U.S. SECURITIES AND EXCHANGE COMMISSION

REPORT NO. 589

February 25, 2026

OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

Fiscal Year 2025 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

February 25, 2026

TO: Peter Gimbrere, Managing Executive, Office of the Chairman

FROM: Kevin Muhlendorf, Inspector General KEVIN MUHLENDORF Digitally signed by KEVIN MUHLENDORF Date: 2026.02.25 16:36:23 -05'00'

SUBJECT: *Fiscal Year 2025 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA)*, Report No. 589

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 has improved its information security program since fiscal year 2024. However, outstanding recommendations from prior year FISMA evaluations continue to present risk to the agency, and the SEC faced challenges in meeting zero-trust architecture compliance milestones. As a result, Sikich concluded that the SEC's information security program did not meet the *Fiscal Year 2025 Inspector General FISMA Reporting Metrics*' definition of "effective," and made two new recommendations for corrective action.

On January 15, 2026, we provided management with a draft of Sikich's report for review and comment. In its February 18, 2026, response, management concurred with Sikich's recommendations and included planned corrective actions with timeframes. Sikich included management's response as Appendix F of the attached report.

We appreciate the courtesies and cooperation extended to us and Sikich during the evaluation. If you have questions, please contact me or Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Paul S. Atkins, Chairman
Michael Friedman, Chief of Staff, Office of Chairman Atkins
Ugonna Eze, Deputy Chief of Staff, Office of Chairman Atkins
Mark Berman, Counsel to the Chairman, Office of Chairman Atkins
Hester M. Peirce, Commissioner
Benjamin Vetter, Counsel, Office of Commissioner Peirce
Mark T. Uyeda, Commissioner
Ivan V. Griswold, Counsel, Office of Commissioner Uyeda
J. Russell McGranahan, General Counsel

Elizabeth McFadden, Deputy General Counsel, General Law, Office of the General Counsel
Erik Hotmire, Director, Office of Public Affairs
Natalia Díez Riggin, Director, Office of Legislative and Intergovernmental Affairs
Charlene Arietti Gold, Acting Chief Operating Officer
Shelly Luisi, Chief Risk Officer
Jim Lloyd, Audit Coordinator/Assistant Chief Risk Officer, Office of the Chief Risk Officer
Jed Hickman, Acting Director/Chief Information Officer, Office of Information Technology
Jeffrey King, Chief Information Security Officer, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance, Office of Information Technology

U.S. SECURITIES AND EXCHANGE COMMISSION

OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

Fiscal Year 2025 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA) Evaluation Report

SIKICH®

REDACTED FOR PUBLIC RELEASE

Abbreviations

CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
CSF 2.0	Cybersecurity Framework Version 2.0
DLP	Data Loss Prevention
DNS	Domain Name System
FISMA	The Federal Information Security Modernization Act of 2014
FY	Fiscal Year
HTTPS	Hypertext Transfer Protocol Secure
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
PAM	Privileged Access Management
SEC, Commission, or agency	U.S. Securities and Exchange Commission
Sikich	Sikich CPA LLC
SP	Special Publication
TLS	Transport Layer Security
ZTA	Zero Trust Architecture

Contents

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) or by an independent external auditor, as determined by the Inspector General (IG). 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) 2025. 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

Several stakeholders, including the Office of Management and Budget (OMB), Cybersecurity and Infrastructure Security Agency (CISA), Council of the Inspectors General on Integrity and Efficiency (CIGIE), and agency Chief Information Security Officer council, coordinated to develop a set of "IG metrics" for OIGs to use in evaluating the effectiveness of agency information security programs and practices. The stakeholders updated the IG metrics for FY 2025 as follows:

- The stakeholders created a new FISMA function (*Govern*) that includes a new domain *(Cybersecurity Governance*), as well as three new supplemental metrics to highlight the role that governance plays in managing cybersecurity risks and incorporating cybersecurity into the broader enterprise risk management strategy. Additionally, the stakeholders moved the Supply Chain Risk Management domain to the *Govern* function and renamed it Cybersecurity Supply Chain Risk Management. Furthermore, the stakeholders added a new Risk and Asset Management domain to the existing *Identify* function to group metrics related to system, hardware, and software inventories, along with data management.[2]
- The stakeholders created two new supplemental metrics related to Zero Trust Architecture (ZTA) implementation that assess the maturity of an organization's (1) data management capabilities and (2) ability to monitor and measure the integrity and security posture of assets.
- The stakeholders revised the core metric regarding information system-level risk management to focus on the implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework.

[1] Public Law 113-283, Federal Information Security Modernization Act of 2014 (December 18, 2014).
[2] The stakeholders made these changes to align with the NIST Cybersecurity Framework Version 2.0.

The IG metrics align with the six function areas included in the NIST Cybersecurity Framework Version 2.0 (CSF 2.0): Govern, Identify, Protect, Detect, Respond, and Recover. CSF 2.0 provides (1) agencies with a common structure for managing and reducing cybersecurity risks, and (2) IGs with guidance for assessing the maturity of controls to address those risks. The IG metrics state that OIGs should also consider data points, such as the results of penetration testing, to support their risk-based determinations of maturity and effectiveness.

In FY 2025, 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. In addition to the 20 core metrics, each IG is also required to evaluate the 5 new supplemental metrics to conclude on the agency's overall cybersecurity posture in FY 2025. In rating each component of information security, the evaluator averages the results of the core metrics and the supplemental metrics for each of the six function areas covered in CSF 2.0 which are further divided into ten 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.

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[3]

Security Function	FY 2025 Assessed Maturity Level	FY 2024 Assessed Maturity Level
Govern	Level 4: *Managed and Measurable*	N/A (new function as of FY 2025)
Identify	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Protect	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Detect	Level 3: *Consistently Implemented*	Level 2: *Defined*
Respond	Level 4: *Managed and Measurable*	Level 4: *Managed and Measurable*
Recover	Level 3: *Consistently Implemented*	Level 3: *Consistently Implemented*
Overall Maturity	**Level 3: *Consistently Implemented***	**Level 3: *Consistently Implemented***

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

[3] Revisions to the FISMA scoring methodology can influence an organization's maturity compared to the previous year. These adjustments, along with annual variations in the scope of FISMA evaluations and updates to individual metric criteria or objectives, mean that maturity ratings should not be interpreted as directly comparable from one year to the next.

The SEC has made many improvements to its information security program since FY 2024. These include refining processes for approving and granting elevated access to portable storage devices; documenting a revised privileged user access provisioning process; creating a plan to improve the competencies of its cybersecurity workforce in a phased, multi-year effort; designing and implementing new baseline controls for agency systems based on NIST Special Publication (SP) 800-53, Revision 5; implementing endpoint detection and response and data loss prevention (DLP) tools; and developing a cybersecurity risk management strategy.

However, outstanding recommendations from prior-year FISMA evaluations continued to present risk to the agency during the period we evaluated. Specifically, the SEC faced challenges with regard to [redacted]; updating its Enterprise Risk Management Strategy document; enforcing recurring privileged user training requirements; performing business impact analyses using complete information; and comprehensively testing system recovery capabilities.

In addition, this year's evaluation team determined that the SEC is facing challenges in meeting ZTA compliance milestones, and the team was unable to complete full testing of seven metrics because requested information was not available within the required timeframe. These limitations appear linked to resource constraints and transitional adjustments within the SEC's Office of Information Technology (OIT) (e.g. staffing changes, contract modifications), which may increase operational risk.

The SEC OIG also engaged Sikich to conduct a series of technical tests, including a penetration test and a phishing test. Although we attempted to uncover exploitable weaknesses, we did not identify any vulnerabilities that a malicious third party could use to compromise internal systems or data from an external position. The external penetration test simulated an attack against internet-accessible SEC systems. The social engineering phishing test simulated a malicious third party attempting to manipulate SEC staff. Sikich used techniques such as phishing in an attempt to steal sensitive data that a malicious third party could use to gain unauthorized access to SEC systems. Based on the results of our social engineering phishing test, Sikich determined that some SEC employees did not consistently identify phishing attacks or report that they fell victim to an attack.

In addition, we also noted that prior-year issues related to [redacted] persisted for this evaluation period. However, with respect to the in-scope IG metrics, the evaluation team did not identify new control deficiencies or weaknesses warranting new recommendations.

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 F** and noted that management concurred with our recommendations. Sikich will evaluate corrective actions addressing current and prior-year recommendations in future FISMA evaluations.

The report below provides a detailed discussion of the findings, grouped by NIST CSF 2.0 function areas. **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. **Appendix D** contains items referred to as "Other Matters for Consideration," which represent potential areas for improvement that management is already aware of and monitoring. Should management's implementation of its existing policies, procedures, and processes in these areas mature, it would enhance the SEC's overall security posture. **Appendix E** contains a detailed summary of the evaluation team's penetration testing results.

Sikich CPA LLC

Alexandria, VA

February 25, 2026

FISMA Evaluation Findings

We organized our conclusions and ratings by function and domain to help orient the reader to deficiencies as categorized by the FISMA IG metrics and NIST CSF 2.0.

SECURITY FUNCTION: PROTECT

The objective of the Protect function is to support the safeguards used to manage the organization's cybersecurity risks, including limiting or containing the impact of a potential cybersecurity event.

Finding 1: Phishing campaign captured several employee credentials and revealed limited reporting of suspicious email.

FY 2025 IG FISMA Function: Protect / Domain: Security Training

Social engineering involves an attacker using human interaction to obtain information about an organization. Phishing is a form of social engineering in which bad actors posing as a credible person or legitimate organization attempt to gain access to sensitive information via email recipients, who are compelled to perform actions such as clicking links to fraudulent websites or downloading file attachments. Technological safeguards and email filters are not guaranteed to block all incoming malicious emails, leaving humans as an organization's last line of defense against phishing.

Sikich used social engineering to obtain employee account credentials by deploying a phishing campaign that targeted the email addresses of 993 SEC employees.[4] Sikich used a phishing campaign [redacted] to trick SEC users into providing credentials. An anti-phishing email filter that the SEC had in place blocked our initial phishing campaign emails, preventing users from visiting the malicious landing page. The SEC modified its email filter rules to allow access to the domain and whitelisted Sikich resources to enable the testing.[5] Once the SEC whitelisted our domain, we successfully transmitted the phishing emails to selected employee inboxes. The phishing campaign began on June 11 and concluded on June 13, 2025. Nine of the 993 employees entered login credentials (username and password) into the malicious landing page allowing Sikich to view these credentials in cleartext. Six additional employees clicked on the phishing link but did not enter login credentials. In total, about 1.5 percent of the employees included in the phishing campaign clicked on the phishing link.[6] Sikich promptly informed the SEC of captured credentials throughout the campaign.

SEC guidance states that users should report unexpected emails that contain an attachment, a hyperlink, or a call to action. The SEC stated that 71 out of 993 targeted employees reported Sikich's email as

[4] The SEC had 4,141 employees with email addresses at the time of testing. We tested a subset of the population.
[5] This is typical practice that is performed by the agency as part of its own phishing testing.
[6] The SEC conducted internal phishing campaigns in Q3 and Q4 of FY 2025, and experienced click rates of 2.0 percent and 3.4 percent, respectively.

phishing, for a report rate of about 7 percent.[7] However, only one of the nine users who entered login credentials subsequently reported the email.

If compromised during a real-world scenario, noncompliant employees could provide an attacker with access to SEC systems or applications, potentially enabling lateral movement across the agency's network, privilege escalation, and access to sensitive data.

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

We recommend that the Office of Information Technology:

1. Reset all identified compromised credentials, forcing password changes across all captured user accounts.
2. Update training for all employees on identifying and reporting suspected phishing emails, and establish a process to periodically remind employees of these responsibilities.

Management's Response: Management concurred with the recommendations and stated that agency staff took action in June 2025 to reset compromised credentials upon being notified by the evaluation team. Furthermore, Management stated that OIT will update training, issue reminders, and revise its rules of behavior guidance.

We have included Management's complete response in **Appendix F**.

Sikich's Evaluation of Management's Response: Management's proposed actions are responsive. Recommendation 1 is resolved and closed for reporting purposes. Recommendation 2 is resolved and will be closed upon completion and verification of the proposed actions.

Finding 2: The SEC has not [redacted] (Zero Trust Architecture – Data Pillar).

FY 2025 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 therefore 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 bad actors from removing the data without authorization.

The *FY 2025 IG FISMA Reporting Metrics* measure the extent to which an organization assigns data classifications to designated data types through tags or labels. Further, the CISA Zero Trust Maturity

[7] The SEC conducted internal phishing campaigns in Q3 and Q4 of FY 2025, and experienced report rates of 34.2 percent and 31.7 percent, respectively.

Model, Version 2.0, published April 2023, represents a gradient of implementation across five distinct pillars, in which organizations can make minor advancements toward optimizing zero trust maturity over time. In its discussion of the "Data" pillar, CISA guidance states that agencies should inventory, categorize, and label data; protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration. Further, it states that agencies should carefully craft and review data governance policies to ensure that they have appropriately enforced all data lifecycle security aspects across the enterprise.

In response to this guidance and Executive Order 14028,[8] on April 2, 2024, the SEC established internal requirements for its FISMA-reportable systems. Titled *Updated Planned Changes to SEC FISMA-Reportable Systems: Zero Trust Compliance,* these requirements included [redacted]

In FY 2024, we recommended that the SEC [redacted]

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

The evaluation team determined that it was not necessary to issue a recommendation due to the existing open recommendations.

[8] Executive Order 14028, *Improving the Nation's Cybersecurity*, published May 2021.

Appendix A – Background

During the peak of the Great Depression, Congress passed the Securities Act of 1933 (Securities Act)[9] and the Securities Exchange Act of 1934 (Securities Exchange Act),[10] 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),[11] 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 had 123 FISMA-reportable systems in place to support its mission during the period we evaluated. These systems are rated as low- and moderate-impact, and contractors operate more than one-third of them.

OIT is led by the SEC's Chief Information Officer and supports the SEC's mission and related strategic objectives by aligning its activities, missions, functions, and strategic goals 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 achieve the SEC's mission.

[9] See https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#secact1933 (last accessed on September 18, 2025) for more detail.
[10] See https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#secact1933 (last accessed on September 18, 2025) for more detail.
[11] See https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#df2010 (last accessed on September 18, 2025) for more detail.

FISMA Reporting Metrics

FISMA[12] 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 or oversee an annual evaluation of the effectiveness of the agency's information security program and practices and to report the results to OMB.

OMB,[13] CISA,[14] CIGIE,[15] 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 six function areas in NIST CSF 2.0 (Govern, Identify, Protect, Detect, Respond, and Recover), as shown in **Table 2** below. NIST CSF 2.0 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 2025 IG Metrics Function Areas and Domains

Function	Domain
Govern	Cybersecurity Governance
	Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset Management
Protect	Configuration Management
	Identity 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 IG metrics.

In FY 2025, 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. In addition to the 20 core metrics, each IG is also required to evaluate the 5 new supplemental metrics to conclude on the agency's overall cybersecurity posture in FY 2025. In rating each component of information security, the evaluator

[12] 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.
[13] OMB issues information security policies and guidelines for federal information resources pursuant to various statutory authorities.
[14] CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.
[15] 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.

averages the results of the core metrics and the supplemental metrics for each of the six function areas—Govern, Identify, Protect, Detect, Respond, and Recover—which are further divided into ten domains.

The IG 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: *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 2025 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 2025 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

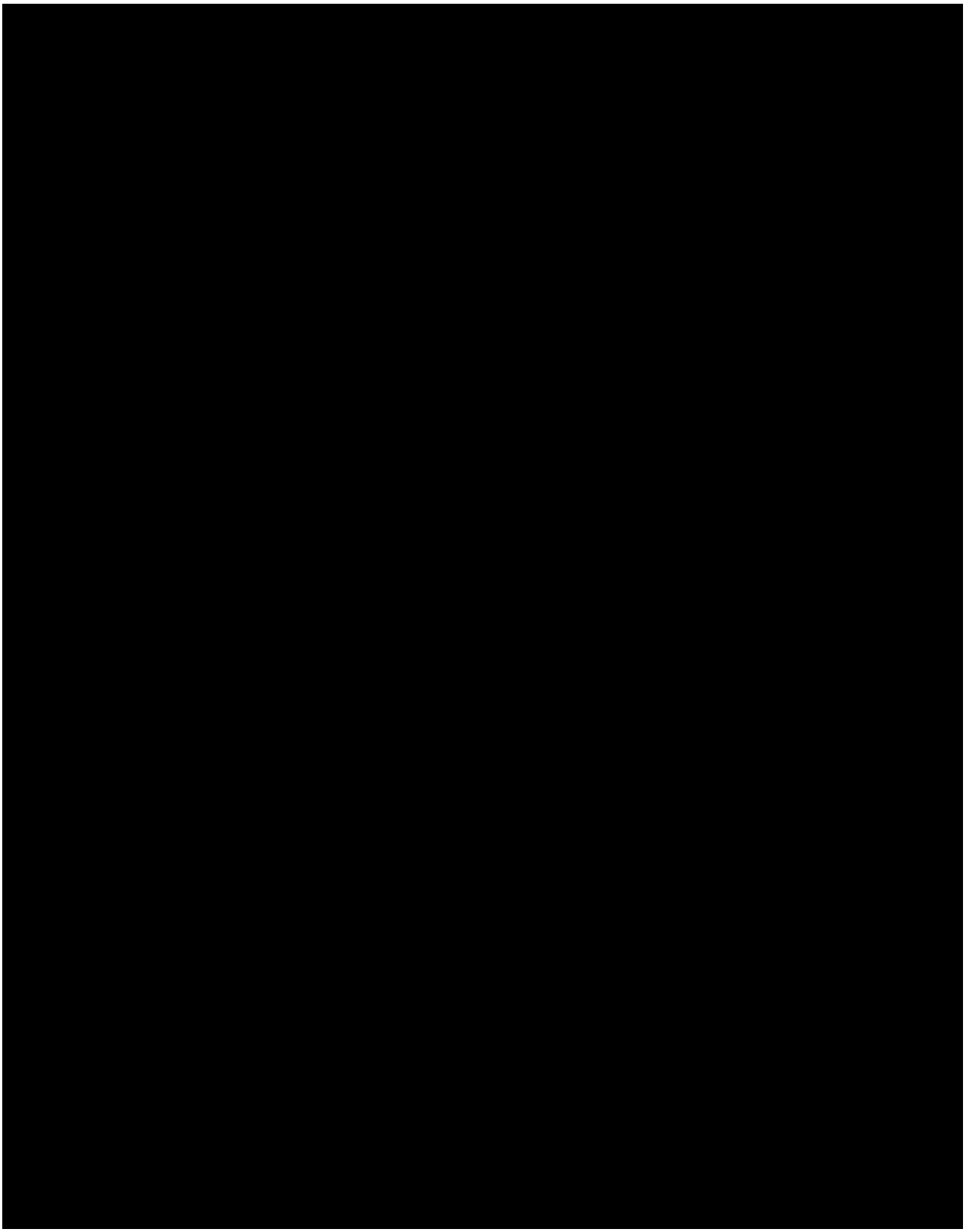
The evaluation covered the period between October 1, 2024, and May 30, 2025, and included assessing the effectiveness and maturity of the SEC's information security program, focusing on the 20 core metrics and 5 supplemental metrics spread across the 10 domains identified in the *FY 2025 IG FISMA Reporting Metrics*. Sikich judgmentally selected and reviewed a non-statistical sample of 8 of the SEC's 123 FISMA-reportable information systems[16]. This sample represents about 7 percent of the SEC's inventory of FISMA-reportable information systems. To select the sample, Sikich considered the following attributes:

- Systems that were not tested in the prior 3 years.
- Systems that the SEC categorized as "moderate" 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.

[redacted]

[16] This count of FISMA reportable systems was as of March 17, 2025.



[redacted]

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

Methodology

We conducted fieldwork for this evaluation from February to September 2025 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 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.
- 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 2025 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*[17]
- NIST SPs
- Department of Homeland Security Binding Operational Directives
- SECURE Technology Act[18]
- Federal Enterprise Architecture Framework, Version 2[19]

[17] 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 18, 2025).
[18] The SECURE Technology Act is publicly available. Please see https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf (last accessed on September 18, 2025).
[19] 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 September 18, 2025).

Sikich also followed up on all prior-year recommendations that were open at the start of the FY 2025 evaluation and that impacted 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 OIT's overall management control structure. Instead, Sikich reviewed OIT's Memorandum of Unmodified Statement Assurance. Based on our review, Sikich 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 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, OIT stated that internal controls over operations, reporting, and compliance were operating effectively through September 30, 2024.

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 a 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.

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 September 30, 2025, the SEC implemented corrective actions to close nine recommendations from prior-year FISMA evaluations in FY 2025. Although OIT addressed these recommendations, as noted in this report, areas requiring improvement still exist. **Appendix C** lists 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 2025, the SEC implemented corrective actions to close nine recommendations from prior-year FISMA evaluations. Another seven recommendations remain open, as depicted in **Table 5**. In addition, we identified two new recommendations for FY 2025, as discussed in this report.

Table 5. Recommendation Status

Domain	Recommendation	Prior Report and Recommendation Number	Status
Risk and Asset Management	Complete efforts to document and implement an enterprise-wide risk management strategy that incorporates the review and approval processes set forth in agency policy.	584-1	Open
Configuration Management	Implement the defined processes for [redacted]	574-6	Open
	Define and implement a process for tracking information technology security vulnerabilities identified through the Vulnerability Management Program using Enterprise Asset Management System tickets and, when appropriate (based on factors such as criticality and time elapsed since identification), Plans of Action and Milestones.	580-1	Closed as of December 10, 2024
	Develop and implement vulnerability disclosure-handling procedures that describe the SEC's process for implementing its VDP [Vulnerability Disclosure Policy], in accordance with Department of Homeland Security Binding Operational Directive 20-01.	580-3	Closed as of November 19, 2024
Identity and Access Management	Document the privileged user access provisioning process, including compensating controls and periodic enforcement reviews, to better ensure that the SEC grants privileged user access and system roles based on tickets, forms, or another method of formal approval and that the Office of Information Technology only grants users the correct level of access.	580-4	Closed as of June 5, 2025
Data Protection and Privacy	[redacted]	584-3	Open
	[redacted]	584-4	Open
	Implement a capability to assist in identifying and correcting endpoint detection and response coverage gaps.	584-5	Closed as of September 29, 2025*

Domain	Recommendation	Prior Report and Recommendation Number	Status
	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.	584-2	Closed as of March 31, 2025
Security Training	Develop and implement a mechanism to enforce recurring privileged user training for applicable personnel.	584-7	Open
	Develop a plan to address the findings of the cybersecurity competency study.	584-6	Closed as of June 25, 2025
Information Security Continuous Monitoring	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.	580-5	Closed as of September 30, 2025*
Incident Response	Develop and implement a log management process to: a. Ensure that the log management system ingests required logs categorized as Criticality Levels 0 through 2 in acceptable formats and that retention complies with the specified timeframes, in accordance with the technical details described in Office of Management and Budget Memorandum M-21-31, Appendix C. b. Implement a mechanism to detect instances in which the information systems are not sending the appropriate log data to the log management system and create a remediation plan to address these instances.	580-6	Closed as of September 29, 2025*
	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.	584-8	Closed as of July 2, 2025*
Contingency Planning	Update its business impact analysis template to ensure that the SEC assesses all systems using a correct and comprehensive set of mission-essential functions.	584-9	Open
	Incorporate assessments of system recovery time objectives into future disaster recovery exercises.	584-10	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 – Other Matters for Consideration

During the FY 2025 FISMA evaluation, Sikich observed that management had self-identified areas needing control optimization. The evaluation team concluded that these "Other Matters" would prevent the agency from attaining an "Optimized" maturity level. However, it was determined that issuing recommendations for these matters was unnecessary, as management was already tracking them internally and had achieved a "Managed and Measurable" maturity level for the related control areas due to existing complementary and compensating controls. They are noted here due to their relevance to federal priorities related to zero trust.

Other Matter #1: The SEC did not [redacted] (Zero Trust Architecture – Identity Pillar).

Service accounts are privileged accounts that provide elevated, often non-restricted access to underlying information systems and technology. As such, organizations should carefully control and monitor these accounts. Agencies use a privileged access management (PAM) service to monitor and control the use of privileged accounts.

The CISA Zero Trust Maturity Model, Version 2.0, "Identity" pillar states that agencies should integrate identity and access management solutions where possible throughout their enterprise to enforce strong authentication and grant tailored context-based authorization. The *FY 2025 IG FISMA Reporting Metrics* measure the extent to which organizations use automated mechanisms to manage privileged accounts centrally. Further, the SEC's internal requirements document for its FISMA-reportable systems, titled *Updated Planned Changes to SEC FISMA-Reportable Systems: Zero Trust Compliance,* states that the SEC must vault and manage service accounts through OIT's PAM service.

As of July 29, 2025, the SEC's FISMA-Reportable Systems Zero Trust Architecture Compliance dashboard showed that the agency did not [redacted]

Other Matter #2: The SEC has not [redacted] (Zero Trust Architecture – Network Pillar).

Agencies use mechanisms such as hypertext transfer protocol secure (HTTPS) and Domain Name Systems (DNS), along with Transport Layer Security (TLS) protocols, to protect data during electronic

dissemination across the internet and provide a secure channel for sending data (i.e. traffic) between a server and a client—typically, a web browser.

The CISA Zero Trust Maturity Model, Version 2.0, "Networks" pillar states that agencies should encrypt all applicable internal and external traffic. NIST SP 800-52, Rev. 2, *Guidelines for the Selection, Configuration, and Use of TLS Implementations*, states that agency servers shall support TLS 1.3 for "both government-only and citizen or business-facing applications by January 1, 2024." Further, the SEC's internal requirements document for its FISMA-reportable systems, titled *Updated Planned Changes to SEC FISMA-Reportable Systems: Zero Trust Compliance,* states that by September 30, 2024, all SEC systems that store and process SEC non-public information must encrypt transportation of HTTPS (using TLS 1.3 or higher), DNS communication (using DNS over TLS or DNS over HTTPS), and email transportation (using TLS 1.3 or higher).

[redacted]

Appendix E – Penetration Test Results Summary

The SEC OIG engaged Sikich to plan and conduct external penetration testing and vulnerability assessment services over the SEC's information technology assets and infrastructure (i.e., networks, systems, and applications) and to report any findings and potential mitigation strategies. We performed this testing—including planning, reconnaissance, vulnerability detection, exploitation, and reporting—using a methodology based on NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*[20], leveraging [redacted]

Sikich, the OIG, and OIT management developed an agreed-upon rules of engagement document that governed the terms of the testing, and Sikich's work was limited to the specific procedures and analyses described within this document.

External Penetration Testing

Sikich performed activities related to the external penetration tests between May 13 and June 13, 2025. Sikich attempted to discover and exploit system-, network-, and application-layer vulnerabilities using both automated and manual methods.

The external penetration test simulated an attack against SEC systems accessible from the Internet. Sikich used tools and techniques that emulated an external attacker, such as organized criminals or a nation-state, in an attempt to steal data from internet-facing systems or gain a foothold for access into server operating systems or internal networks. Sikich discovered web services and performed a thorough assessment of open ports and accessible interfaces. Specifically, we leveraged [redacted]

- [redacted]
  - [redacted]
- [redacted]
- [redacted]
  - [redacted]
- [redacted]
- [redacted]

Although we attempted to uncover exploitable weaknesses, we did not identify any vulnerabilities that a malicious third party could use to compromise internal systems or data from an external position.

[20] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (last accessed November 20, 2025)
[21] [redacted]

Social Engineering Phishing Testing

Sikich used social engineering to obtain employee account credentials by deploying a phishing campaign from June 11 to June 13, 2025 that targeted the email addresses of 993 SEC employees.[22] The social engineering phishing test simulated a malicious third party attempting to manipulate the SEC's staff. Sikich used a phishing campaign [redacted] to trick SEC users into providing credentials.

An anti-phishing email filter that the SEC had in place blocked our initial phishing campaign emails, preventing users from visiting the malicious landing page. The SEC modified its email filter rules to allow access to the domain and whitelisted Sikich resources to enable the testing. Once the SEC whitelisted our domain, we successfully transmitted the phishing emails to employee inboxes.

Nine employees entered login credentials into the malicious landing page; Sikich was able to view these credentials in cleartext. Six additional employees clicked on the phishing link but did not enter login credentials. In total, about 1.5 percent of the employees included in the phishing campaign clicked on the phishing link.

Sikich promptly informed the SEC of captured credentials throughout the campaign. We did not attempt to conduct attacks using account credentials captured during the phishing campaign, nor did we verify whether the credentials were valid.

[22] The SEC had 4,141 employees with email addresses at the time of testing.

Appendix F – Management Comments

U.S. Securities and Exchange Commission

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

From: Peter Gimbrere, Managing Executive, Office of the Chairman

PETER GIMBRERE Digitally signed by PETER GIMBRERE Date: 2026.02.18 13:55:39 -05'00'

Date: February 18, 2026

Subject: Management Response to Draft Office of Inspector General Report, *Fiscal Year 2025 Independent Evaluation of the U.S. Securities and Exchange Commission'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's (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) 2025. Please find enclosed our response and details of our planned actions.

The Report evaluates the SEC's information security program against the *FY 2025 Inspector General FISMA Reporting Metrics*, which measure maturity across six functional areas of the National Institute of Standards and Technology Cybersecurity Framework.[1]

We appreciate the recognition of progress in key areas such as data protection and privacy, identity and access management, continuous monitoring, and an effective rating in the cybersecurity governance domain in its first year of evaluation. These improvements reflect the Office of Information Technology's (OIT) commitment to advancing the maturity of the SEC's information security program and addressing evolving risks. Notably, the successful closure of nine prior-year recommendations demonstrates our ability to implement corrective actions effectively and sustain compliance with FISMA requirements.

Looking ahead, we remain focused on strengthening the Agency's security posture and aligning our program with federal standards and industry best practices. We concur with the Report's two recommendations and have prioritized their implementation as part of our broader strategy to enhance resilience and safeguard mission-critical information.

We appreciate the professionalism and collaboration demonstrated by the OIG and its contractor, Sikich, throughout this review. We support the timely completion of the corrective actions and will work with your office to confirm implementation.

cc: Jed Hickman, Acting Director and Chief Information Officer
Jeffrey King, Chief Information Security Officer and Senior Agency Official for Privacy
Shelly Luisi, Chief Risk Officer

Enclosure: Appendix A

[1] Office of Management and Budget, *FY 2025 Inspector General FISMA Reporting Metrics* v2.0 (Apr. 3, 2025), https://www.cisa.gov/sites/default/files/2025-04/Final_FY_2025_IG_FISMA_Reporting_Metrics_Ver_2.0_April_2025-508_0.pdf; National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* v1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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

The following are management's responses to the recommendations provided in the Report.

Recommendation 1: Reset all identified compromised credentials, forcing password changes across all captured user accounts.

Response: Concur. As noted in the Report, "nine of the 993 employees entered login credentials (username and password) into the malicious landing page allowing Sikich to view these credentials in cleartext." In June 2025, OIT immediately contacted the affected employees, informed them of the phishing campaign, and directed them to change their network passwords. Clear instructions were provided, and OIT received confirmation that all passwords were successfully reset.

To support closure of this recommendation, OIT submitted a report to the OIG verifying that all nine accounts had updated credentials as of June 2025. Additionally, logs from the SEC's Security Information and Event Management (SIEM) tool were provided to the OIG, further confirming the password changes.

Recommendation 2: Update training for all employees on identifying and reporting suspected phishing emails and establish a process to periodically remind employees of these responsibilities.

Response: Concur. OIT will update training, issue phishing awareness reminders, and revise the SEC's Technology Rules of Behavior. We will aim to complete this planned corrective action by December 2026.

OIG General Office Contact Information

EMPLOYEE SUGGESTION PROGRAM

The OIG SEC Employee Suggestion Program, established under the Dodd-Frank Wall Street Reform and Consumer Protection Act, welcomes suggestions by all SEC employees for improvements in the SEC's work efficiency, effectiveness, productivity, and use of resources. The OIG evaluates all suggestions received and forwards them to agency management for implementation, as appropriate. SEC employees may submit suggestions by calling the OIG Hotline at (833) SEC-OIG1 or by filing a complaint online as indicated below.

COMMENTS AND IDEAS

The SEC OIG also seeks ideas for possible future audits, evaluations, or reviews. We will focus on high-risk programs, operations, and areas where substantial economies and efficiencies can be achieved. Please send your input to AUDPlanning@sec.gov.

TO REPORT

fraud, waste, and abuse

Involving SEC programs, operations, employees, or contractors

FILE A COMPLAINT ONLINE AT

SEC OIG Hotline

CALL THE 24/7 TOLL-FREE OIG HOTLINE

833-SEC-OIG1