerability Disclosure Policy, in	Closed as of November 19, 2024*

Domain	Prior Report and Recommendation Number	Recommendation	Status
		accordance with Department of Homeland Security Binding Operational Directive 20-01.	
Identity, Credential, and Access Management	546-12	Implement strong authentication for all non-privileged users, and, in accordance with Federal best practices, consider taking steps to ensure that users with local administrator privileges did not use the same credentials to perform privileged and non-privileged functions.	Closed as of July 9, 2024*
	574-7	Develop and implement a process, including the timelines, for completing user access recertification for information systems that have moved to a cloud service provider in order to ensure the consistent completion of user access recertification for the U.S. Securities and Exchange Commission's information systems on a biannual basis.	Closed as of January 30, 2024
	580-4	[REDACTED]	Open
Data Protection and Privacy	574-8	Develop a process for conducting data exfiltration exercises in order to manage and measure the effectiveness of the agency's data exfiltration and enhanced network defenses.	Closed as of January 30, 2024
Information Security Continuous Monitoring	580-5	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.	Open
Incident Response	580-6	Develop and implement a log management process to: a. [REDACTED] b. [REDACTED]	Open

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

*The SEC submitted the closure package for this recommendation after our fieldwork phase concluded. Sikich assessed the closure package and concluded that the recommendation could be closed.

Appendix D – 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: Kenneth A. Johnson, Chief Operating Officer **KENNETH JOHNSON**
David Bottom, Chief Information Officer **Bottom David**

Date: November 1, 2024

Subject: Management Response to OIG Report, *Fiscal Year 2024 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014*

Digitally signed by KENNETH JOHNSON
Date: 2024.11.01
13:25:33 -0400

Digitally signed by Bottom, David
Date: 2024.11.01
15:37:42 -0400

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) 2024. The Report evaluates the SEC's information security program in accordance with the *FY 2023-2024 Inspector General FISMA Reporting Metrics*,¹¹ 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*.¹²

We are pleased your Report has highlighted improvements in the SEC's information security program particularly in supply chain, risk management, configuration management, and identity and access management. The SEC's Office of Information Technology (OIT) remains committed to advancing the program's maturity, recognizing that not all metrics are assessed and scored annually. A testament to our ongoing progress is the successful resolution of previous findings, with the OIG confirming the closure of seven prior-year recommendations in FY 2024, six of which were specific to FISMA. Moving forward, we are dedicated to strengthening the Agency's security posture and continuously maturing our program in alignment with FISMA metrics and industry best practices.

We concur with your Report's 10 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, Sikich, 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: Shelly Luisi, 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: Complete efforts to document and implement an enterprise-wide risk management strategy that incorporates the review and approval processes set forth in agency policy

Response: We concur. Agency staff will develop an administrative regulation addressing enterprise risk management at the agency.

Recommendation 2: Update the approval process to require that File and Removable Media Policy exception justifications contain a specific business or technical need for the elevated access.

Response: We concur. OIT will review and update the existing categories in the Justification field of the [REDACTED] Removable Media Exception workflow to align to typical exception reasons more closely. In addition, OIT will provide additional guidance on the Additional Information field, which is a required field when the Justification of "Reason not listed" is selected.

Recommendation 3: [REDACTED]

Response: We concur [REDACTED]
[REDACTED]
[REDACTED]

Recommendation 4: [REDACTED]

Response: We concur [REDACTED]
[REDACTED]
[REDACTED]

Recommendation 5: [REDACTED]
[REDACTED]

Response: We concur [REDACTED]
[REDACTED]
[REDACTED]

Recommendation 6: Develop a plan to address the findings of the cybersecurity competency study.

Response: We concur. OIT will utilize the competency study results to develop a human capital plan to improve the skills, knowledge, and abilities of its cybersecurity workforce.

Recommendation 7: Develop and implement a mechanism to enforce recurring privileged user training for applicable personnel.

Response: We concur. OIT will review and enforce its privileged user training procedures for assigning, managing, and reporting compliance for applicable personnel.

Recommendation 8: Identify a list of SEC teams that operate in capacities relevant to the agency's incident response capability and provide those teams with training to ensure that they correctly report potential incidents in a timely manner.

Response: We concur. For additional context regarding the event described in the OIG's Finding 7, Recommendation 8, the Agency determined that the recipient (at another federal agency) was authorized to receive the information and the email in question had been encrypted, and therefore no breach occurred. The team that was noted as having received the report from the user does not work with incident tickets, and therefore had no reason to regularly check for this type of ticket assignment. But once the ticket was discovered the team forwarded it to the Security Operations Center.

The SEC's Security Operations Center is comprised of skilled subject matter experts in matters related to incident handling. Further, all staff are provided guidance in annual training about reporting potential incidents, which is further reinforced in multiple SEC Regulations and SEC Today announcements.

To address this recommendation, OIT will identify teams that manage [REDACTED] workflows and provide an additional communication to remind individuals to re-route any misreported incidents to the correct party.

Recommendation 9: Update its business impact analysis template to ensure that the SEC assesses all systems using a correct and comprehensive set of mission-essential functions.

Response: We concur. OIT will update the business impact analysis template to align with the SEC's mission-essential functions defined in the SEC's Continuity Plan.

Recommendation 10: Incorporate assessments of system recovery time objectives into future disaster recovery exercises.

Response: We concur. OIT will coordinate with the SEC Continuity team to establish recovery time objectives for SEC systems that support agency continuity operations. Once the recovery time objectives (RTO) are updated, the SEC will incorporate timeframe-based testing of the RTOs into future disaster recovery exercises.

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

