

REPORT NO. 585

MARCH 31, 2025

OFFICE OF
INSPECTOR
GENERAL

OFFICE OF AUDITS

Additional Oversight and Monitoring of the SEC's CAT Usage Is Needed

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

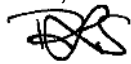


UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

M E M O R A N D U M

March 31, 2025

TO: Kenneth Johnson, Chief Operating Officer

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

SUBJECT: *Additional Oversight and Monitoring of the SEC's CAT Usage Is Needed,*
Report No. 585

Attached is the Office of Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) controls for safeguarding Consolidated Audit Trail (CAT) data within the SEC's environment. The report contains five recommendations to strengthen the SEC's oversight and monitoring of its CAT data usage and to define technical controls for tagging, tracking, and controlling CAT data already within the SEC's environment.

On March 7, 2025, we provided management with a draft of our report for review and comment. In its March 26, 2025, response, management concurred with our recommendations. We have included management's response as an Appendix III in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how management will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or Kelli Brown-Barnes, Audit Manager.

Attachment

cc: Mark T. Uyeda, Acting Chairman
Gabriel Eckstein, Chief of Staff, Office of Acting Chairman Uyeda
Peter Gimbrere, Managing Executive, Office of Acting Chairman Uyeda
Hester M. Peirce, Commissioner
Benjamin Vetter, Counsel, Office of Commissioner Peirce
Caroline A. Crenshaw, Commissioner
Malgorzata Spangenberg, Counsel, Office of Commissioner Crenshaw
Jeffrey Finnell, Acting General Counsel

Elizabeth McFadden, Deputy General Counsel General Litigation, Office of the
General Counsel
Stephanie Allen, Acting Director, Office of Public Affairs
Natalia Díez Riggín, Acting Director, Office of Legislative and Intergovernmental Affairs
Shelly Luisi, Chief Risk Officer
Jim Lloyd, Assistant Chief Risk Officer/Audit Coordinator, Office of the Chief Risk
Officer
Austin Gerig, Chief Data Officer
Oluwaseun Ajayi, Acting Chief Counsel, Office of the Chief Data Officer
David Bottom, Director/Chief Information Officer/Acting Chief Information Security
Officer, Office of Information Technology
Matthew Toscano, Assistant Director, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information
Technology
Deborah J. Jeffrey, Inspector General



EXECUTIVE SUMMARY

Additional Oversight and Monitoring of the SEC's CAT Usage Is Needed

REPORT NO. 585 | MARCH 31, 2025

WHY WE DID THIS AUDIT

The consolidated audit trail (CAT) tracks all activity in national market system securities throughout the U.S. markets. The CAT centralizes information about all orders throughout their life cycle and identifies the broker-dealers handling them. The U.S. Securities and Exchange Commission (SEC, agency, or Commission) does not own or operate the CAT, but authorized staff and contractors can access and share CAT data to perform a variety of regulatory functions. Inadequate safeguards would pose a greater risk to the Commission and/or outside parties and could hinder the agency's ability to meet its regulatory and oversight responsibilities.

We conducted this audit to assess whether the SEC's information security controls for safeguarding CAT data within the SEC's environment complied with key government-wide standards.

AGENCY'S RESPONSE

Management concurred with our five recommendations, which will be closed upon completion and verification of the proposed actions. This report contains non-public information about the SEC's protection of consolidated audit trail data. We redacted the non-public information to create this public version.

WHAT WE FOUND AND RECOMMENDED

The SEC implemented several Federal security controls to protect CAT data, along with additional policy-based safeguards that allow staff to access, download, and share CAT data as needed for their regulatory work.

However, the SEC did not: (1) implement measures to proactively detect and prevent the external release of CAT data; (2) [REDACTED] or (3) regularly monitor the policy-based safeguards to ensure user compliance.

During our audit, the risks of unauthorized disclosure and misuse of CAT data were elevated. Recent agency action has reduced these risks. For example, in September 2024 as part of its adoption of zero-trust cybersecurity principles, the SEC implemented automated safeguards for CAT data that prevent unauthorized external sharing of the data. Further, in February 2025, the Commission eliminated the requirement for the CAT to collect identifying information for U.S. natural person customers. We recommended additional steps to strengthen the SEC's oversight and monitoring of its CAT usage and to define the agency's new technical controls. These steps include:

- [REDACTED]
- Defining the scope, processes, and frequency for the SEC's periodic CAT data usage reviews to identify, analyze, and respond to risks related to the agency's access, use, extraction, and sharing of CAT data.
- Increasing the frequency of monitoring the SEC's user access lists to ensure only authorized users have access to CAT data, user access matches approved authorizations, and user access is disabled in a timely manner once access is no longer needed.
- [REDACTED]
- Finalizing responsibility for the SEC's regular monitoring of safeguards to [REDACTED]

We also discussed with agency management the availability of information needed to review SEC staff use of certain CAT transaction and customer data, which did not warrant recommendations.

Contents

Executive Summary	i
Introduction and Objective	1
Results	3
Finding. Additional Oversight and Monitoring of the SEC's CAT Usage Is Needed	3
Recommendations, Management's Response, and Evaluation of Management's Response	7
Other Matters of Interest	10
Appendices	11
Appendix I. Scope and Methodology	11
Appendix II. Background Information	15
Appendix III. Management Comments	18

Abbreviations

CAT	consolidated audit trail
FINRA	Financial Industry Regulatory Authority
FY	fiscal year
NIST	National Institute of Standards and Technology
OCDO	Office of the Chief Data Officer
OIG	Office of Inspector General
OIT	Office of Information Technology
SEC, agency, or Commission	U.S. Securities and Exchange Commission
SP	Special Publication

Introduction and Objective

INTRODUCTION

The consolidated audit trail (CAT) is the largest data repository of information regarding securities and options trading on U.S. exchanges. Centralizing this data allows the U.S. Securities and Exchange Commission (SEC, agency, or Commission) and its supervised entities to monitor national market system securities, identify and investigate market misconduct, and reconstruct disruptive or anomalous events.¹ The repository combines information about the lifecycle of a transaction in one place to enhance oversight, ensure the efficient functioning of markets, and boost investor confidence. The CAT was implemented in phases between July 2020 and July 2024 and is operated by an independent entity, known as FINRA CAT.²

The CAT contains two sets of data, stored separately:

1. Transaction data relating to orders, which conceals the identity of customers by using a unique anonymized identifier, and
2. Customer data, which links transactions to individual customers using an anonymized CAT customer ID number.^{3,4}

The SEC does not own or operate the CAT, but authorized staff and contractors can access and share CAT data on a need-to-know basis to perform a variety of regulatory functions. As of July 2024, 226 SEC users had access to the transaction data; 97 of those users could also access customer data. Authorized personnel include staff and contractors from the agency's divisions of Enforcement, Economic and Risk Analysis, Examinations, Investment Management, and Trading and Markets. The SEC categorized the CAT dataset at its highest risk level and added additional policy-based controls to govern the access, use, extraction, and internal sharing of CAT data.⁵

¹ In an anomalous event that became known as the "Flash Crash," on May 6, 2010, the prices of many U.S.-based equity products experienced a sudden breakdown of orderly trading. That afternoon, major equity indices in both futures and securities markets, each already down over four percent from their prior-day close, suddenly fell an additional five to six percent in a matter of minutes, only to rebound almost as quickly. Due in part to the lack of centralized trading data, the SEC required many months to issue a joint report with the Commodities Future Trading Commission regarding the causes of the Flash Crash. This, in turn, led to the plan to create the CAT. See Consolidated Audit Trail, 77 Fed. Reg. 45722, 45732-45733 (Aug. 1, 2012).

² FINRA CAT, LLC is a subsidiary of the Financial Industry Regulatory Authority (FINRA). SEC Rule 613 required the stock and options exchanges and FINRA to develop a plan to establish and maintain the CAT; ensure its accuracy, integrity, and security; and select an entity to build and operate the CAT. The CAT funding structure and annual operating cost estimates have generated controversy but are beyond the scope of this report.

³ Order Granting Conditional Exemptive Relief, 85 Fed. Reg. 16,152, 16,156-16,157 (Mar. 20, 2020); Order Approving the National Market System Plan Governing the Consolidated Audit Trail, 81 Fed. Reg. 84,696, 84,724-84,725, 84,767-84,768 (Nov. 23, 2016).

⁴ On February 10, 2025, the SEC granted exemptive relief to eliminate the requirement to report names, addresses, and years of birth of U.S. natural persons. SEC Press Release 2025-38 (February 10, 2025). Broker-dealers must still submit certain information for each order and when needed to identify individual customers, the SEC will request that the appropriate broker-dealer provide the customer's name, address, and/or year of birth. 90 Fed. Reg. 9642 (February 14, 2025).

⁵ The SEC categorizes datasets based on the risk to the agency or third parties should the dataset be compromised. Certain datasets that contain large volumes of sensitive information, such as CAT, are categorized as "High Datasets" and require heightened protection. SEC Administrative Regulation 2-1, *Dataset Access, Use and Internal Sharing Policy*; Section 5.1, August 5, 2022.

OBJECTIVE

The overall objective of this [audit](#) was to determine whether the SEC's information security controls for safeguarding CAT data within the SEC's environment complied with key government-wide standards. We focused on whether those controls complied with select requirements established in the National Institute of Standards and Technology's Special Publication 800-53 (NIST SP 800-53).⁶ We reviewed the SEC's processes and significant internal controls for securing, requesting access to, and extracting and sharing CAT data, and controls for logging and monitoring SEC user access between January 2023 and August 2024.

Appendix I of this report includes information about our scope and methodology, relevant internal controls, and prior coverage. Appendix II describes the SEC's use of CAT data, how the data is accessed and stored in the SEC's environment, and applicable Federal and SEC requirements, policies, procedures, and guidelines.

⁶ NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*; September 2020.

Results

FINDING. ADDITIONAL OVERSIGHT AND MONITORING OF THE SEC'S CAT USAGE IS NEEDED

The SEC implemented several NIST SP 800-53 security controls to protect CAT data along with additional policy-based safeguards that allow staff to access, download, and share CAT data as needed for their regulatory work. However, when facilitating broader use of CAT data within the SEC environment, the agency did not

- implement measures to proactively detect and prevent the external release of CAT data;
- [REDACTED] and
- regularly monitor the policy-based safeguards to ensure user compliance.

This occurred because of technical limitations and resource allocation decisions. Those decisions prioritized developing, testing, and deploying automated zero trust controls that could replace policy-based safeguards over developing a comprehensive formal monitoring regime for the policy-based safeguards themselves.⁷ According to the Office of the Chief Data Officer (OCDO), there was no evidence of unauthorized disclosures or misuse of CAT data by SEC or contractor staff during the period we reviewed. However, risks of unauthorized disclosure and misuse were elevated. In September 2024, the SEC implemented the automated zero trust controls for CAT data. In addition, in February 2025, the Commission granted exemptive relief to eliminate the requirement to collect U.S. natural person customers' identifying information. These actions reduced risks associated with unauthorized disclosure and misuse of CAT data by SEC users. As described further below, we recommend additional actions to strengthen the SEC's oversight and monitoring of its CAT usage and to define technical controls for [REDACTED]

A. The SEC Could Not Proactively Detect and Prevent the External Release of CAT Data

During the period we reviewed, the SEC could not proactively detect emails containing CAT data and prevent them from leaving the agency. According to SEC officials, they explored potential CAT-specific data loss prevention strategies but (1) those solutions were incompatible with the SEC's migration of its email to the cloud, and (2) there were insufficient unique identifiers in CAT data extracts. Ingesting CAT data without these protections increased the risk that a user could intentionally or unintentionally disclose

⁷ On January 26, 2022, the Office of Management and Budget issued *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09). M-22-09 directed all federal agencies to meet an initial set of zero trust standards by September 30, 2024. On December 1, 2022, SEC leadership directed staff to meet the M-22-09 standards for staff use and handling of CAT data by the September 30, 2024, deadline. The SEC designed the new CAT policy it adopted on January 20, 2023, to facilitate its development of zero trust security controls that would meet or exceed the M-22-09 standards by the September 30, 2024, deadline.

the data outside the SEC without authorization, and the agency would not be aware or be able to prevent the compromise. Not only is CAT data nonpublic,⁸ the agency categorizes it at the SEC's highest risk level, restricting where it can be

Officials explored but did not implement CAT-specific strategies to prevent data loss

stored, who can access it, and whether it can be extracted from a primary storage location and shared with others.⁹ For high-risk data, an effective data loss prevention strategy must include tools that monitor data at rest, in use, and in transit and can assist organizations in automating several NIST SP 800-53 security controls, including controls to prevent unauthorized disclosure.¹⁰

After our fieldwork ended, the SEC deployed automated controls in September 2024 and implemented a data labeling policy in October 2024 to enforce rules about sharing CAT data with external parties. Records labelled as containing internal market activity data are automatically blocked from leaving the agency unless the file owner or a designated official confirms that external sharing is authorized.¹¹ We are not making any recommendations regarding CAT data labeling at this time but will monitor the SEC's progress in this area.

B. The SEC

Government-wide information security standards require organizations to monitor for inappropriate or unusual activity that may indicate unauthorized access or misuse of confidential data.¹² Consistent with these standards, systems in which the SEC accessed and processed CAT data were monitored for unusual activity. The SEC accessed CAT data in the FINRA CAT repository and FINRA CAT's monitoring of this activity generated unusual activity alerts that were triaged by the SEC. In addition, SEC systems that stored, transmitted, or processed CAT data had automated unusual activity monitoring enabled.

The *SEC CAT Data Use and Handling Training*, which all SEC CAT data users must complete, expressly prohibits personal use of CAT data.

⁸ 5 C.F.R. § 2635.703(b) ("Nonpublic information is information that the employee gains by reason of Federal employment and that the employee knows or reasonably should know has not been made available to the general public."). SEC Administrative Regulation 23-2, *Safeguarding Nonpublic Information*, August 15, 2023, also defines "nonpublic information" as "information that Staff or a contractor gains by reason of Federal employment or a Federal contract and that has not been made available to the general public."

⁹ SEC Administrative Regulation 2-1, *Dataset Access, Use and Internal Sharing Policy*; August 5, 2022.

¹⁰ NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*; September 2011.

¹¹ *Consolidated Audit Trail Data Extraction Guidelines, Section 2.2.3 External Sharing*; October 4, 2024.

¹² NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*; September 2020.

13

OCDO's monitoring processes did not identify other fulfillment issues with CAT data access controls.¹⁷ For example, 28 of the 198 SEC users with access to CAT data in February 2024 had access that did not match their approved authorization form. This included users who requested and were authorized access to query CAT data using one technical mechanism (i.e., an SEC application) but were mistakenly not added to the group that would allow use of that application. OCDO was also unaware of problems with the process for removing user accounts from the group when access to CAT data was no longer needed. We identified six users who reported no longer requiring access to CAT data in October 2023 but still had access in early 2024.¹⁸

These issues occurred because one individual had responsibility for fulfilling and removing access to CAT data and OCDO did not systemically monitor the fulfillment process. During our audit, OCDO transferred account management responsibilities to a team within the SEC's Office of Information Technology (OIT). In addition, OCDO increased the frequency of access reviews. Ensuring that only authorized individuals with an ongoing business need have access to CAT data and that user access is timely removed when no longer needed will reduce the risk of unauthorized access to CAT data.

OCDO Did Not Conduct Regular Reviews to Ensure Users Followed CAT Data Extraction

Guidelines. To manage CAT data extractions, the SEC established policy-based restrictions that relied on users' compliance. The SEC created a formal CAT use and handling training to familiarize users with the policy-based restrictions and encourage compliance but did not conduct regular monitoring to assess compliance. [REDACTED]

[REDACTED]¹⁹

- SEC users were only allowed to extract CAT data files that were smaller than [REDACTED].²⁰ Yet on four occasions one system administrator and two users were able to extract more than [REDACTED]
[REDACTED]
[REDACTED]
- The SEC's CAT extraction guidelines stipulated that users must first download CAT data files from the repository to the SEC's [REDACTED] before moving them to other locations or sharing them with other users. [REDACTED]
[REDACTED]
[REDACTED] Although the agency implemented this process, [REDACTED]
[REDACTED]
[REDACTED] more than half the time (126 of

¹⁷ The 24 unapproved users did not complete necessary steps, such as submitting a user access request form, before being given access to CAT data. Once they were identified, OCDO directed them to either request access to the data or notify OCDO that they no longer required access. Half of the 24 individuals completed the access request process and the other half stated that they no longer required access.

¹⁸ All six users still had access in February 2024 and five of the six users still had access in April 2024.

¹⁹ The SEC did review fiscal year user extraction activities during its annual usage review and noted the first example we cite. However, the agency's review was not timely because of contracting issues.

²⁰ *Consolidated Audit Trail Data Extraction Guidelines*; January 20, 2023.

248 file extractions in FY 2023). While the files remained secure within the SEC's network,

Overall, more narrowly tailored, timely, and frequent monitoring would have alerted OCDO that users were not always following the SEC's CAT data guidelines, allowing for prompt corrective action. The Chief Data Officer expects

More frequent monitoring would allow OCDO to more promptly address noncompliant users

will evolve as the SEC executes its *FY23-FY24 Zero Trust Strategy and Implementation Plan* for addressing the Office of Management and Budget's federal zero trust requirements.²¹

While we are encouraged by the agency's plans and recent actions, the SEC has not

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

To better protect CAT data within the SEC's environment, we recommend that OCDO:

Recommendation 1:

Management's Response. Management concurred with the recommendation. According to the Chief Data Officer, , the Office of the Chief Data Officer will

Management's complete response is reprinted in Appendix III.

OIG'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.

²¹ Office of Management and Budget M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*; January 26, 2022.

Recommendation 2:

Define the scope, processes, and frequency for the SEC's periodic CAT data usage reviews to identify, analyze, and respond to risks related to the agency's access, use, extraction, and sharing of CAT data.

Management's Response. Management concurred with the recommendation. According to the Chief Data Officer, the Office of the Chief Data Officer has defined the scope, processes, and frequency for the SEC's periodic CAT data usage reviews and will provide evidence of the actions taken. Management's complete response is reprinted in Appendix III.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive. The recommendation will be closed upon verification of the proposed actions.

Recommendation 3:

Increase the frequency of monitoring the SEC's user access lists to ensure only authorized users have access to CAT data, user access matches approved authorizations, and user access is disabled in a timely manner once access is no longer needed.

Management's Response. Management concurred with the recommendation. According to the Chief Data Officer, the Office of the Chief Data Officer [REDACTED] and will provide evidence of the actions taken. Management's complete response is reprinted in Appendix III.

OIG'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.

Recommendation 4:

[REDACTED]

Management's Response. Management concurred with the recommendation. According to the Chief Data Officer, the Office of Information Technology and Office of the Chief Data Officer will [REDACTED] Management's complete response is reprinted in Appendix III.

OIG'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.

Recommendation 5:

Finalize responsibility for the SEC's regular monitoring of safeguards to [REDACTED]

Management's Response. Management concurred with the recommendation. According to the Chief Data Officer, the Office of Information Technology and Office of the Chief Data Officer have [REDACTED]

[REDACTED]

[REDACTED] Management's complete response is reprinted in Appendix III.

OIG'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.

Other Matter of Interest

During our audit, we requested information that would show the SEC's use of CAT transaction and customer data accessed through FINRA CAT applications. [REDACTED]

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

Additionally, the SEC requested that FINRA provide a direct data feed for the transaction data logs that are available [REDACTED]

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

Although we are not making recommendations related to these matters at this time, we presented these matters to OCDO management for their consideration.

Appendix I. Scope and Methodology

We conducted this performance audit from May 2023 to March 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Objective and Scope

Our objective was to determine whether the SEC's information security controls for safeguarding CAT data within the SEC's environment complied with key government-wide standards. We focused on whether those controls complied with select requirements established in NIST SP 800-53. Our audit included the SEC's processes and significant internal controls (including policies and procedures) for securing, requesting access to, and extracting and sharing CAT data, and controls for logging and monitoring SEC user access between January 2023 and August 2024. We did not review controls related to the security of the FINRA CAT Data Repository or FINRA CAT applications.

Methodology

To address our objective, we conducted fieldwork at the SEC's Headquarters in Washington, DC, and met with SEC staff from multiple divisions and offices, including OCDO, OIT, CAT dataset approvers, and personnel from the SEC divisions that use CAT data. We also reviewed:

- applicable federal laws, regulations, and guidance; SEC policies and procedures; the Division of Enforcement's policy related to CAT data; and the Division of Examinations' guide related to nonpublic information;
- cryptographic protection mechanisms for SEC information systems that store or transmit CAT data;
- the process for requesting access to query CAT data;
- mechanisms to limit CAT data extraction and sharing;
- log files to determine whether users followed the SEC's *CAT Data Extraction Guidelines*;
- OCDO plans for monitoring CAT data use and extractions; and
- CAT user incident response procedures.

We also tested the CAT data user list for the period we reviewed to ensure all users had an approved authorization request and that the access granted matched their approved authorization. Finally, we observed pilot testing of data labeling and the configuration of a secure download location that was planned for September 2024 and was implemented the following month.

Internal Controls

We identified and assessed internal controls, applicable internal control components, and underlying principles significant to our objective, as described below.

Control Environment. We assessed the control environment established by OCDO and OIT senior management. We reviewed OCDO's and OIT's organizational structure and interviewed staff responsible for reviewing and maintaining the organizations' internal control documentation. We also met with those responsible for implementing safeguards over CAT data, including the SEC's Chief Information Officer, Chief Information Security Officer, and Chief Data Officer.

Risk Assessment. We obtained and reviewed the management assurance statements for the SEC divisions that use CAT data, as well as the Division of Investment Management, OCDO, OIT, and the Office of the Investor Advocate. We also obtained and reviewed OIT's and OCDO's risk control matrices for FY 2022 and FY 2023 to identify risks and controls related to the security of CAT data. We assessed risks identified by OIT and OCDO and reviewed the security categorization worksheet and privacy analysis worksheet for the SEC CAT application. We also reviewed system security plans, security assessment reports, and authorizations to operate for six SEC systems.

Control Activities. We identified and reviewed control activities related to our objective, and we interviewed OIT and OCDO representatives and tested key internal controls for encryption, user training, user access, and access logs and monitoring. We also tested key internal controls established in SEC policy, including the *Dataset Access, Use, and Internal Sharing Policy*, *CAT Standard Operating Procedures*, and *CAT Data Extraction Guidelines*. As this report describes, we determined that additional safeguards are needed to protect CAT data within the SEC's environment.

Information and Communication. OIT is responsible for managing the SEC's information technology program including security. OIT communicates with its workforce policies and procedures related to the information technology program and safeguarding nonpublic information through its internal web site and memoranda from the Chief Information Officer. As the steward for the CAT dataset, OCDO is authorized to define relevant standard operating procedures. OCDO communicates through its internal web sites about procedures, guidance, and training related to CAT data.

Monitoring. We reviewed the SEC's *CAT Standard Operating Procedures* and *CAT Data Extraction Guidelines* and met with OCDO personnel responsible for conducting periodic CAT data usage reviews. Overall, the agency established several safeguards around user access, user training, encryption, and incident reporting that complied with the NIST controls we tested. We did not identify any incidents during the period we reviewed that resulted in the loss of CAT data. However, as this report describes, we identified opportunities to improve monitoring compliance with the *CAT Data Extraction Guidelines*.

Data Reliability

The U.S. Government Accountability Office's *Assessing Data Reliability* (GAO-20-283G, December 2019) states reliability of data means that data are applicable for audit purpose and are sufficiently complete and accurate. Data primarily pertains to information that is entered, processed, or maintained in a data

system and is generally organized in, or derived from, structured computer files. Furthermore, GAO-20-283G defines “applicability for audit purpose,” “completeness,” and “accuracy” as follows:

“Applicability for audit purpose” refers to whether the data, as collected, are valid measures of the underlying concepts being addressed in the audit’s research objectives.

“Completeness” refers to the extent to which relevant data records and fields are present and sufficiently populated.

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

To address our objective, we relied on computer-processed data from the SEC’s access request tool, encryption reports, extraction and download audit logs, and training records. To assess the reliability of this data, we:

- Interviewed knowledgeable OCDO and OIT personnel, including the access request tool point of contact, information technology specialists for workstation encryption, and OCDO staff responsible for monitoring audit logs.
- Reviewed the parameters used to obtain data reports such as the user access authorization list and training completion records; observed OIT personnel generate the encryption reports; and reviewed the data reports provided during the audit to test for missing, duplicative, or irregular data or values.
- Performed walkthroughs of the access request process and encryption report tool.

Based on our assessment, we found the data sufficiently reliable for the purpose of this audit

Prior Coverage

Between 2017 and 2024, the SEC Office of Inspector General (OIG) issued the following reports and management letter of particular relevance to this audit, which are accessible at <https://www.sec.gov/oig>:

- *Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546; March 30, 2018).
- *Fiscal Year 2018 Independent Evaluation of SEC’s Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 552; December 17, 2018).
- *The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services* (Report No. 556; November 7, 2019).
- *Fiscal Year 2019 Independent Evaluation of SEC’s Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 558; December 18, 2019).
- *Fiscal Year 2020 Independent Evaluation of SEC’s Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 563; December 21, 2020).
- *Fiscal Year 2021 Independent Evaluation of the SEC’s Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 570; December 21, 2021).

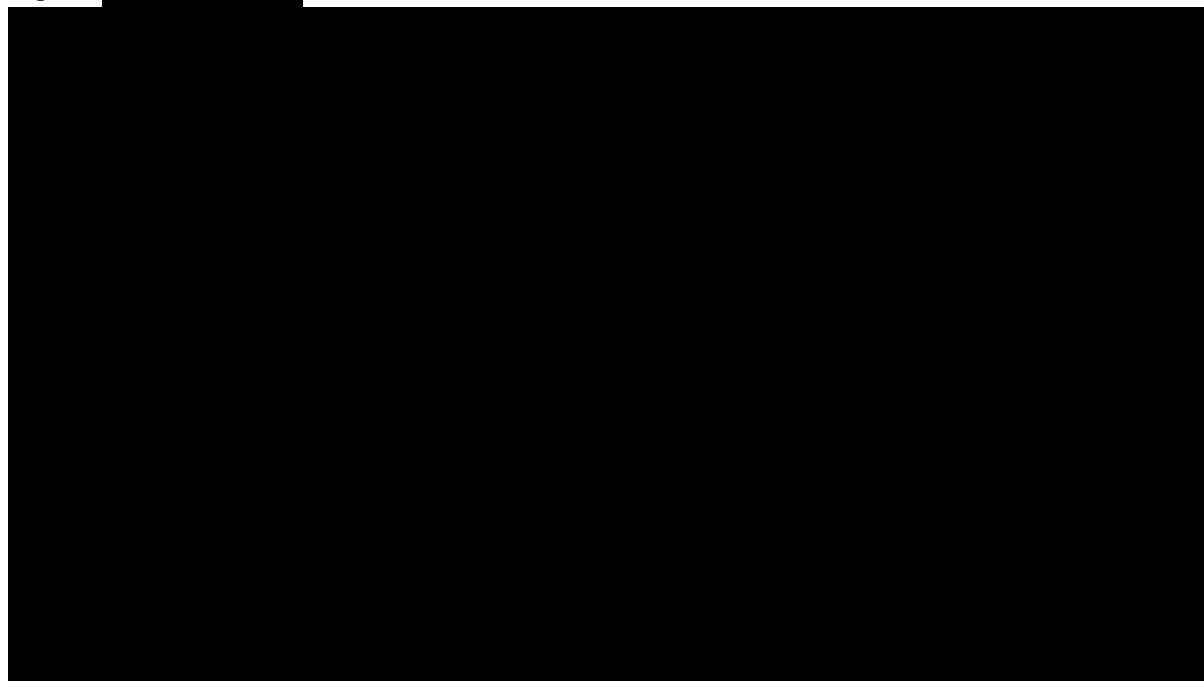
- *Fiscal Year 2022 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 574; November 15, 2022).
- *Final Management Letter: Readiness Review – The SEC's Progress Toward Implementing Zero Trust Cybersecurity Principles* (September 27, 2023).
- *Fiscal Year 2023 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 580; December 20, 2023).
- *Fiscal Year 2024 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 584; November 25, 2024).

Appendix II. Background Information

SEC Use of CAT Data. In December 2022, the SEC reported that the Enforcement Division’s Market Abuse Unit—with assistance from the Unit’s Analysis and Detection Center and the Division of Economic and Risk Analysis—used CAT data to uncover allegedly fraudulent trading and determine how two individuals profited from a multi-year front-running scheme.²³ Additionally, in September 2023, the SEC Chair stated that, “. . . with respect to the Commission, CAT data was beneficial for our staff’s GameStop report from 2021, for our analysis of insider trading, as well as for a number of the Commission’s proposed rulemakings.”²⁴ According to agency personnel, the SEC has also used CAT data to assist in examinations and risk assessments.

As the following figure shows, SEC users use FINRA or SEC CAT applications to query or analyze data from the FINRA CAT Data Repository. While FINRA is responsible for protecting and managing FINRA’s resources, the SEC is responsible for protecting the data within its environment. This includes an SEC [REDACTED], SEC CAT applications, [REDACTED], and other file storage locations such as user workstations and network drives.

Figure. [REDACTED] Access, Extract, and Store CAT Data Within the SEC Environment



²³ See U.S. Securities and Exchange Commission, *SEC Charges Financial Services Professional and Associate in \$47 Million Front-Running Scheme*, Press Release 2022-228. In a parallel action, the U.S. Attorney’s Office for the Southern District of New York announced criminal charges against the two individuals. In May 2024, one of the individuals was sentenced in U.S. District Court to 70 months in prison and to three years of supervised release. He was also ordered to pay forfeiture of \$12,249,000. See U.S. Attorney’s Office for the Southern District of New York, *Former Insider At TIAA-CREF Sentenced To 70 Months In Prison For Involvement In Multimillion-Dollar Insider Trading Ring*, Press Release 24-177.

²⁴ SEC Chair Gary Gensler, *Statement on CAT Funding*; September 6, 2023.

Applicable Federal Requirements. Federal agencies must meet minimum security requirements to protect the confidentiality, integrity, and availability of federal information systems and the information they process, store, and transmit.²⁵ Agencies meet these requirements by selecting and implementing appropriate security controls to protect information and manage information security risk, as described in NIST SP 800-53. The SEC's *Information Security and Privacy Controls Manual* documents the agency's information security policy framework in accordance with these minimum federal requirements.

In 2022, the Office of Management and Budget issued new guidance directing Federal agencies to implement a zero-trust framework to secure their data and information systems.²⁶ The SEC then developed its *FY23-FY24 Zero Trust Strategy and Implementation Plan*. In September 2023, we reported that, while the SEC developed and defined data categories, it did not include a goal for monitoring and restricting sensitive electronic documents.²⁷ After our fieldwork for this audit ended, in September 2024 the SEC implemented the initial phase of [REDACTED]

SEC Roles and Responsibilities. Within the SEC, OIT supports the Commission and agency staff in all aspects of information technology and has overall management responsibility for the Commission's information technology program. Next, OCDO ensures the SEC collects only the data it needs and can effectively secure, and is responsible for administering the agency's data policies, reviewing logs, generating data audit reports, and monitoring for compliance. Last, SEC users are expected to follow all enterprise, division, and/or office data policies and procedures, and must annually complete certain training.

SEC CAT Data Policies, Procedures, and Guidelines. The SEC's initial CAT data usage policy significantly restricted staff's ability to access and share the data.²⁸ While the policy allowed authorized users to share the data via phone or video conferencing, it prohibited users from extracting the data and sharing it more broadly.²⁹ Some divisions and offices reported that the restrictions impaired staff's ability to use CAT data in support of the agency's mission. In response, OCDO proposed a new governance structure to facilitate more access, use, and sharing of the data. The SEC Chair approved new CAT procedures and guidelines that went into effect in January 2023 and allowed for more sharing of CAT data amongst agency staff and across the agency's environment.³⁰ Management designed the following safeguards to address the risks that fewer restrictions might create:

²⁵ Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*; March 9, 2006.

²⁶ Office of Management and Budget M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*; January 26, 2022.

²⁷ U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC's Progress Toward Implementing Zero Trust Cybersecurity Principles*; September 27, 2023; pg. 6.

²⁸ *Interim Policies and Procedures for Access to the Consolidated Audit Trail System and Use of CAT Data*, Version 2.0; March 4, 2022.

²⁹ Any other mechanism for sharing the data was prohibited unless the SEC Chief Operating Officer (or designee) granted an exception.

³⁰ *Consolidated Audit Trail Standard Operating Procedures*, January 20, 2023, and *Consolidated Audit Trail Data Extraction Guidelines*, January 20, 2023.

- Access to CAT data in its primary storage locations was limited to only those staff and contractors whose work duties required it.³¹
- The file size for CAT data exported from FINRA or SEC applications was limited to [REDACTED], and [REDACTED]^{32,33}
- The transmission of CAT data and locations where CAT data is or may be stored within the SEC's environment were encrypted.³⁴
- An incident reporting process was added to respond to security events related to CAT data.³⁵

In addition to these CAT-specific policies, procedures, and guidelines, an SEC administrative regulation governs the risk-based approach used to ensure the security of the agency's datasets.³⁶

³¹ To access CAT data in these locations, users must complete use and handling training, submit a user access request and justification, and receive approval from their supervisor and a data officer or senior officer in their division or office. This process for establishing accounts complied with NIST SP 800-53, Control AC-2.

³² This file size limit was based on the risk of unauthorized disclosure of the anonymized data. Also, desktop applications that staff use to analyze data generally cannot process more than [REDACTED]

³³ The *Consolidated Audit Trail Data Extraction Guidelines* designated the SEC's [REDACTED] for CAT [REDACTED]

³⁴ Encryption of data in transit and at rest complied with NIST SP 800-53, Controls SC-8 and SC-28.

³⁵ The incident reporting process complied with NIST SP 800-53, Control IR-6. OCDO was not aware of any reports of unauthorized disclosures of CAT data during the period we reviewed and, during our audit, there were no reports of security incidents related to CAT data in the SEC's security incident reporting system. As a result, we were unable to test the effectiveness of the incident reporting process.

³⁶ SEC Administrative Regulation 2-1, *Dataset Access, Use, and Internal Sharing Policy*; August 5, 2022.

Appendix III. 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: Austin Gerig, Chief Data Officer **AUSTIN GERIG**

Date: March 26, 2025

Subject: Management Response to *Additional Oversight and Monitoring of the SEC's CAT Usage Is Needed*

Digitally signed by
AUSTIN GERIG
Date: 2025.03.26
14:10:23 -04'00'

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG)'s draft report of the OIG's audit to assess the SEC's information security controls for safeguarding Consolidated Audit Trail (CAT) data within the agency's environment. The dates of the audit, and its associated findings, covered a period of transition for data security within the SEC. During this time, the agency established policy-based data security controls, over and above federal requirements, that controlled the access, use, and sharing of data across system boundaries, including CAT data. These policy controls were aligned with anticipated zero trust cybersecurity principles defined by the Office of Management and Budget (OMB) in January 2022, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (M-22-09). In M-22-09, OMB set September 30th, 2024 as the initial deadline for agencies to demonstrate progress toward meeting the zero trust principles, and the SEC prioritized developing, testing, and deploying automated zero trust controls that could replace the policy-based safeguards by that date.

I am pleased that your draft report confirmed the SEC's rollout of automated zero trust controls in September 2024, after the OIG's review period, and that these controls strengthened the agency's protection of CAT data. I am proud of the collaboration between my office and other groups in the SEC that enabled the SEC to meet the September deadline set by OMB, and that the automated zero trust controls we deployed exceeded the degree of progress that OMB required agencies to meet by that date. The ability of the SEC to automatically tag and control extractions of CAT data is unique within the federal government, and it is a big achievement. As outlined below, CAT data handled by the SEC were at all times protected by a wide range of safeguards meeting the requirements of NIST SP 800-53 and a system of internal control meeting the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* (the "Standards for Internal Control" or "Standards").



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

The draft report discusses the SEC's email safety practices during OIG's review period. Under Commission authorization and to accomplish regulatory objectives, members of the SEC staff often share nonpublic data with law enforcement partners, other regulators, regulated entities and others securely by email. [REDACTED]

[REDACTED] met the standards of NIST SP 800-53. This process continued until the [REDACTED] was replaced by the SEC's successful implementation of zero trust labeling and label-based email controls for CAT data in September 2024.

As the draft report states, the SEC implemented system controls where CAT data was located that met NIST SP 800-53 requirements for the monitoring of unusual activity. OCDO performed a [REDACTED] of user access, which discovered compliance issues that were immediately elevated within the SEC for resolution. The root cause of these issues has been resolved, and OCDO now has increased the frequency of user reviews to [REDACTED]. To monitor other areas of the CAT policy, and consistent with the Standards for Internal Control, OCDO prioritized monitoring of compliance with key policy requirements such as those regarding [REDACTED] while at the same time investing in the automation of controls, which was ultimately completed in September 2024. As the draft report notes, OCDO's periodic CAT usage review was delayed due to a work stoppage on a contract. This delay did not affect [REDACTED] monitoring, including the detection of unusual query activity, malicious activity, and unusual access attempts.

In addition, once the SEC approved CAT policy guidelines and procedures in January 2023, OCDO developed a dedicated training program that both current and prospective CAT users were required to complete. After completing the training, prospective users were also required to submit CAT access requests for approval by their supervisor and a designated second approver in their division. OCDO's approach provided reasonable assurance that CAT data would be both protected and effectively used in support of the SEC's mission.

Your report recommends additional steps to further protect CAT data. We concur with all recommendations and have implemented or will implement the recommendations by April 2025.

Attachment: Appendix 1: Management Responses to Recommendations



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

Appendix 1: Management Responses to Recommendations

Please find below the Office of the Chief Data Officer's management response to each recommendation:

Recommendation 1: [REDACTED]

Response: We concur. The Office of the Chief Data Officer will [REDACTED]

Recommendation 2: Define the scope, processes, and frequency for the SEC's periodic CAT data usage reviews to identify, analyze, and respond to risks related to the agency's access, use, extraction, and sharing of CAT data.

Response: We concur. The Office of the Chief Data Officer has defined the scope, processes, and frequency for the SEC's periodic CAT data usage reviews. The Office is preparing a closure package evidencing the actions taken, to request closure of this recommendation.

Recommendation 3: Increase the frequency of monitoring the SEC's user access lists to ensure only authorized users have access to CAT data, user access matches approved authorizations, and user access is disabled in a timely manner once access is no longer needed.

Response: We concur. The Office of the Chief Data Officer [REDACTED]
[REDACTED] The Office is preparing a closure package evidencing the actions taken, to request closure of this recommendation.

Recommendation 4: [REDACTED]

Response: We concur. The Office of Information Technology and the Office of the Chief Data Officer will [REDACTED]



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

Recommendation 5: Finalize responsibility for the SEC's regular monitoring of safeguards to

[REDACTED]

Response: We concur. The Office of Information Technology and the Office of the Chief Data Officer have

[REDACTED]

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov.

TO REPORT

fraud, waste, and abuse

Involving SEC programs, operations, employees,
or contractors

FILE A COMPLAINT ONLINE AT

www.sec.gov/oig



CALL THE 24/7 TOLL-FREE OIG HOTLINE

833-SEC-OIG1

