U.S. SECURITIES AND EXCHANGE COMMISSION

REPORT NO. 593

NOVEMBER 23, 2026

OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

Improvements Needed in the SEC's Change Control Process

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

REDACTED FOR PUBLIC RELEASE

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

November 23, 2026

TO: Paul Knight, Chief Operating Officer

FROM: Kevin B. Muhlendorf, Inspector General KEVIN MUHLENDORF Digitally signed by KEVIN MUHLENDORF Date: 2026.11.23 08:44:34 -05'00'

SUBJECT: *Improvements Needed in the SEC's Change Control Process*, Report No. 593

Attached is the Office of Inspector General final report detailing the results of our audit of the U.S. Securities and Exchange Commission's change control process. The report contains 14 recommendations that should further strengthen the agency's change control process.

On September 16, 2026, we provided management with a draft of our report for review and comment. In its October 22, 2026, response, management fully concurred with 10 of our 14 recommendations, partially concurred with 2 recommendations, and nonconcurred with 2 recommendations. We consider recommendations 3, 7, 8, 10, and 11 open and unresolved. We have included management's response as Appendix II in the final report.

We appreciate the courtesies and cooperation extended to us during the audit. 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
Taylor Asher, Deputy Chief of Staff - Operations, Office of Chairman Atkins
Mark T. Uyeda, Commissioner
Ivan 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, Chief External Affairs Officer and Director, Office of Public Affairs
Graham Conlan, Director and Counsel to the Chairman, Office of Legislative and Intergovernmental Affairs
Ada Fernandez Johnson, Senior Counsel, Office of the Chief Operating Officer
Shelly Luisi, Chief Risk Officer
Jim Lloyd, Assistant Chief Risk Officer/Audit Coordinator, Office of the Chief Risk Officer
Olivier Girod, Director, Office of Support Operations
Jed Hickman, Acting Chief Information Officer and Director, EDGAR Business Office
Bridget Hilal, Branch Chief, Cyber Risk and Governance, Office of Information Technology

EXECUTIVE SUMMARY

Improvements Needed in the SEC's Change Control Process

REPORT NO. 593 | NOVEMBER 23, 2026

WHY WE DID THIS AUDIT

System integrity is maintained by controlling changes to established baselines. System changes that should be controlled include software updates, maintenance, development, and patches. The U.S. Securities and Exchange Commission's (SEC or agency) change control process is designed to ensure, among other things, that changes to SEC systems are adequately described, reasons for changes are documented, testing is conducted and impacts are assessed before changes are implemented, and those impacted approve of the changes to be made.

We conducted this audit to assess the SEC Office of Information Technology's (OIT) process for managing changes to the SEC's operational environment to prevent unintended consequences that can affect the performance and security of SEC systems and data. Specifically, we sought to determine whether OIT adequately defined and consistently implemented a change control process, to include appropriate testing of changes before deployment and regular monitoring for unapproved system changes.

AGENCY'S RESPONSE

Management concurred with 10 of our recommendations, partially concurred with 2, and nonconcurred with 2. Nine recommendations are resolved and will be closed upon verification of the actions taken and five are unresolved. Management's complete response is reprinted in Appendix II.

This report contains non-public information about the SEC's information technology program. We redacted the non-public information to create this public version.

WHAT WE FOUND AND RECOMMENDED

OIT developed change control policies and procedures and established change control boards (CCBs) to systematically manage changes through proper review, evaluation, and approval. We reviewed a judgmental sample of SEC information systems that underwent changes during calendar year 2024 as well as samples of change requests and identified several areas where improvements could be made to strengthen the SEC's change control process.

First, OIT did not [redacted]

Second, although emergency changes by their nature are the riskiest change type, the agency's CCBs did not retroactively review and approve these changes, as required. This may have allowed unanticipated issues to persist longer than necessary, resulting in greater security impacts and/or reputational harm.

Third, agency and contractor personnel inconsistently implemented the SEC's change control process. Our analysis identified incorrect classifications of emergency changes, missing or inadequate root cause analyses, untimely closure of change requests, [redacted] These inconsistencies may have introduced security risks, led to disruptions or delays in needed functionality, and made it harder to troubleshoot issues.

Fourth, change control procedures did not fully define requirements for testing information presented to the CCBs or included in change requests. As a result, CCBs were provided inconsistent information, which increased the likelihood that changes were made to the SEC's production environment without adequate testing and raised the potential for unintended consequences affecting the performance and security of agency systems and data.

Fifth, CCBs lacked predefined evaluation criteria, which limited their ability to ensure that each proposed and implemented change was evaluated in a consistent and repeatable manner, balancing security, business, and technical viewpoints.

Sixth, the SEC's enterprise change control tool did not effectively maintain records or ensure that unique unambiguous configuration item identifiers were used, potentially resulting in an inaccurate and/or unverifiable portrait of the agency's production environment. If left unaddressed, this could impact federal records management compliance and troubleshooting efforts.

We made 14 recommendations to further strengthen the SEC's change control process, including improvements to policies, procedures, records management, and monitoring controls, and training and reminders for responsible personnel.

Finally, we identified two matters related to the change control process that did not warrant recommendations. We discussed these matters with agency management for their consideration.

Contents

Executive Summary i

Abbreviations iii

Background and Objectives 1

Background 1
Objectives 4

Results 5

Finding 1. [redacted] 5
Recommendations, Management's Response, and Evaluation of Management's Response 7

Finding 2. CCBs Did Not Retroactively Review and Approve Emergency Changes, as Required 8
Recommendation, Management's Response, and Evaluation of Management's Response 9

Finding 3. Agency and Contractor Personnel Inconsistently Implemented the Change Control Process 10
Recommendations, Management's Response, and Evaluation of Management's Response 12

Finding 4. Change Control Procedures Did Not Fully Define Requirements for Testing Information 15
Recommendations, Management's Response, and Evaluation of Management's Response 16

Finding 5. CCBs Lacked Predefined Evaluation Criteria 19
Recommendation, Management's Response, and Evaluation of Management's Response 20

Finding 6. The SEC's Enterprise Change Control Tool Did Not Effectively Maintain Records or Ensure Unambiguous Configuration Item Identifiers 21
Recommendations, Management's Response, and Evaluation of Management's Response 22

Other Matters of Interest 23

Appendices 25

Appendix I. Scope and Methodology 25
Appendix II. Management Comments 28

Tables

Table 1. Change Management Roles, Responsibilities, and Resources 2

Table 2. SEC Annual CRs (CY 2019 – CY 2025) 3

Table 3. SEC Emergency CRs (CY 2021 – CY 2025) 8

Table 4. Examples of Ambiguous Configuration Item Identifiers..... 22

Table 5. Change Control Issues Grouped by Possible Causes 23

Abbreviations

CCB	change control board
CR	change request
CY	calendar year
EBO	EDGAR Business Office
EDGAR	Electronic Data Gathering, Analysis, and Retrieval system
NIST	National Institute of Standards and Technology
OCCB	Operational Change Control Board
OIG	Office of Inspector General
OIT	Office of Information Technology
RCM	risk and control matrix
SEC or agency	U.S. Securities and Exchange Commission
SCCB	Software Change Control Board
SP	Special Publication

Background and Objectives

BACKGROUND

Change control maintains a system's integrity by managing changes to established baselines. Changes that should be controlled include software updates, maintenance, development, and patches. The U.S. Securities and Exchange Commission's (SEC or agency) change control process is designed to ensure:

- All changes to SEC systems are adequately described.
- The reasons for changes are appropriately documented.
- Applicable testing is conducted and results are documented.
- Implementation is formalized.
- Procedures needed to back out of a change when necessary are documented.
- Business and technical impacts are thoroughly assessed.
- Those impacted by a change have approved the change.
- The organization is aware of all of the above.

The SEC's Office of Information Technology (OIT) established two change control boards (CCBs) with representatives from over a dozen SEC branches, offices, and/or functions (hereinafter referred to as "entities"): (1) the Operational Change Control Board (OCCB)—responsible for approving operational changes to the SEC's production environment,[1] and (2) the Software Change Control Board (SCCB)—responsible for approving software changes. Both CCBs review so-called "CCB changes," and are sponsored by OIT's Capital Planning and Lifecycle Management Branch,[2] which retains organizational responsibility for enterprise change management.

In addition to CCB changes, OIT's *Change Management Process Operating Procedure* defines the following three other change request (CR) types that do not involve CCB review:

1. **Emergency changes** – Required to correct an outage, an imminent outage, or a severe decrease in performance to an application or service.
2. **Urgent changes** – A change which, due to a business need, must be expedited before the next CCB meeting.
3. **Standard changes** – A low risk, low impact change that has been pre-approved by the CCB.

Overview of the Change Management Process. The SEC uses an automated change control tool to submit, approve, and track all production environment changes. When submitting a CR, requestors must

[1] The production environment is the live infrastructure, or operational environment, where end-users interact with the actual applications or services. Production environments are separate from development or testing environments.

[2] Before June 28, 2026, this branch was named the "Capital Planning and Governance Branch."

provide required information and as much detail as possible about the change. The tool then ensures that the appropriate SEC staff approve the CR, validating that the CR is complete and resources are available, before agency personnel and contractors implement the change. Table 1 shows the SEC's change control roles, responsibilities, and resources.

Table 1. Change Management Roles, Responsibilities, and Resources

Role	Responsibilities	Resource Type
Requestor	• Submits CRs via the SEC's enterprise change control tool • Assigns CRs to the appropriate implementing branch • Provides initial acceptance of the completed change	SEC staff or contractor
Submitting Branch Chief/Designated Approval Authority	• Ensures appropriate planning and analysis for changes • Preliminarily approves/rejects CRs • Provides final acceptance that change was completed as requested	SEC staff
Implementing Branch Chief/Designated Approval Authority	• Approves/rejects requested change implementation date • Ensures appropriate information to implement changes is included • Ensures resources are available to complete changes	SEC staff
CR Assignee	• Implement changes • Updates CRs with required closeout information, including implementation artifacts and outcome codes	SEC staff or contractor
Change Management Staff	• Reviews and validates CRs • Schedules CRs for CCB reviews and provides agendas to CCB members • Updates CRs to reflect CCB decisions • Independent Verification and Validation Team reviews CCB CRs for completeness	SEC staff or contractor
OCCB Member	• Meets once a week to review CRs for scheduled changes • Manages changes to the SEC's production environment through proper review, evaluation, and approval • Reviews and determines whether to approve, disapprove, or defer CRs for further discussion or completion of action items	SEC staff
SCCB Member	• Assesses compliance with mandatory federal requirements and alignment with SEC standards and policies • Manages changes to the SEC's production environment through proper review, evaluation, and approval • Reviews and votes on CRs included in weekly SCCB agendas	SEC staff

Source: Office of Inspector General (OIG)-generated based on SEC change control operating procedures, SCCB process operating procedure, and CCB charters available during our scope period.

Between calendar year (CY) 2019 and CY 2025, the SEC averaged approximately 6,400 CRs per year[3] and the CCBs reviewed approximately 27 percent. The remaining CRs were either standard, emergency,

[3] We included in our calculations non-cancelled production environment CRs in the "closed complete" state that also had implementation finish dates between CY 2019 and CY 2025.

or urgent changes that did not involve CCB review. Notably, a large number of CRs were closed in 2025 due to a new procedure that prohibited new CCB or standard CRs until previously implemented CRs were closed. See Table 2.

Table 2. SEC Annual CRs (CY 2019 – CY 2025)

CY	Number of CRs Implemented	Number of CCB Changes	Number of CRs Closed
2019	6,057	1,485 (~25 percent)	5,465
2020	6,710	1,893 (~28 percent)	6,140
2021	6,755	1,836 (~27 percent)	6,786
2022	6,228	1,728 (~28 percent)	5,777
2023	6,080	1,742 (~29 percent)	5,507
2024	6,915	2,078 (~30 percent)	5,658
2025	6,206	1,393 (~22 percent)	9,097

Source: OIG-generated based on data from the SEC's enterprise change control tool.

Prior OIG engagements reported on change control issues that impacted the performance, security, and availability of certain SEC systems, applications, and resources. For example:

- In July 2019, the SEC's infrastructure support services contractor erroneously deployed a software patch to 825 SEC laptops, rendering the laptops inoperable. In response, the SEC designed new change control processes.[4]
- An April 2022 operating system update unintentionally prevented backups of public comments submitted through the SEC's rulemaking comment webform. The lack of backups went unnoticed for approximately four months until a separate system error blocked and deleted comments submitted through the webform. Without backups of the public comments, the SEC was at risk of losing permanent records. To ensure all information was properly received, the SEC contacted each commentor and requested that they resubmit their comments. Ultimately, OIT took steps to address the issue and backups resumed.[5]
- In August 2023, OIT implemented changes to the SEC's mobile device management system that were not well documented, tested, or understood, and at least one was handled as an emergency change when it should not have been. These changes contributed to the loss of former SEC Chair Gary Gensler's text messages, which included federal records. Furthermore, the SEC expended limited resources troubleshooting and attempting to recover the federal records. The SEC has since implemented our recommendation to update policies and procedures to ensure

[4] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Has Taken Steps To Strengthen Its Monitoring Of ISS Contractor's Performance, But Additional Actions Are Needed* (Report No. 565; February 24, 2021); pgs. 16-17.

[5] U.S. Securities and Exchange Commission, Office of Inspector General, *Final Management Letter: Review of SEC Controls Over Public Comments Submitted Online and Actions Taken in Response to a Known Error* (April 14, 2023); pg. 8.

that OIT thoroughly documents and understands changes to the agency's mobile device management system before such changes are implemented.[6]

- [redacted][7]

Early in our audit, agency officials alerted the OIG to two additional instances in which system changes led to unintended consequences:

- The EDGAR Business Office (EBO) implemented a change to the Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) that resulted in the inadvertent dissemination of certain nonpublic information submitted by filers. The issue was identified shortly thereafter but not fully resolved until several months later.
- In January 2025, EBO implemented a change to EDGAR that caused an unintended bottleneck of certain company filings. EBO made an emergency change to address the bottleneck; however, the emergency change introduced a new flaw that allowed certain non-public reporting data to be made public for approximately three months until the flaw was discovered and resolved.[8]

Additionally, OIT experienced staffing changes, transitional adjustments, and contract modifications as part of the SEC's broader workforce optimization efforts. As a result, OIT informed the OIG that it was updating its change control process including revising the charters for the OCCB and SCCB.

OBJECTIVES

The objective of this audit was to assess OIT's process for managing changes to the SEC's operational environment to prevent unintended consequences that can affect the performance and security of SEC systems and data. Specifically, we sought to determine whether OIT adequately defined and consistently implemented a change control process, to include appropriate testing of changes before deployment and regular monitoring for unapproved system changes.

Our audit included judgmentally selected samples of information systems that underwent changes during CY 2024, CRs implemented during the fourth quarter of CY 2024, and CRs with potential unintended consequences implemented between January 2024 and February 2025. Because sample items were judgmentally selected based on a variety of factors, including indicators of potential nonconformance with policies and procedures, our results cannot be projected to the total populations. However, the evidence we gathered helped support our findings, conclusions, and recommendations. Appendix I of this report includes additional information about our scope and methodology, including our review of relevant internal controls and prior coverage.

---

[6] U.S. Securities and Exchange Commission, Office of Inspector General, *Special Review: Avoidable Errors Led to the Loss of Former SEC Chair Gary Gensler's Text Messages* (Report No. 587; September 3, 2025); pgs. i, 4, and 7.

[7] U.S. Securities and Exchange Commission, Office of Inspector General, *Observations on the SEC's Rulemaking Process* (Report No. 588; September 29, 2025); [redacted]

[8] *SEC Statement on Certain Form N-PORT Data* (May 14, 2025).

Results

FINDING 1. [redacted]

[redacted]

[redacted]

[

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

[15] [redacted]

[16] [redacted]

[17] [redacted]

[18] [redacted]

[19] [redacted]

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

To further improve the SEC's change control process, we recommend that the Office of Information Technology:

Recommendation 1:

[redacted]

Management's Response. Management concurred with the recommendation. [redacted] Management's complete response is reprinted in Appendix II.

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

Recommendation 2:

[redacted]

Management's Response. Management concurred with the recommendation. [redacted] Management's complete response is reprinted in Appendix II.

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

FINDING 2. CCBS DID NOT RETROACTIVELY REVIEW AND APPROVE EMERGENCY CHANGES, AS REQUIRED

Emergency changes, by their nature, are the riskiest change type. They may be [redacted] require limited testing before implementation, and involve less documentation at the time of the change.[20] Industry best practices include keeping emergency changes to an absolute minimum and reevaluating such changes after implementation to ensure they were properly categorized and handled. As Table 3 shows, the number of SEC emergency CRs created during the last five CYs (as a percentage of total CRs created) has decreased.

Table 3. SEC Emergency CRs (CY 2021 – CY 2025)[21]

CY	Number of CRs Created	Number of Emergency CRs Created
2021	6,729	664 (~10 percent)
2022	6,207	577 (~9 percent)
2023	6,106	546 (~9 percent)
2024	6,948	583 (~8 percent)
2025	6,182	418 (~7 percent)

Source: OIG-generated based on data from the SEC's enterprise change control tool.

According to NIST SP 800-128:

- Situations may arise that necessitate an emergency change; however, emergency changes must still go through the change control process, "even if it is after the fact."
- Emergency changes are reviewed/resolved by the CCB as soon as is practical after the changes are made.[22]

Similarly, the *Federal Information System Controls Audit Manual*[23] states that, shortly after an emergency change is made, the usual configuration management controls are applied retroactively, and the change is subjected to the same review, testing, and approval processes that apply to scheduled changes.

OIT's *Information Security and Privacy Controls Manual* requires the CCBs to provide oversight of change control activities. This policy also requires the CCBs and/or senior management to evaluate and approve changes to the operational environment. Nonetheless, OIT's procedures did not include retroactive CCB review and approval of emergency changes. Instead, we observed that these changes were reviewed and approved by the submitter's branch chief, which is the lowest level of approval of any change type defined in OIT's procedures. Without CCB oversight of emergency changes even after the fact, unanticipated issues may persist longer than necessary and result in increased operational, security, and/or reputational harm.

[20] Notably, the SEC's fiscal year 2023 RCM identified improper control of emergency changes as a high risk.

[21] We included in our calculations non-cancelled production environment CRs in the "closed complete" state that were also created between CY 2021 and CY 2025.

[22] NIST SP 800-128; pg. 37.

[23] U.S. Government Accountability Office, *Federal Information System Controls Audit Manual* (GAO-24-107026, September 2024).

One example of an emergency CR we identified that would have benefited from a retroactive CCB review and approval process involved the EDGAR system. In early 2025, the SCCB approved a change to update the system. The change unintentionally caused a bottleneck of certain EDGAR submissions. To alleviate the bottleneck, EBO implemented an emergency change reverting a portion of the updated software to an older version. After the emergency change, EBO intended to deploy a fix that would allow the new optimized software to work as intended, however, this did not happen. Unbeknownst to EBO, the older software then caused certain nonpublic information to be publicly disseminated for the next three months. After discovering this in May 2025, EBO implemented another change (an urgent change) to correct the issue.

When we inquired about EBO's approach, SCCB members stated that the emergency change should have involved a full—not partial—software rollback. Had this emergency change been retroactively reviewed by the SCCB, the SEC's dissemination of nonpublic information via EDGAR may have been corrected sooner.

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

To further improve the SEC's change control process, we recommend that the Office of Information Technology:

Recommendation 3:

Update change control policies and procedures to ensure that emergency changes receive retroactive change control board review and approval.

Management's Response. Management partially concurred with the recommendation, noting that current practice already includes weekly review of emergency, urgent, and non-compliant change requests by change management and senior operations leadership. OIT agrees with the need for strengthened oversight of emergency changes but believes the existing governance structure appropriately manages retroactive reviews. To enhance transparency, OIT will update change control procedures to formally document this practice and will include a list of emergency changes in the weekly change control board agenda for review. Completion is targeted by March 2027. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that OIT agrees with the need for strengthened oversight of emergency changes; however, management's response does not describe how such improved oversight will be achieved. Therefore, the proposed actions do not fully address the intent of the recommendation and we consider the recommendation unresolved pending clarification of whether change control boards will retroactively approve emergency changes listed in weekly board agendas. We note that OIT's *Information Security and Privacy Controls Manual* states that its policies involving change control shall comply with federal standards and guidelines. NIST SP 800-128 states emergency changes go through the change process—which includes change control board approval—as soon as is practical after the changes are made. The recommendation can be closed when we receive and accept evidence that OIT updated policies and procedures to ensure that emergency changes receive retroactive change control board review and approval.

FINDING 3. AGENCY AND CONTRACTOR PERSONNEL INCONSISTENTLY IMPLEMENTED THE CHANGE CONTROL PROCESS

OIT's *Change Management Process Operating Procedure* and *Change Requests User's Guide* detail the SEC's change management processes and the requirements for submitting CRs. Although OIT adequately defined aspects of its change control process, implementation was not always consistent. For example, we reviewed a judgmental sample of each of the four CR types (CCB, emergency, urgent, and standard)[24] and noted the following:

- More than half of the 25 emergency CRs we reviewed did not appear to meet the definition of an emergency change or include a root cause analysis, as required.
- Approximately 21 percent of CRs among all four change types we reviewed were not timely updated to reflect implementation or completion of the change.
- Almost half of the 25 standard CRs we reviewed were [redacted]

These occurred due to gaps in oversight of the CR process and a lack of controls to [redacted] Specifically, submitting branch chiefs approved CRs without ensuring submitter inputs were accurate and supporting artifacts were complete. Branch chiefs also did not promptly confirm final acceptance of completed changes, resulting in delays in updating and closing CRs after implementation. Furthermore, as mentioned in Finding 1, OIT had not [redacted] Inconsistent implementation of the change control process may introduce security risks, lead to disruptions or delays in functionality, and/or complicate troubleshooting when issues arise.

Some CRs Did Not Appear to Be Emergencies or Include a Root Cause Analysis

According to OIT's *Change Requests User's Guide*, emergency changes correct severely degraded services, correct a break or fix an outage, or must be implemented quickly to avoid such issues. Emergency changes require branch approval before they are implemented, but implementation may occur before the change is fully documented. Within 12 hours of the change, however, an emergency CR must be submitted for approval and must explain the root cause of the emergency.

Fifteen of the 25 emergency CRs we reviewed did not appear to meet the definition of an emergency. When asked, OIT stakeholders agreed that, in four of the cases we questioned, a different change type would have been more appropriate, and they provided additional information to explain why seven of the CRs qualified as emergency changes. Based on the information available, we did not agree with OIT's assertion that the remaining four CRs were properly categorized as emergency changes because the changes did not correct a break or fix an outage and were not needed to avoid such issues. Additionally,

[24] Our judgmental sample included 25 CCB changes, 25 emergency changes, 27 urgent changes, and 25 standard changes out of the 1,771 total CRs implemented during the fourth quarter of CY 2024. See Appendix I for additional details on our methodology.

18—or more than half—of the emergency CRs in our sample lacked the required root cause analysis explaining the reason(s) for the emergency change.

The SEC's request, validation, and approval process for emergency changes requires that the requester submit a CR that details the change to be implemented. The requestor must ensure that the CR type and urgency level selected are appropriate, the source of the defect or problem that must be (or was) fixed is explained clearly, a root cause analysis is documented, and the appropriate implementation branch is selected. The submitter's branch chief reviews the CR to ensure it contains the appropriate level of detail to warrant immediate implementation and, if so, approves the CR in the SEC's enterprise change control tool. Although all 25 emergency CRs we reviewed were approved by the submitting branch, there were gaps in the oversight process that allowed submitting branch chiefs to approve CRs even though required information was missing. Providing additional training to personnel responsible for submitting, reviewing, and approving CRs could help ensure consistent implementation of the CR process.

As discussed in Finding 2, OIT's policies and procedures did not include retroactive CCB review and approval of emergency changes. OIT's implementation of Recommendation 3 would help confirm that the correct change type was chosen.

Some CRs Were Not Timely Updated to Reflect the Outcome of Changes

According to OIT's *Change Management Process Operating Procedure*,[25] assignees implement changes as described in CRs and update CRs with the appropriate "Outcome Code," the specific actions taken, and the date and time changes were implemented. Assignees, requesters, and approvers also ensure changes were completed as required and indicate acceptance in the SEC's enterprise change control tool.[26]

In CY 2025, OIT's Capital Planning and Lifecycle Management Branch noted delays in updating CRs to the "closed complete" state. Such overdue CRs—that is, CRs left in the "Implementation," "Requester Acceptance," or "Submitting Branch Acceptance" state for 30 or more days past the implementation date—can hinder the SEC's ability to determine whether a change was implemented as described. In February 2025, the Branch began monitoring and helping to close 2,077 overdue CRs. By July 2025, the number of overdue CRs had decreased by more than half to 784. The Branch issued guidance for closing the remaining overdue CRs by August 2025, actively monitored backlogs, and, beginning in September 2025, restricted branches from submitting new CCB or standard CRs if overdue CRs were not closed. OIT also created a step-by-step guide for how to close a CR in the enterprise change control tool.

As of August 2026, approximately 360 overdue CRs remained, including 164 with implementation finish dates from 2025 and prior years. Additional steps are needed to close the remaining overdue CRs and ensure CRs are timely closed going forward.

[25] 24-03-BOD-CMCC-01, Revision 9, *Operating Procedure Governance: Change Management Process*, January 2025.

[26] *Id.* at pgs. 9 and 10.

Some Standard CRs Were Implemented [redacted]

According to OIT's *Change Management Process Operating Procedure*, all standard and CCB changes must be scheduled within the approved [redacted] Any work completed [redacted] requires a [redacted] waiver request from the Assistant Director or designee. Controls that restrict the timing of changes help reduce confusion, errors, and unintended consequences. As such, each CR contains a field for the requester to enter the start date and time agreed to by the group assigned to implement the change, and the enterprise change control tool records the actual implementation time.

Eleven of the 25 standard CRs we reviewed were implemented before the approved time.[27] In each case, the configuration management quality assurance reviewer flagged that the change was implemented before the approved time. When asked about this issue, OIT officials indicated that the SEC is [redacted]

In one example, [redacted] According to the root cause analysis, this change could have been more disastrous had another administrator not already been logged in and capable of manually rolling back the change. Without that access, personnel would have had to physically reset a device at the SEC's data center which would have taken several hours.

According to OIT, [redacted] access is configured for Cloud Administrator accounts [redacted]

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

To further improve the SEC's change control process, we recommend that the Office of Information Technology:

Recommendation 4:

Remind, and as needed train, change request submitters and branch approvers about the proper use of emergency changes, [redacted] for standard changes, and the expected timeframe for requester and branch acceptance of change requests after implementation.

> **Management's Response.** Management concurred with the recommendation, stating that a training program is in place, and users must review change control training documentation and successfully complete a knowledge assessment before gaining access to the change control system. In response to the recommendation, OIT will send periodic communications to reinforce proper use of

[27] The other 14 CRs in our sample were either implemented within the approved date and time or had a waiver.

emergency changes, [redacted] and timely acceptance of completed change requests. Evidence of management action will be provided by March 2027. Management's complete response is reprinted in Appendix II.

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

Recommendation 5:

Close change requests with implementation finish dates from 2025 and prior years.

Management's Response. Management concurred with the recommendation, noting that closure activities for change requests with implementation finish dates from 2025 and prior years were underway before the audit. Completion is targeted by March 2027. Management's complete response is reprinted in Appendix II.

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

Recommendation 6:

Update change request procedures to include expected timeframes for closing approved change requests, and establish responsibility for regular monitoring of overdue change requests.

Management's Response. Management concurred with the recommendation, stating that OIT will establish and publish new guidelines for the timely closing of change requests and formally assign responsibility for regular monitoring of overdue requests. Completion of this task is planned by March 2027. Management's complete response is reprinted in Appendix II.

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

Recommendation 7:

Implement control(s) [redacted]

Management's Response. Management partially concurred with the recommendation, stating that, while OIT agrees that [redacted] OIT will [redacted] and determine the most effective and risk-based approach by March 2027. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management agrees that [redacted] During the audit, OIT stated it was in the process of [redacted] However, we acknowledge management's right and responsibility [redacted] to determine the most effective and risk-based approach. We consider this recommendation unresolved pending the outcome of OIT's [redacted] The recommendation can be closed when we receive and accept evidence that OIT implemented control(s) [redacted]

FINDING 4. CHANGE CONTROL PROCEDURES DID NOT FULLY DEFINE REQUIREMENTS FOR TESTING INFORMATION

NIST SP 800-128 states that change control procedures include requirements for the format and types of testing information presented to CCBs. In addition, the *Federal Information System Controls Audit Manual* states documentation supporting implemented changes should provide sufficient evidence that test plans and results were reviewed. Likewise, OIT's *Change Management Process Operating Procedure* and the charters for the SEC's OCCB and SCCB seek to ensure that the agency's change management process includes testing, testing results are documented, and the CCBs systematically manage changes through proper review, evaluation, and approval. However, SEC change control procedures did not fully define the format and types of testing information to be included in CRs or presented to the CCBs.[28] As a result, testing information used for decision-making was inconsistent and, in some cases, there was a lack of evidence that test plans and results were reviewed. This increased the likelihood of changes based on inadequate testing and unintended consequences that can affect the performance and security of SEC systems and data.

Some CRs Included Inconsistent Testing Information

OIT's *Change Requests User's Guide* requires test results to be attached to CRs if a change was tested. OIT's CR training slides also state that the submitter must attach the applicable security assessment, testing documentation, and any artifacts demonstrating that the work to support the change was performed correctly. However, OIT has not clearly defined the format of testing information that should be attached. We judgmentally selected and reviewed the attachments for 25 of 474 CRs implemented during the fourth quarter of CY 2024 and for which testing occurred, noting the following inconsistencies:

- 21 did not include a security assessment or indicate that one was not applicable.
- 21 did not include test plan information or explain the type and scope of testing performed.
- 14 did not include conclusive test results.

Additionally, CRs include a "Security Comments" field, which OIT's *Change Requests User's Guide* states is a placeholder for security comments. This field was blank for all but two of the CRs we reviewed.

Although OIT officials acknowledged test plans are considered "best and common practices," OIT has not required them and has not enabled the enterprise change control tool to include test plans and allow for standardizing test plan information.

Lack of Evidence That Test Plans and Results Were Reviewed

OIT's *Change Management Process Operating Procedure* states the submitting branch chief shall review CRs to ensure compliance with all testing, documentation, and user acceptance requirements. Similarly, OIT's *Software Change Control Board Process Operating Procedure* states the submitting branch chief

[28] Notably, the SEC's fiscal year 2023 RCM identified a lack of policies and procedures as a risk.

shall review CRs to ensure appropriate testing is completed. Because the CRs we reviewed did not consistently include required testing documentation, we question the efficacy of these reviews.

OIT's procedures state that if a change cannot be tested then a reason should be documented. We judgmentally selected a sample of systems, including those with CRs that indicated that testing occurred and others indicating that testing could not be completed [redacted] According to OIT, the discrepancies we observed generally resulted from errors and inaccurate information, which may allow submitters to avoid testing, prevent testing information from being reviewed, and/or deny CCB members useful information for decision-making.

In addition, the respective system security plans for each of the systems in our judgmentally selected sample indicated that control CM-3(2), "Testing, Validation, and Documentation of Changes," was implemented. For this control, NIST SP 800-53 states, "Test, validate, and document changes to the system before finalizing the implementation of the changes." NIST SP 800-53 also states that operational systems may need to be taken offline or replicated before testing can be conducted, and if testing cannot be conducted, organizations employ compensating controls. Therefore, CRs like many we reviewed that indicate no testing was performed [redacted] should also include an explanation of compensating controls.

Finally, according to the Branch Chief for OIT's Capital Planning and Lifecycle Management Branch, CCB members should review test results before voting. This aligns with the requirements discussed in NIST SP 800-128 and the objective of the CCBs to systematically manage changes to the SEC's production environment. However, some CCB members told us that it is not their responsibility to review or evaluate testing information attached to the CRs.

An example of a CR that could have benefited from a documented test plan and CCB review of testing information involved a change to an SEC filer system. An SCCB-approved change implemented in September 2024 prematurely introduced October 2024 fee rates. This resulted in the suspension of three filer submissions because the submitted fees and calculated fees differed. After a filer notified the SEC of this issue, the agency implemented an emergency change to revert to the correct fee rate. Had the CR submitter developed a test plan detailing the scope and methodology of testing and attached this test data to the CR for review, the unintended consequences from this change may have been avoided. In addition, one of the seven user acceptance testing signoff sheets attached to the CR stated that the user who signed off had little experience and no expertise with the system tested and "received insufficient training specific to conducting [user acceptance testing] for this system development." Had the SCCB reviewed and acted on this information, additional measures may have been taken before the change was approved and implemented.

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

To further improve the SEC's change control process, we recommend that the Office of Information Technology:

Recommendation 8:

Update change control policies, procedures, and/or training materials to (a) specify the requirements for the format and types of testing information presented to SEC's change control boards, and (b) reinforce requirements for pre-release testing.

Management's Response. Management nonconcurred with the recommendation, stating that existing policies, procedures, and training materials already specify testing requirements, documentation expectations, and pre-release testing requirements. Project teams, as system subject-matter experts, are responsible for determining the format and type of appropriate testing, and testing results are required as an attachment to change requests that will be reviewed by change control board members. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Based on management's nonconcurrence with the recommendation, we consider this recommendation unresolved. We acknowledge, as stated in the report, that OIT requires test results to be attached to change requests if a change was tested, along with any artifacts demonstrating that the work to support the change was performed correctly. Furthermore, we agree project teams determine the appropriate format and type of ***testing***. However, OIT has not fully defined the format and types of ***testing information*** that should be attached to the change requests. As a result, useful ***testing information*** (such as a summary of the testing scope, types of testing performed, and/or degree of testing success) is not consistently provided to the change control boards. OIT's *Information Security and Privacy Controls Manual* states that its policies involving change control shall comply with federal standards and guidelines. NIST SP 800-128 states that change control procedures include requirements for the format and types of ***testing information*** presented to change control boards. The recommendation can be closed when we receive and accept evidence that OIT specified requirements for the format and types of ***testing information*** presented to the change control boards, and notified staff of these requirements.

Recommendation 9:

Review the capabilities of the SEC's enterprise change control tool and determine whether the agency could benefit from enabling functions related to test plans and testing information, then update applicable policies and procedures accordingly.

Management's Response. Management concurred with the recommendation. OIT is reviewing the SEC's enterprise change control tool to identify whether additional test-related capabilities would benefit the agency. If so, OIT will update the applicable policies and procedures. Completion is planned by May 2027. Management's complete response is reprinted in Appendix II.

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

Recommendation 10:

Determine which change control board member(s) should review testing information as part of their predefined evaluation criteria (see Finding 5).

Management's Response. Management nonconcurred with the recommendation, stating that testing results are required for all changes unless they meet specific, pre-approved exceptions. Responsibility for reviewing testing results rests with the system or product owners, who have the necessary subject-matter expertise. The SEC's change control boards rely on these attestations and supporting documentation rather than independently reviewing testing information. This approach provides appropriate oversight, and additional specification of change control board member responsibilities is unnecessary. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. Based on management's nonconcurrence with the recommendation, we consider this recommendation unresolved. In management's response to Recommendation 8, OIT states that "testing results are required as an attachment to change requests that will be reviewed by change control board (CCB) members." The recommendation can be closed when we receive and accept evidence OIT determined which change control board member(s) should review testing information as part of their predefined evaluation criteria.

Recommendation 11:

Develop quality assurance procedures to ensure testing is performed when warranted and compensating controls are documented when needed.

Management's Response. Management concurred with the recommendation. OIT will further clarify the change request form to require submitter attestation that testing was completed and accepted by the system owner. Completion is targeted by March 2027. Management's complete response is reprinted in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurs with the recommendation and plans to clarify submitter attestation requirements, however, management's response does not address documenting compensating controls. Therefore, the proposed actions do not fully address the intent of the recommendation and we consider the recommendation unresolved pending clarification of whether management will develop quality assurance procedures to ensure compensating controls are documented in [redacted]

FINDING 5. CCBS LACKED PREDEFINED EVALUATION CRITERIA

The SEC's OCCB and SCCB each include members representing over a dozen SEC entities. The boards' charters state that they may "[a]pprove, disapprove or defer any change request based on documented approval criteria." Similarly, NIST SP 800-128 states CCB predefined evaluation criteria "helps to ensure that each proposed and implemented change is evaluated in a consistent and repeatable manner balancing security, business, and technical viewpoints." However, OIT's Capital Planning and Lifecycle Management Branch—which retains organizational responsibility for enterprise change management and chairs both boards—did not collect or centrally maintain evaluation criteria for each of the CCB members. Although OIT has established various SharePoint sites and frameworks to assist in stakeholder coordination, most of the board members told us that they had not established predefined evaluation criteria. Without such criteria, CCB approval of CRs may not be consistent, repeatable, or thorough, which increases the risk to the SEC's systems and data.

OCCB

The OCCB meets weekly and includes representatives from 14 branches, primarily within OIT.[29] The Capital Planning and Lifecycle Management Branch develops OCCB agendas—listing all CRs up for vote—and furnishes all meeting materials two business days before each meeting. According to the OCCB Chair, each CR on the agenda is discussed, allowing time for questions before members vote.

During the last quarter of CY 2024, the OCCB met 13 times to review 437 CRs, and the board approved 99.3 percent of those CRs.[30] On average, OCCB meetings involved votes on 34 CRs and lasted 42 minutes (or approximately one minute and 14 seconds per CR). In addition, one meeting (scheduled for December 24, 2024) was conducted via email. On Friday, December 20, 2024, at 2:29 PM, the Capital Planning and Lifecycle Management Branch emailed to OCCB members the agenda and details for 20 CRs and asked board members to review and submit their approval (or rejection) by 12:00 PM on Monday, December 23, 2024. Three members submitted their approvals within three hours. The remaining members submitted their approvals on December 23, 2024.

Notably, OCCB members told us that they can ask questions and review materials before formal meetings, and some coordinate with submitters before CRs even reach the OCCB. Nonetheless, the OCCB Chair acknowledged that the process could benefit from additional buy-in, review, and questioning from board members. Moreover, although some OIT branches represented by OCCB members have requirements, the Capital Planning and Lifecycle Management Branch has not established or collected predefined evaluation criteria for the various OCCB members or maintained it in a centralized location.

SCCB

The SCCB includes representatives from 17 different SEC entities and, as a virtual board, it typically votes via email.[31] The Capital Planning and Lifecycle Management Branch develops the SCCB

[29] According to the OCCB charter, dated January 7, 2025.

[30] The three CRs the OCCB did not approve included two that were withdrawn and one that was deferred.

[31] According to the SCCB charter, dated January 7, 2025.

agendas—listing all CRs up for vote—and furnishes the materials two business days before each weekly board meeting. Project teams generally submit CRs for SCCB review when software changes are ready to go live in the SEC production environment after successful completion of all applicable lifecycle requirements.

During the last quarter of CY 2024, the SCCB voted 13 times, covering a total of 81 CRs (or, on average, approximately 6 CRs per vote). The SCCB voted to approve 60 (or approximately 74 percent) of these CRs. For the CRs that were disapproved, "no" votes typically came from the Security Assessments and Compliance Branch, Privacy and Information Assurance Branch, and/or Cyber Risk and Governance Branch representatives. The remaining representatives either did not vote during the period or voted to approve the CRs nearly 100 percent of the time. Furthermore, some representatives voted to approve all CRs in a weekly agenda within minutes of receiving the materials.

According to the SCCB Chair, the board uses a spreadsheet to track each change voted on, providing a consistent, repeatable process that every team must follow before a change is put into production. However, the spreadsheet does not contain evaluation criteria used by each SCCB member to review and approve changes, and OIT has yet to update its *Software Change Control Board Process Operating Procedure* or *Change Requests User's Guide* to reflect this process. Additionally, although the SCCB SharePoint site included some useful information that could be used to develop predefined SCCB evaluation criteria, some links were broken and others were outdated at the time of our review. In response to our questions, some SCCB members provided draft evaluation criteria that, if formally established, could be used to ensure board members evaluate each proposed and implemented change in a consistent and repeatable manner.

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

To further improve the SEC's change control process, we recommend that the Office of Information Technology:

Recommendation 12:

Coordinate with the change control boards to develop and document predefined evaluation criteria for each of the SEC entities represented.

Management's Response. Management concurred with the recommendation. OIT will require each change control board voting member to document evaluation criteria for assessing change requests and ensure the criteria are accessible to stakeholders. Completion is targeted by May 2027. Management's complete response is reprinted in Appendix II.

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

FINDING 6. THE SEC'S ENTERPRISE CHANGE CONTROL TOOL DID NOT EFFECTIVELY MAINTAIN RECORDS OR ENSURE UNAMBIGUOUS CONFIGURATION ITEM IDENTIFIERS

National Archives and Records Administration and SEC criteria require the SEC to retain records of configuration-controlled changes.[32] However, OIT changed the SEC's enterprise change control tool resulting in the loss of key CR record information. Specifically, the required "Configuration Item" field, which identifies the product or system being changed, was deleted for over 100 CRs implemented as of January 2024. Additionally, NIST SP 800-128 states that each configuration item is assigned an unambiguous identifier so it can be uniquely referenced within the change management process. However, due to ineffective controls, many configuration item entries used slightly different names for the same system. CR records that (1) do not identify the configuration items changed, or (2) include ambiguous identifiers create an inaccurate and/or unverifiable portrait of the SEC's production environment, negatively impact management of federal records, and hinder the SEC's troubleshooting efforts when issues arise.

CRs Did Not Always Name the Product or System Being Changed

The SEC's Records and Information Management Group is responsible for ensuring the agency complies with federal laws regarding record creation, maintenance, and disposition. In doing so, the group publishes the SEC's comprehensive records schedule. The *Records Schedule for Configuration and Change Management Records* (0620-050-1) includes "records created and retained for…configuration and change management" with disposition five years after the system is superseded by a new iteration, terminated, defunded, etc. The SEC's record schedule includes a link to the National Archives and Records Administration's records schedule, which adds that configuration and change management records include "documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes."

Despite these requirements, we identified over 100 CRs implemented since January 2024 that did not include the required "Configuration Item" field, naming the product or system being changed. OIT told us this was due to the retirement of these configuration items in its configuration management database, which resulted in the data in the corresponding CR fields being deleted by an automated discovery tool.

Many Records Included Ambiguous Configuration Item Identifiers

OIT's *Change Request User Guide* states for the required "Configuration Item" field, users are to select impacted products or systems from a drop-down list. If the appropriate product or system cannot be found, users are to contact the configuration management database point of contact to request that it be added to the list. However, we identified at least 20 configuration item entries that used slightly different names for the same system, demonstrating the ineffectiveness of OIT's process for assigning unambiguous identifiers. Table 4 shows examples of these configuration item identifiers.

[32] National Archives and Records Administration General Records Schedule 3.1: General Technology Management Records (November 2019); SEC Comprehensive Records Schedule Category 0620: Information Technology Services.

Table 4. Examples of Ambiguous Configuration Item Identifiers

Configuration Item Version 1	Configuration Item Version 2
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Source: OIG-generated based on data from the SEC's enterprise change control tool.

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

To further improve the SEC's change control process, we recommend that the Office of Information Technology:

Recommendation 13:

In conjunction with the SEC's Records and Information Management Group, implement technical and procedural controls to ensure configuration management database records associated with configuration-controlled items and change requests are maintained in accordance with the SEC's records schedule and federal records retention requirements.

Management's Response. Management concurred with the recommendation. OIT will update the configuration management database procedures and strengthen both technical and procedural controls so that records associated with configuration-controlled items and change requests are maintained in accordance with SEC records schedule and federal records retention requirements. Completion is targeted by May 2027. Management's complete response is reprinted in Appendix II.

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

Recommendation 14:

Develop procedures to maintain an inventory of configuration items that are unique and unambiguous.

Management's Response. Management concurred with the recommendation. OIT will develop procedures to maintain an inventory of configuration items that are unique and unambiguous. Completion is targeted by May 2027. Management's complete response is reprinted in Appendix II.

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

Other Matters of Interest

During our audit, we identified two matters that did not warrant recommendations. We discussed these matters, described below, with agency management for their consideration.

OIG Analysis of Changes That Had Unintended Consequences

During our audit, we identified 22 examples where it appeared changes, to varying degrees, had unintended consequences affecting the performance and/or security of SEC systems and data.[33] We grouped these issues by the possible causes shown in Table 5. Notably, one or more cause unique to a particular set of circumstances may be relevant in each situation (e.g., specific personnel, system, event, etc.), making broad recommendations for improvement a challenge. Regardless, we discussed these issues and corresponding CRs with the stakeholders involved and, in some cases, stakeholders took corrective action to prevent future occurrences.

Table 5. Change Control Issues Grouped by Possible Causes

Possible Cause 1: Limited Testing
Regression testing did not exist for the particular function that experienced the issue*
Scope of the testing did not cover the particular issue
Lack of user acceptance testing for this change
Post-implementation testing did not occur and/or was insufficient for this change
Code mergers were not reviewed/conflicts were not detected prior to this release*
Possible Cause 2: Lack of Representative Test Environment
Difficulty in creating an exact test environment match of this legacy system with multiple dependencies
No test environment existed or was available for certain cloud environments*
Lower test environment did not exactly match the production environment
Possible Cause 3: Contractor Reliance and/or Ineffective Oversight
System personnel did not question a particular contractor proposal that introduced a flaw
Contractor had insufficient knowledge of confidential forms
System personnel did not ensure requirements were timely captured
System personnel did not ensure version control*
System personnel did not ensure the contractor was using the most current driver*
System personnel did not ensure an emergency change was timely documented
System personnel did not ensure contractors used the appropriate account to make the change*
System personnel did not prevent contractors from prematurely implementing the change

[33] We reviewed problem and incident tickets, after-action reports, plans of action and milestones, and lessons learned information, among other sources, from January 2024 through February 2025 to identify these examples.

Possible Cause 4: Nondescript/Inaccurate CR Information
Incorrect information regarding plan of action and milestones and production readiness review
CR description did not match the actual change
CR was missing details on groups to be excluded
Inaccurate response regarding whether the change needed to be tested
Inaccurate change type assigned
Possible Cause 5: Human Error
Use of incorrect fee rate file*
Poorly developed validation checks
Accidental overwriting of prior correction
“Tunnel vision” (i.e., not understanding subnets involved)
Forgot to refresh load balance or purge cache
Did not check the defaults
Did not anticipate 64-bit would impact 32-bit*

Source: OIG-developed based on our analysis of the 22 change control issues identified.

*Stakeholders took corrective action to prevent future occurrences.

OIT Could Benefit from a Centralized After-Action Report Repository

Although OIT occasionally tasks personnel or contractors with developing after-action reports after unsuccessful changes and other events, according to OIT these reports are not maintained in a centralized repository. This could limit OIT’s ability to correlate, investigate, and resolve issues that are more systemic in nature and/or limit OIT’s ability to review and more broadly understand lessons learned. OIT should consider establishing a centralized location to store after-action reports so that the reports are available and accessible when needed to support reviews of system incidents or other problems.

Appendix I. Scope and Methodology

We conducted this performance audit from December 2024 to November 2026 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.

Objectives and Scope

The objective of this audit was to assess OIT's process for managing changes to the SEC's operational environment to prevent unintended consequences that can affect the performance and security of SEC systems and data. Specifically, we sought to determine whether OIT adequately defined and consistently implemented a change control process, to include appropriate testing of changes before deployment and regular monitoring for unapproved system changes.

Methodology

To address our objectives, among other work performed, we conducted fieldwork at the SEC's Headquarters in Washington, DC, and met with personnel from OIT, EBO, the Office of the Chief Data Officer, and the Office of Support Operations, who are responsible for aspects of the SEC's change management process. We also reviewed:

- Applicable federal laws, regulations, and guidance, and relevant SEC policies and procedures.
- OCCB and SCCB charters.
- Judgmentally selected samples of CRs created and tracked via the SEC's enterprise change control tool.
- Test plans and test results for selected CRs.
- Circumstances and after-action reports for certain CRs that appeared to have unintended consequences and were implemented between January 2024 and February 2025.
- Change control matters that came to our attention during our audit.

Our audit included a sample of information systems that underwent changes during CY 2024 as well as samples of CRs. Specifically, to assess whether the SEC consistently implemented a change control process, we judgmentally sampled CRs across the four change types (CCB, urgent, emergency, and standard) implemented during the fourth quarter of CY 2024. We reviewed the selected CRs to determine whether staff selected the appropriate change type and then tested that the CR contained the required attributes for the change type selected. To determine whether changes were appropriately tested before deployment, we reviewed evidence of testing attached to the CRs. We also requested [redacted] Finally, we identified and reviewed examples of CRs with potential unintended consequences implemented between January 2024 and February 2025.

Because sample items were judgmentally selected based on a variety of factors, including indicators of potential nonconformance with policies and procedures, our results cannot be projected to the total populations. However, the evidence we gathered helped support our findings, conclusions, and recommendations.

Internal Controls

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

Control Environment. We assessed the control environment established by OIT's senior management, reviewed OIT's organizational structure, and interviewed staff responsible for OIT's internal control documentation and for annually reviewing and testing internal controls.

Risk Assessment. We reviewed OIT's management assurance statements and RCMs to identify risks and controls related to the SEC's change control process. In reviewing recent RCMs, we noted that the number of risk items attributed to OIT has been significantly reduced, from 90 in fiscal year 2023 to 15 in fiscal year 2025. Some of the associated risks no longer included in the fiscal year 2025 RCM involved aspects of configuration management, unauthorized system changes, and emergency changes.

Control Activities. We reviewed applicable federal guidance, SEC policies and procedures, and OIT standard operating procedures to identify and test key control activities. We reviewed control activities for the creation and review of CRs, and we tested related attributes in our CR sample testing. We also reviewed OCCB and SCCB meeting minutes and approvals. Lastly, we interviewed OIT staff and contractors involved in submitting and implementing CRs to understand the change request process, and members of the OCCB and SCCB to understand their CR review and approval processes.

Information and Communication. OIT established policies and procedures related to the change management process. OIT also maintains a centralized intranet site with supplemental guidance, user guides, change management metrics, and additional information that may be useful to staff in ensuring all CRs are created and tracked in the SEC's enterprise change control tool.

Monitoring. We reviewed OIT's internal control documentation and standard operating procedures, and discussed with OIT management its roles and responsibilities for monitoring the change management process. As noted in Finding 1, OIT did not [redacted]

As noted in this report, we gained an understanding of controls relating to the request, documentation, testing, and approval of changes that affect the SEC's operational production environment, and we tested the implementation of those controls. Weaknesses in internal controls that were identified during the audit are detailed in the "Results" section of this report. Our recommendations, if implemented, should help strengthen the SEC's change control process.

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 objectives, we relied on data in the SEC's enterprise change control tool. We generated a list of in-scope CRs from the tool to identify those subject to sampling; however, we were unable to test the completeness of the listing because changes may have bypassed the enterprise tool. We also used the information in the change control tool to assess the timeliness of completing CR processing. To assess the reliability of data we:

- Interviewed knowledgeable personnel from OIT's Capital Planning and Lifecycle Management Branch, which governs the information technology change management process.
- Interviewed personnel involved in submitting, approving, and implementing CRs.
- Filtered data by CY and change type and compared the results to identify the existence of any anomalies.
- Tested data from our scope period to determine whether required fields were missing data.

Based on the work we performed (Finding 6 of this report notwithstanding), we found the enterprise change control data sufficiently reliable for the purpose of this audit.

Prior Coverage

Between 2017 and 2025, the SEC OIG issued the following reports of particular relevance to this audit:

SEC OIG:

- *Observations on the SEC's Rulemaking Process* (Report No. 588, September 29, 2025).
- *Special Review: Avoidable Errors Led to the Loss of Former SEC Chair Gary Gensler's Text Messages* (Report No. 587, September 3, 2025).
- *Final Management Letter: Review of SEC Controls Over Public Comments Submitted Online and Actions Taken in Response to a Known Error* (April 14, 2023).
- *The SEC Has Taken Steps To Strengthen Its Monitoring Of ISS Contractor's Performance, But Additional Actions Are Needed* (Report No. 565, February 24, 2021).
- *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 552, December 17, 2018).
- *Audit of the SEC's Progress in Enhancing and Redesigning the Electronic Data Gathering, Analysis, and Retrieval System* (Report No. 544, September 28, 2017).

These reports can be accessed at https://www.sec.gov/oig.

Appendix II. Management Comments

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

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

From: Jed Hickman, Acting Chief Information Officer and Director, EDGAR Business Office

JEFFREY HICKMAN Digitally signed by JEFFREY HICKMAN Date: 2026.10.22 07:47:12 -04'00'

Date: October 22, 2026

Subject: Management Response to Draft Office of Inspector General Report, *Improvements Needed in the SEC's Change Control Process*

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the Securities and Exchange Commission's (SEC) change control process. We appreciate the OIG's observations and remain committed to strengthening the controls that safeguard the integrity, security, and availability of SEC systems and data.

The Office of Information Technology (OIT) and the EDGAR Business Office (EBO) have made sustained progress in maturing change control governance across the agency. OIT has formalized oversight through the Operational Change Control Board (OCCB) and Software Change Control Board (SCCB), each supported by policies that define change types, approval workflows, and supporting artifacts. These structures have enhanced consistency, transparency, and accountability for changes promoted into production environments.

EBO similarly implements disciplined change management practices for EDGAR system changes, supported by detailed documentation, specialized procedures, and active participation in SCCB and technical reviews. EBO fosters a culture committed to risk identification and continuous improvement.

We view the OIG's findings as highlighting areas for more consistent implementation of existing processes rather than deficiencies in the underlying governance framework. Several observations point to opportunities to more fully formalize or reinforce existing practices. To address these areas, management is strengthening oversight through enhanced training, clearer communication, improved monitoring, and formalization of weekly reviews of emergency and non-compliant change requests.

Of the 14 OIG recommendations, we concur with 10, partially concur with two, and nonconcur with two. For the two nonconcurrences, we respectfully offer alternative perspectives where we believe current controls sufficiently mitigate the underlying risks. Additional details are presented in Appendix A.

Management has already initiated several enhancements, including updates to policies and procedures, enhanced staff training, improved communication mechanisms, assessments of supporting tool capabilities, and expanded quality assurance processes. We remain committed to ensuring that changes are accurately described, justified, tested, assessed for impact, and approved by the appropriate stakeholders. The OIG's recommendations align with our ongoing efforts to strengthen change management across the SEC, and we welcome continued collaboration as these improvements progress.

cc: Paul Knight, Chief Operating Officer
Shelly Luisi, Chief Risk Officer

Enclosure: Appendix A: Management Response to OIG Recommendations

Appendix A: Management Response to OIG Recommendations

The auditors recommended that the Office of Information Technology:

Recommendation 1: [redacted]

Response: Concur. [redacted]

Recommendation 2: [redacted]

Response: Concur. [redacted]

Recommendation 3: Update change control policies and procedures to ensure that emergency changes receive retroactive change control board review and approval.

Response: Partially Concur. Current practice already includes weekly review of Emergency, Urgent, and Non-compliant change requests by change management and senior operations leadership. Change requests that utilized the wrong type or did not follow the prescribed process are noted and addressed by senior operations management, with reports sent to OIT leadership. While OIT agrees with the need for strengthened oversight of emergency changes, we believe this existing governance structure appropriately manages retroactive reviews. To enhance transparency, OIT will update change control procedures to formally document this practice and will include a list of emergency changes in the weekly CCB agenda for review. Completion is targeted by March 2027.

Recommendation 4: Remind, and as needed, train the change request submitters and branch approvers about the proper use of emergency changes [redacted] for standard changes, and the expected timeframe for requester and branch acceptance of change requests after implementation.

Response: Concur. A training program is in place, requiring users to review change control training documentation and successfully complete a knowledge assessment before gaining access to the change control system. Training materials and user guides are provided, and automated alerts notify users of relevant procedures. To support closure of this recommendation, OIT will send periodic communications to reinforce proper use of emergency changes, [redacted] and timely acceptance of completed change requests. Evidence of two periodic awareness messages will be provided by March 2027.

Recommendation 5: Close change requests with implementation finish dates from 2025 and prior years.

Response: Concur. Closure activities for change requests with implementation finish dates from 2025 and prior years were underway before the audit. Completion is targeted by March 2027.

Recommendation 6: Update change request procedures to include expected timeframes for closing approved change requests and establish responsibility for regular monitoring of overdue change requests.

Response: Concur. OIT will establish and publish new guidelines for the timely closing of change requests and formally assign responsibility for regular monitoring of overdue requests. OIT plans to reduce the current 30-day closure window to improve timeliness and oversight. Completion of this task is planned by March 2027.

Recommendation 7: Implement control(s) [redacted]

Response: Partially Concur. While OIT agrees that [redacted] OIT will [redacted] and determine the most effective and risk-based approach by March 2027.

Recommendation 8: Update change control policies, procedures, and/or training materials to (a) specify the requirements for the format and types of testing information presented to SEC's change control boards, and (b) reinforce requirements for pre-release testing.

Response: Nonconcur. Existing policies, procedures, and training materials already specify testing requirements, documentation expectations, and pre-release testing requirements. All changes to the production environment must be tested unless an approved exception applies. These requirements are documented in the current training materials, the change management procedure, and the user guide. Project teams, as system subject-matter experts, are responsible for determining the format and type of appropriate testing, and testing results are required as an attachment to change requests that will be reviewed by change control board (CCB) members.

Recommendation 9: Review the capabilities of the SEC's enterprise change control tool and determine whether the agency could benefit from enabling functions related to test plans and testing information, then update applicable policies and procedures accordingly.

Response: Concur. OIT is reviewing the SEC's enterprise change control tool to identify whether additional test-related capabilities would benefit the agency. If so, OIT will update the applicable policies and procedures. Completion is planned by May 2027.

Recommendation 10: Determine which change control board member(s) should review test information as part of their predefined evaluation criteria.

Response: Nonconcur. Testing results are required for all changes unless they meet specific, pre-approved exceptions. These requirements are documented in the current training materials, change management procedure, and the user guide. Responsibility for reviewing testing results rests with the system or product owners, who have the necessary subject-matter expertise. The SEC's CCBs rely on these attestations and supporting documentation rather than independently reviewing testing information. This approach provides appropriate oversight, and additional specification of CCB member responsibilities is unnecessary.

Recommendation 11: Develop quality assurance procedures to ensure testing is performed when warranted and compensating controls are documented when needed.

Response: Concur. OIT will add further clarification on the change request form requiring submitter attestation that testing was completed and accepted by the system owner. Updates to the user guide and training materials will be made as needed. Completion is targeted by March 2027.

Recommendation 12: Coordinate with the change control boards to develop and document predefined evaluation criteria for each of the SEC entities represented.

Response: Concur. In March 2025, the SCCB implemented a self-attestable release process that included defined criteria that trigger SCCB review. OIT will require each CCB voting member to document evaluation criteria for assessing change requests and will ensure these criteria are accessible to stakeholders. Completion is targeted by May 2027.

Recommendation 13: In conjunction with the SEC's Records and Information Management Group, implement technical and procedural controls to ensure configuration management database records associated with configuration-controlled items and change requests are maintained in accordance with the SEC's records schedule and federal records retention requirements.

Response: Concur. OIT currently maintains procedures governing records retention and deletion approvals; however, to fully align with the recommendation, OIT will update configuration management database procedures and strengthen both technical and procedural controls, so that records associated with configuration-controlled items and change requests are maintained in accordance with SEC records schedule and federal records retention requirements. Completion is targeted by May 2027.

Recommendation 14: Develop procedures to maintain an inventory of configuration items that are unique and unambiguous.

Response: Concur. OIT will develop procedures to maintain an inventory of configuration items that are unique and unambiguous. Completion is targeted by May 2027.

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