U.S. SECURITIES AND
EXCHANGE COMMISSION

REPORT NO. 587

SEPTEMBER 3, 2025

OFFICE OF
INSPECTOR
GENERAL

Special Review: Avoidable Errors Led to the Loss of Former SEC Chair Gary Gensler's Text Messages

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

September 3, 2025

TO: Kenneth Johnson, Chief Operating Officer

FROM: Kevin Muhlendorf, Inspector General KEVIN MUHLENDORF Digitally signed by KEVIN MUHLENDORF Date: 2025.09.03 13:56:41 -04'00'

SUBJECT: *Special Review: Avoidable Errors Led to the Loss of Former SEC Chair Gary Gensler's Text Messages*, Report No. 587

Attached is the Office of Inspector General final report detailing the results of our special review of the loss of the former U.S. Securities and Exchange Commission (SEC) Chair Gary Gensler's text messages. The report contains five recommendations that should further strengthen the SEC's management of mobile devices and federal records.

On July 23, 2025, we provided management with a draft of our report for review and comment. In its August 22, 2025, response, management concurred with our recommendations and submitted planned corrective actions with timeframes. We have included management's response as Appendix II in the final report.

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

Attachment

cc: Paul S. Atkins, Chairman
Gabriel Eckstein, Chief of Staff, Office of Chairman Atkins
Mark Berman, Deputy Chief of Staff, Office of Chairman Atkins
Peter Gimbrere, Managing Executive, Office of Chairman Atkins
Hester M. Peirce, Commissioner
Benjamin Vetter, Counsel, Office of Commissioner Peirce
Caroline A. Crenshaw, Commissioner
Malgorzata Spangenberg, Counsel, Office of Commissioner Crenshaw
Mark T. Uyeda, Commissioner
Ivan V. Griswold, Counsel, Office of Commissioner Uyeda
Jeffrey Finnell, Acting General Counsel
Elizabeth McFadden, Deputy General Counsel General Law, Office of the General Counsel
Erik Hotmire, Director, Office of Public Affairs
Natalia Díez Riggin, Director, Office of Legislative and Intergovernmental Affairs
Shelly Luisi, Chief Risk Officer

Jim Lloyd, Assistant Chief Risk Officer/Audit Coordinator, Office of the Chief Risk Officer
David Bottom, Director/Chief Information Officer/Acting Chief Information Security Officer, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology
Olivier Girod, Director, Office of Support Operations
Raymond McInerney, Assistant Director of FOIA Services and Acting Assistant Director of Records Management Services, Office of Support Operations

EXECUTIVE SUMMARY

Special Review: Avoidable Errors Led to the Loss of Former SEC Chair Gary Gensler's Text Messages

REPORT NO. 587 | SEPTEMBER 3, 2025

WHY WE DID THIS REVIEW

Records are the foundation of open government, and electronic recordkeeping (including recordkeeping of text messages) helps ensure transparency, efficiency, and accountability.

On January 17, 2024, the U.S. Securities and Exchange Commission (SEC or agency) Office of Information Technology (OIT) reported to us that, about four months earlier, the agency erased nearly a year's worth of text messages sent and received by the then SEC Chair, Gary Gensler.

We undertook this review to determine what happened and why, how the agency responded, and any implications for federal records management.

AGENCY'S RESPONSE

Management concurred with our five recommendations and provided responsive corrective actions with estimated timeframes. The recommendations are resolved and will be closed upon verification of the actions taken. Management's complete response is reprinted in Appendix II.

WHAT WE FOUND AND RECOMMENDED

OIT's decisions and actions resulted in the inadvertent loss of text messages sent and received by Gensler between October 18, 2022, and September 6, 2023. Specifically, in August 2023 OIT implemented a poorly understood and automated policy that caused an enterprise wipe of Gensler's government-issued mobile device. The device was erroneously thought to be inactive and no longer in use, and OIT had not backed up the device for nearly a year. In an effort to recover from the enterprise wipe, OIT hastily performed a factory reset, which deleted text messages stored on the device and the device's operating system logs.

OIT's response to this incident culminated in a contractor-produced after-action report at an estimated cost of about $53,000. However, inadequacies in the report impacted its reliability and usefulness.

Furthermore, because OIT did not collect or maintain necessary log data, neither OIT, its contractor, nor we could determine why Gensler's device stopped communicating with the SEC's mobile device management system, which caused the device to appear inactive and led to the enterprise wipe. A series of additional OIT actions, deficiencies, and missed opportunities, including a lack of backups and procedures that failed to consider record retention requirements for Capstone officials (such as Gensler) exacerbated the situation and hindered the SEC's response.

Although the SEC took steps to recover or recreate the deleted text messages, the agency was unable to collect or determine the entire universe, including some federal records. Since notifying our office, the SEC has disabled text messaging agencywide (with some exceptions), notified the National Archives and Records Administration in June 2025 of the lost records, and taken additional steps to back up Capstone officials' records and data, among other actions. However, the loss of Gensler's text messages may impact the SEC's response to certain Freedom of Information Act requests.

While some matters we identified did not warrant recommendations, we are recommending specific actions to further strengthen the SEC's management of mobile devices and federal records. These actions include updating or developing plans, policies, and procedures related to change management, Capstone officials' devices, and the system used to manage mobile devices, among other topics.

Contents

Abbreviations

AAR	after-action report
CIO	Chief Information Officer
COO	Chief Operating Officer
FOIA	Freedom of Information Act
FOIA Services	Office of Freedom of Information Act Services
NARA	National Archives and Records Administration
OIG	Office of Inspector General
OIT	Office of Information Technology
ORMS	Office of Records Management Services
SEC or agency	U.S. Securities and Exchange Commission

Background and Objectives

BACKGROUND

What is a Federal Record and Why Are Records Important? Records are the foundation of open government. They document agency actions and decisions, protect the rights and interests of people, and can be used to assess program impacts, reduce costs, and share knowledge across the Government.[1] Electronic recordkeeping by federal agencies can also help ensure transparency, efficiency, and accountability.[2]

Records include:

> [A]ll recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. . .[3]

For the purpose of federal recordkeeping, "electronic messages" are email and other electronic messaging systems used to communicate between individuals.[4] Among other things, they include text messages. Regardless of format, the head of each federal agency must make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency, and must generally ensure effective controls over those records.[5]

Relevant Roles and Responsibilities at the SEC. The U.S. Securities and Exchange Commission's (SEC or agency) Office of Records Management Services (ORMS) ensures that the SEC complies with federal laws regarding records creation, maintenance, and disposition. ORMS also meets with divisions and offices as needed to provide guidance on proper records scheduling and retention, while offering records management training throughout the agency. Additionally, the SEC's Office of Freedom of Information Act Services (FOIA Services) receives and responds to requests for nonpublic records made under the Freedom of Information Act (FOIA) and the Privacy Act.

The SEC's Office of Information Technology (OIT) supports the Commission and staff of the SEC in all aspects of information technology. Among other responsibilities, OIT manages the SEC's government-

[1] Presidential Memorandum, *Managing Government Records*; November 28, 2011. *See also* Office of Management and Budget, M-12-18, *Managing Government Records Directive*; August 24, 2012; pg. 1.

[2] M-12-18; pg. 3.

[3] Federal Records Act of 1950, as amended, Pub. L. 81-754, 64 Stat. 583 (Sept. 5, 1950); 44 U.S.C. § 3301(a)(1)(A). Records do not include library and museum material made or acquired and preserved solely for reference or exhibition purposes, or duplicate copies of records preserved only for convenience. 44 U.S.C. § 3301(a)(1)(B)(i) and (ii).

[4] 44 U.S.C. § 2911(c)(1).

[5] 44 U.S.C. §§ 3101; 3102(1).

issued mobile devices, which are relevant to the agency's records management concerns given today's mobile environment.[6]

To fulfill its responsibilities with respect to mobile devices, OIT (with the help of contracted subject matter experts) used a mobile device management system, which provided security, application management, and remote system administration and allowed OIT to remotely wipe devices using either an "enterprise wipe" or a "factory reset."[7] An enterprise wipe partially wipes a device by removing the content controlled by the SEC, which does not include text messages. A factory reset is more destructive and removes all device content (e.g., text messages, operating system logs, etc.), returning the device to its factory state.

Additionally, various branches and individuals within OIT carry out the SEC's mobile device policy, identify users with inactive devices, establish and execute monitoring activities (including logs of certain data), and remediate vulnerabilities. Finally, OIT's Security Operations Center provides investigative and mitigation support and the SEC's primary incident response capability.

SEC employees also play a role in ensuring effective records management and mobile device management. For example, employees must complete mandatory records management training, must not conduct SEC business using personal email accounts or other non-federal electronic messaging systems (e.g., instant, chat, or text messaging services), and must ensure requirements have been met before destroying records.[8] Employees must also adhere to privacy and information security awareness training and guidance and must timely update their government-issued mobile device to the latest operating system as instructed by OIT.[9]

The SEC's "Capstone" Approach. To comply with federal records requirements from the Office of Management and Budget and the National Archives and Records Administration (NARA), in October 2016 the SEC implemented a "Capstone" approach for managing email records of senior agency officials.[10] This required permanent retention of about 200 Capstone officials' accounts.[11]

In October 2022, the SEC expanded its approach to retain Capstone officials' text messages. As part of this effort, OIT provided SEC's Capstone officials with new mobile devices and retained their old devices for recordkeeping purposes. Then, in March 2024, the Chief Information Officer (CIO) announced that

---

[6] At the time of our review, OIT managed about 5,700 government-issued mobile devices.

[7] During the summer of 2024, OIT replaced the mobile device management system discussed in this report. The SEC's new mobile device management system provides similar capabilities.

[8] SEC Administrative Regulation SECR 7-1, *Records and Information Management Program*; August 3, 2021.

[9] OIT's *[Operating System] Update Via the Mobile Device Manager Operating Procedure*; February 13, 2023.

[10] According to NARA Bulletin 2013-02, *Guidance on a New Approach to Managing Email Records*; August 29, 2013, "Capstone offers agencies the option of using a more simplified and automated approach to managing email, as opposed to using either print and file systems or records management applications that require staff to file email records individually. Using this approach, an agency can categorize and schedule email based on the work and/or position of the email account owner. The Capstone approach allows for the capture of records that should be preserved as permanent from the accounts of officials at or near the top of an agency or an organizational subcomponent."

[11] The SEC's Capstone officials include the Chairman, the Commissioners, and their staff; the agency's division directors, their deputies, and their chief counsels; the heads of designated program offices and their chief counsels; the General Counsel and the General Counsel's deputies; principal regional officials; and other designated federal employees and political appointees serving in equivalent or comparable positions.

OIT would coordinate with Capstone officials to back up their new devices. Most SEC Capstone officials' text messages had not been backed up since October 2022; therefore, if a Capstone official's device was factory reset or a backup was unsuccessful, the agency risked losing more than a year of text message records.

OBJECTIVES

We initiated this review upon being notified that OIT had inadvertently erased nearly a year's worth of text messages sent and received by the then SEC Chair, Gary Gensler (Gensler) when OIT factory reset his government-issued mobile device (hereinafter, "device" or "smartphone"). We sought to determine what happened and why, how the agency responded, and any implications for federal records management.

Appendix I of this report includes additional information about our scope, methodology, and prior coverage.

Results

1. WHAT HAPPENED AND WHY

On July 6, 2023, Gensler's smartphone stopped communicating with the SEC's mobile device management system. Although the device otherwise functioned normally and was used regularly, for 62 days it showed up as "inactive" within the system (a condition that went unnoticed by OIT personnel). On August 10, 2023, OIT instituted a new policy of remotely wiping any SEC mobile device that did not communicate with the mobile device management system for at least 45 days. This new policy was based on the erroneous assumption that such devices were not in use, were potentially lost or stolen, and could no longer connect to the SEC's network.

On the morning of September 6, 2023, when Gensler arrived at the SEC Headquarters building, he noticed that SEC applications were missing from his smartphone and he sought help from OIT personnel. Unbeknownst to Gensler and the OIT personnel who initially assisted him that morning, his smartphone had been wiped pursuant to the new policy.[12] Although the smartphone had been wiped, it would have been possible at that point to retain Gensler's text messages. However, in an effort to assist Gensler expeditiously, OIT personnel hastily performed a factory reset of the smartphone, which resulted in the permanent deletion of the device's data, including nearly a year's worth of text messages. As further described below, OIT failed to:

- ensure proper change management;
- properly maintain its mobile device inventory and identify inactive devices;
- effectively review and escalate relevant system-generated notifications;
- identify and address known vendor product flaws; and
- timely back up Gensler's text messages, or remove the texting application from SEC devices.

1a. OIT Did Not Ensure Proper Change Management with Respect to Its Mobile Device Management System

In July 2023, OIT implemented an automated policy—through an emergency change—that resulted in sending multiple emails to SEC Capstone officials regarding government-issued mobile devices.[13] The emails notified the officials that their devices would soon lose network connection if certain steps were not taken. However, the devices in question had already been turned in and were no longer in use. In response to complaints about these numerous inaccurate emails, OIT implemented another new policy—again, through an emergency change—to automatically issue an enterprise wipe to any SEC mobile device that had not communicated with the agency's mobile device management system within 45 days,

[12] Gensler's smartphone appears to have been the only active SEC device wiped as a result of this policy.

[13] OIT's *Change Management Process Operating Procedure* states, "To qualify as an Emergency, a change must require immediate implementation to rectify a service outage, imminent outage, or a severe decrease in performance." Compared to other types of changes (e.g., "standard" and "urgent"), emergency changes require approval at a lower level. OIT acknowledged that, in hindsight, the change in question did not qualify as an emergency as defined.

reasoning that such action would address OIT's concerns with the old devices. OIT's *Change Management Process Operating Procedure* states, in part, that the change management process ensures all changes are adequately described, reasons for changes are appropriately documented, and the business and technical impact of the changes are thoroughly assessed. However, OIT failed to first assess the impact and risks of its new, admittedly "aggressive" 45-day wipe policy or consider Capstone record retention requirements.[14] Thus, OIT was unprepared to respond to the situation with Gensler's smartphone.

1b. OIT Did Not Follow Its Procedures to Maintain Its Mobile Device Management System Inventory and Identify Inactive Devices

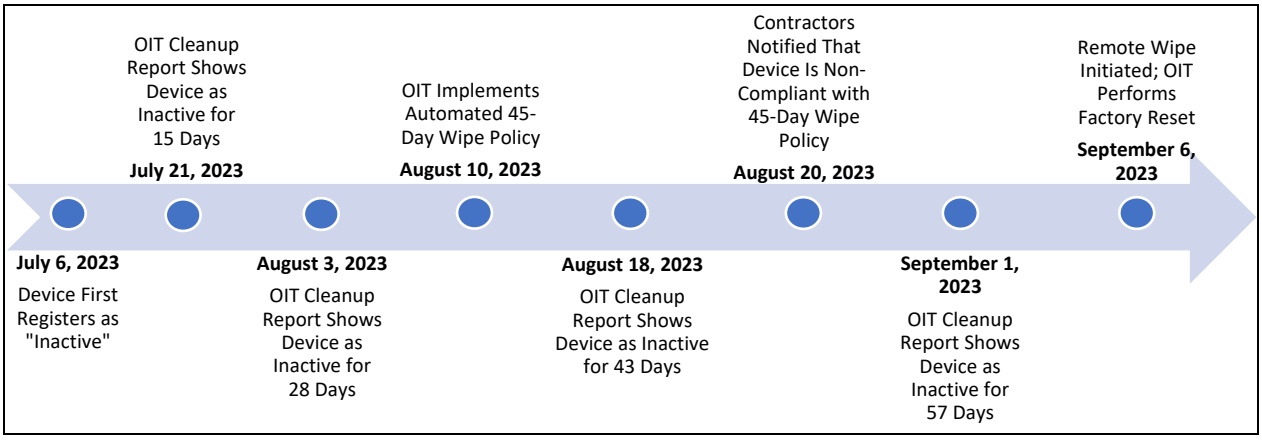
OIT defined procedures to identify, report on, and address devices registering as inactive (that is, no longer communicating with the SEC's mobile device management system). In fact, about every two weeks before being wiped, Gensler's smartphone showed up as inactive in mobile device management "cleanup" reports dated July 21, 2023; August 3, 2023; August 18, 2023; and September 1, 2023. Nonetheless, OIT took no action to investigate or effectively resolve the matter, which could have prevented the enterprise wipe of Gensler's device on September 6, 2023.

1c. OIT Did Not Have an Effective Process to Review and Escalate Mobile Device Management System Notifications

In addition to showing up as inactive in at least four cleanup reports, Gensler's device was the subject of an automated email sent by the SEC's mobile device management system to OIT contractor personnel more than two weeks before the device was wiped. The email was to alert OIT that the device was registering as inactive. Despite this, contractor personnel took no action to review or escalate the matter, stating they received many emails at that time and it was overlooked. Had OIT established processes with its contractor to triage and respond to system-generated notifications, particularly those involving SEC Capstone officials, actions could have been taken to prevent Gensler's device from being wiped.

Responsible officials and OIT contractor personnel acknowledged the multiple oversights and missed opportunities to prevent the wiping of Gensler's device.

FIGURE 1. Timeline of Significant Events Leading to the Loss of Gensler's Text Messages



Source: Office of Inspector General (OIG)-generated based on data obtained from OIT.

[14] In light of this and other change management concerns, the OIG has begun an audit of the SEC's change control process.

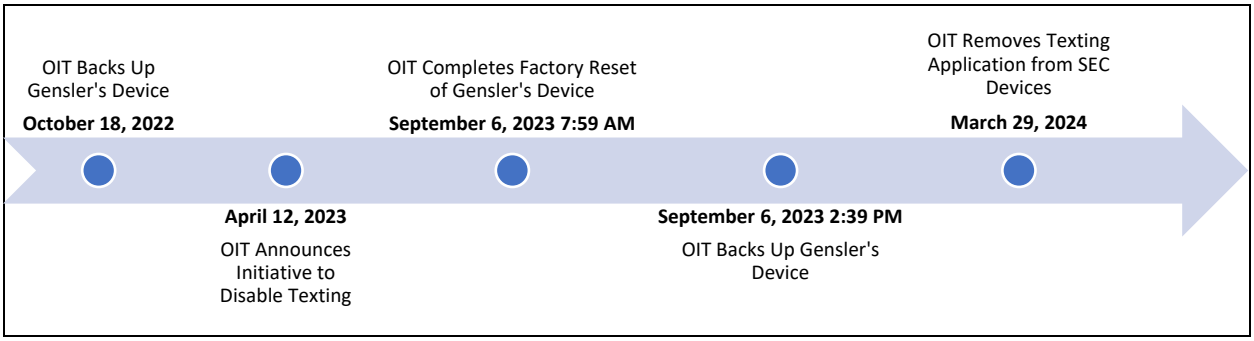
1d. OIT Did Not Have a Process to Identify and Address Known Vendor Product Flaws

The SEC's mobile device vendor knew of a "bug" in prior versions of its operating system that could break the connection between a mobile device and a mobile device management system. However, OIT did not have a process to coordinate with vendors to understand and track known technical risks. Had OIT been aware, effective compensating controls could have been developed to detect devices, such as Gensler's, that lost communication with the mobile device management system and were wrongly deemed inactive. Furthermore, if this technical flaw in the mobile device operating system persists, it could have security implications if OIT is unable to timely perform remote wipes of lost or stolen SEC mobile devices due to a break in communication between the devices and the mobile device management system.

1e. OIT Had Not Backed Up Gensler's Text Messages for Nearly a Year, and Did Not Timely Remove the Texting Application from SEC Devices

In October 2022, OIT initiated a process to collect and retain electronic records, including text messages, for all SEC Capstone officials in accordance with federal guidance, and OIT backed up Gensler's smartphone on October 18, 2022. On April 12, 2023, OIT announced an initiative to remove the texting application from SEC mobile devices to "promote better recordkeeping practices," and requested that SEC personnel stop using the texting application. OIT formally prohibited text messaging on SEC devices in a July 31, 2023, update to relevant SEC administrative regulations. However, OIT postponed enforcing the prohibition until the agency could establish a process for granting exceptions. The prohibition was also delayed due to a potential government shutdown. In the meantime, OIT did not back up Gensler's smartphone again. Thus, when Gensler's device was factory reset on September 6, 2023, text messages from October 18, 2022, to September 6, 2023, were lost. OIT backed up Gensler's smartphone on the afternoon of September 6, 2023, but by then the device had been factory reset and the missing data could not be recovered. OIT eventually removed the texting application from SEC devices in March 2024.[15] Had OIT timely backed up his device and completed its initiative to promote better recordkeeping practices as initially planned, Gensler's text messages would not have been at risk of loss on September 6, 2023.

FIGURE 2. Timeline of Decisions Regarding Text Messaging at the SEC and Backups of Gensler's Device



Source: OIG-generated based on data obtained from OIT.

[15] Certain SEC personnel have been granted exceptions and still have the texting application on their smartphones.

Leading up to the removal of the texting application from SEC devices, the CIO stated in a March 6, 2024, memorandum, "OIT will coordinate directly with those senior agency officials designated as Capstone officials to make a soft copy of their [mobile devices] before the [texting application] is removed from their devices." Although OIT removed the texting application on March 29, 2024, OIT was still in the process of obtaining and backing up text messages from about 50 Capstone officials in September 2024. In addition, OIT was unable to successfully back up the mobile devices used by about 40 other Capstone officials. As a result, the text messages stored on these SEC devices are at greater risk of loss or may have already been lost.

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

We recommend that OIT:

Recommendation 1:

Update policies and procedures to ensure that OIT (a) thoroughly documents and understands changes to the SEC's mobile device management system before such changes are implemented; (b) maintains an accurate inventory of mobile devices enrolled in the SEC's mobile device management system (including timely follow-up and removal of inactive devices); (c) reviews and escalates mobile device management system notifications involving Capstone officials' devices; and (d) regularly obtains and, as necessary, responds to information about technical risks from vendors whose products may impact the SEC's mobile devices.

> **Management's Response.** Management concurred with the recommendation, stating that the SEC will update OIT policies and procedures to require that (a) the SEC's mobile device management system changes are documented before implementation, (b) an accurate inventory of mobile devices enrolled in the SEC's mobile device management system is maintained, (c) mobile device management system notifications involving Capstone officials' devices are reviewed and escalated, and (d) reviews of vendor release notes about technical risks impacting the SEC's mobile devices are performed. Management plans to complete these actions by December 2025. 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 action taken.

Recommendation 2:

Ensure that all SEC Capstone officials' devices were backed up at the time OIT removed the texting application from SEC devices, and (for each device) document the date OIT verified that all electronic records, including text messages, were successfully saved (as of the October 2022 Capstone initiative and with each subsequent backup). If text messages from any Capstone officials' devices were not successfully saved, work with ORMS to determine if NARA notification is required.

Management's Response. Management concurred with the recommendation, stating OIT will review its records to confirm that all Capstone officials' devices were backed up, the date on which this occurred, and that text messages from these backups are accessible. Management plans to complete these actions by December 2025. In addition, as of July 29, 2025, the SEC reported to NARA the potential loss of federal records from 21 devices. 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 action taken.

2. THE SEC'S RESPONSE

By the end of the day on September 6, 2023, OIT had disabled its 45-day wipe policy and initiated the first steps of an investigation into the events surrounding Gensler's smartphone and the loss of text messages he sent and received. The following week, OIT directed a contractor to broaden the scope of the investigation beyond Gensler's device. Federal information security standards and SEC policy require the SEC to collect and retain adequate logs and other information to support such after-the-fact investigations.[16] Because OIT did not collect or retain the necessary logs, neither the SEC, its contractor, nor we could determine why Gensler's smartphone stopped communicating with the agency's mobile device management system in the first place, and the agency's response overall was hindered.[17] Furthermore, OIT's response led to an after-action report (AAR), dated December 6, 2023, that 12 contractor employees produced at an estimated cost of about $53,000.[18] In addition to the contracting officer's representative, eight OIT employees oversaw this action. However, inadequacies in the AAR impacted its reliability and usefulness.

The sections that follow further describe these matters.

2a. OIT Did Not Ensure Mobile Device Management Console Logs Were Forwarded as Intended

The SEC's mobile device management system security plan in place at the time (dated June 13, 2023) stated, "Application log forwarding is enabled. Logs are sent to [the security information and event management tool]," which is used to aggregate and retain logs across the SEC's network and provides centralized monitoring and alerting. However, OIT did not begin consistently forwarding the logs until July 18, 2023 (about two weeks *after* Gensler's smartphone lost communication with the mobile device management system). Therefore, key system-level logs were not available to assist the SEC once it was discovered that Gensler's device had lost connection and had been wiped.

2b. Troubleshooting Activities Resulted in the Deletion of Device and Operating System Logs

While trying to restore Gensler's smartphone on the morning of September 6, 2023, OIT personnel took actions that caused a factory reset of the device without first making a backup or explicitly seeking OIT management approval. This action deleted all local device and operating system logs, which could have been useful in investigating why the device stopped communicating with the mobile device management system in the first place.

---

[16] National Institute of Standards and Technology Special Publication 800-53, Rev. 5; and the SEC's *Information Security and Privacy Controls Manual* and mobile device management system security plan.

[17] The lack of mobile device logs was previously brought to OIT's attention during the OIG's 2020 mobile device audit and during a January 2023 Security Operations Center investigation involving another SEC mobile device.

[18] OIT officials stated that this cost was calculated based on hours of effort multiplied by the individual contractors' hourly rates. The AAR was not a separate deliverable under the contract.

2c. The Security Operations Center's Assessment of Potential Malicious Activity Was Hindered

The lack of log data hindered the SEC Security Operations Center's ability to determine whether malicious activity took place when Gensler's smartphone stopped communicating with the agency's mobile device management system. OIT security officials and other personnel acknowledged that they did not have all the data needed to perform a thorough assessment. In addition—despite its role as the SEC's primary incident response capability—the Security Operations Center was not initially given key information from the investigation conducted by SEC contractors and vendors.

2d. Inadequacies in the AAR Impacted Its Reliability and Usefulness

Deficient Reporting of a Critical Date. The purpose of the AAR was to "review the reason(s) that SEC [mobile devices] did not check into the [mobile device management] console." However, the AAR erroneously calculated that Gensler's smartphone stopped communicating with the SEC's mobile device management system on July 23, 2023. The device actually lost connection 17 days earlier on July 6, 2023.[19] When we notified the Security Operations Center of the correct date (which we identified by reviewing mobile device management system reports containing contemporaneous data), OIT officials and responsible personnel acknowledged that their investigation did not focus on the events leading up to July 6, 2023, because they did not realize the importance of that date.

Unexplained Discrepancy in Timing. The AAR states that an enterprise wipe was executed on Gensler's smartphone because of a new OIT policy regarding inactive devices (that is, devices no longer communicating with the mobile device management system for a period of 45 days). However, the AAR does not explain why the wipe did not take place until 62 days after the device stopped communicating with the mobile device management system. The AAR states, "Efforts are still ongoing to determine why the Chair's phone reinstated communication with the console after not checking in for 45+ days." When we followed up, OIT management was still unable to explain this issue.

Incomplete Information on Mobile Device Operating System Versions. The AAR cites a flaw in smartphone operating system versions—previously unknown to the SEC's contracted subject matter experts—as a possible reason that Gensler's device stopped communicating with the SEC's mobile device management system. However, the device was not running one of the operating system versions in question when it lost communication. In follow-up, OIT management was unable to explain this discrepancy.

Citations to Inaccurate or Incomplete Standard Operating Procedures. The AAR states, "The following [standard operating procedures] are followed by the Remote Access Team," yet the embedded procedures were either out-of-date or incomplete. When asked about this, one of OIT's contracted subject matter experts acknowledged that even the name "Remote Access Team" was outdated and no longer used. The same subject matter expert stated that there has since been a concerted effort to ensure all policies and standard operating procedures are current and followed by the teams involved.

---

[19] Similarly, when OIT notified the OIG of the issue, the CIO stated that "in late July 2023" Gensler's smartphone stopped communicating with the SEC's mobile device management system.

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

We recommend that OIT:

Recommendation 3:

Update the applicable system security plan(s) to accurately reflect the mobile device management system audit events and logs that should be forwarded to the SEC's security information and event management tool, and ensure that those logs support after-the-fact investigations of incidents.

Management's Response. Management concurred with the recommendation, stating the SEC will update the applicable system security plans to identify auditable events and logs that should be forwarded to the SEC's security information and event management tool to support after-the-fact investigations of incidents. Management plans to complete these actions by March 2026. 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 action taken.

Recommendation 4:

Develop procedures to periodically verify that the mobile device management system audit events and logs identified in the applicable system security plan(s) are successfully retained in the SEC's security information and event management tool.

Management's Response. Management concurred with the recommendation, stating the SEC will update its procedures to include processes for reviewing and retaining mobile device management audit events and logs. Management plans to complete these actions by March 2026. 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 action taken.

Recommendation 5:

Update policies and procedures to require OIT management's approval of commands during troubleshooting activities that result in a factory reset of Capstone officials' devices, and verification that appropriate device logs and forensic data have been collected and retained beforehand.

Management's Response. Management concurred with the recommendation, stating the SEC will update its policies and procedures to require OIT management's approval of commands during troubleshooting activities that result in a factory reset of Capstone officials' devices and verify that appropriate device logs and forensic data have been collected and retained beforehand. Management plans to complete these actions by November 2025. 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 action taken.

3. IMPLICATIONS FOR FEDERAL RECORDS

In an effort to recover the text messages deleted from Gensler's smartphone, the agency employed multiple methods, including both forensic and less-technical approaches. However, these methods were not entirely successful, and the SEC was unable to recover or determine the entire universe of missing text messages. Moreover, our review determined that the text messages recovered as of October 2024 included federal records, and those messages that remain missing likely do as well.

3a. Overview of the SEC's Deleted Text Message Recovery Efforts

In the months following the deletion of Gensler's text messages, both OIT and the Division of Enforcement IT Forensics Lab attempted to recover the missing data through forensic means but were unsuccessful. The OIG was unable to conduct an independent forensic examination of the smartphone because OIT returned it to the vendor on January 8, 2024, before the OIG was notified of the incident.[20]

The SEC then attempted to recreate the messages through a more manual process. OIT reviewed a report of phone numbers that exchanged SMS text messages[21] with Gensler's smartphone and created a spreadsheet to map those numbers to certain SEC and non-SEC issued numbers. This process allowed OIT to identify, collect, and copy data from a handful of agency employees. In addition, Gensler's office identified two non-SEC federal officials from the non-SEC numbers, and the agency obtained screenshots of 49 text exchanges between Gensler and these officials.

Gensler's staff also compiled a list of 34 agency employees with whom they predicted he texted most frequently. OIT collected these employees' smartphones and extracted any retrievable text messages exchanged with Gensler during the relevant period. This recovery effort was not all-inclusive; for example, Gensler did not provide input into the list, and the original list did not include his fellow Commissioners.[22] Gensler's staff acknowledged that the list was "meant to be a floor, not a ceiling," and their effort could not identify and/or recover all missing text message exchanges.[23]

With respect to his texting habits, Gensler and his staff explained that he usually texted for administrative reasons such as scheduling calls, meetings, or transportation. However, our review found multiple instances of substantive, mission-related communications between Gensler, his staff, his fellow Commissioners, and other senior officials, adding an additional layer of uncertainty to the effectiveness of the recovery process and the exact nature of the text messages that remain missing.

---

[20] Based on the information it was able to obtain, the OIG's Digital Forensics Investigations Unit concurred that it was unlikely the deleted text messages could be recovered following the device's wipe and subsequent factory reset.

[21] The mobile device vendor could provide no information for texts sent and received through the mobile device texting application. Because the SEC used this texting application at the time, the information the vendor provided was of limited value in recreating a list of contacts with whom Gensler texted. The report also included a small number of picture/video messages and a few text messaging numbers that Gensler's office identified as "spam."

[22] We requested and subsequently received, reviewed, and analyzed the text messages from the other Commissioners as potential records.

[23] Among the text messages yet to be recovered are those that may have been exchanged between Gensler and a former SEC Office of Public Affairs employee. According to OIT, multiple passcodes provided by the former employee were ineffective, and the Division of Enforcement IT Forensics Lab was also unable to access the data on the former employee's device.

3b. Recovered Text Messages We Reviewed Included Agency Records

We reviewed and analyzed about 1,500 recovered text messages to determine whether they included federal records.[24] Based on (1) the Federal Records Act, (2) applicable federal regulations, (3) NARA guidance, and (4) the position taken by ORMS during a meeting with the OIG and upon reviewing a sample of recovered text messages, we believe the majority of the text messages we reviewed are SEC records. Furthermore, based on our review and analysis, we believe it is likely that the majority of missing text messages are agency records as well.

Under the Federal Records Act, a "record" includes all recorded information, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business. Federal regulations have applied this definition to electronic messages;[25] and NARA Bulletin 2023-02 provides that electronic messages, including text messages, created or received during the normal course of agency business are likely records. Consistent with NARA and federal regulations, ORMS has issued guidance that SEC employees' electronic communications are federal records unless personal. SEC Capstone officials—like Gensler—are subject to additional recordkeeping requirements, including the permanent preservation of their records, because of their position "at or near the top of an agency or an organizational subcomponent."[26] Taken together, federal law, regulations, NARA guidance, and agency policy support our conclusion that most of Gensler's recovered text messages are federal records.

For the purposes of our review, we characterized Gensler's text messages as logistical/administrative, mission related, or personal. The logistical/administrative text messages typically involved day-to-day operations of Gensler and his staff, such as scheduling meetings and calls, missed calls, dealing with information technology-related issues, and arranging for transportation. These text messages seldom communicated substantive, mission-related information but are, nonetheless, federal records because they were made or received by Gensler (the former SEC Chair) in connection with the transaction of public business.[27] Our review determined that around 56 percent of the recovered texting conversations with Gensler were logistical/administrative. We provided ORMS officials with representative samples of these text messages and they confirmed that, "Given that the samples you have provided are related to the official business of Capstone-level officials of the SEC, ORMS posits that these would be considered records which would require preservation."

Our review also determined that around 38 percent of the recovered text conversations were mission related and concerned matters directly involving SEC senior staff and/or Commissioners at the time, making them records. Examples include:

---

[24] Approximately 200 text message "bubbles" contained no actual text message and could not, therefore, be reviewed for record status.

[25] 36 C.F.R. § 1220.18.

[26] NARA Bulletin 2013-02. *See also*, *Capstone Approach for Managing Electronic Messages – FAQs* (January 2025).

[27] 44 U.S.C. § 3301(a)(1)(A).

- A May 2023 conversation involving Gensler, his staff, and the Director of the Division of Enforcement about when the SEC would be filing an action against certain crypto asset trading platforms and their founder.
- A May 2023 conversation involving the Office of International Affairs Director and Deputy Director regarding a series of subjects—ranging from crypto to climate—on which Gensler would be speaking.
- A June 2023 conversation with a Commissioner concerning a proposed Division of Enforcement settlement with a leading global financial services firm.
- A June 2023 text message from Gensler to a Commissioner regarding White House Presidential Press Office plans to announce the appointment of a fellow Commissioner.
- A July 2023 conversation with a Commissioner regarding an upcoming meeting with the White House.

We determined that the remaining six percent of the recovered text conversations qualified as personal and thus were not federal records.[28]

Although we cannot review the missing text messages to definitively determine their status as records, we can surmise based on our review of the recovered text messages that many, if not most, would be records.

3c. Additional Records Management Issues Existed

Our review uncovered the following additional SEC records management issues: (1) the lack of specialized training for Capstone officials, including Gensler; (2) the agency's four-month delay in notifying our office of the loss of Gensler's text messages; and (3) the agency's decision not to notify NARA of the loss of records until we completed our review.[29]

Specialized Training for Capstone Officials. At the time Gensler's device was wiped and text messages lost due to the factory reset, there was no specialized records management training in place for Capstone officials. Rather, Capstone officials were assigned the same online training offered to all SEC staff, which did not address their additional recordkeeping requirements. Gensler told us that he takes records management "very seriously" and considers records "an important part of government." He acknowledged that his understanding of records management at the SEC came from (1) training he received upon his arrival at the agency, (2) taking the annual SEC-wide online training, and (3) his prior federal government experience. None of these were SEC Capstone-specific. During our review, in May 2024, the SEC developed and launched Capstone-specific training entitled "The Capstone Approach at the SEC," which consists of an 11-minute video providing "Capstone officials with an overview of the

[28] 36 C.F.R. § 1220.18 (personal files are excluded from the definition of "federal records").

[29] Upon learning of the existence of our review, the SEC's new Chairman, Paul Atkins, immediately directed the agency to notify NARA.

Capstone approach, including its creation and implementation at the SEC and resources for Capstone officials."[30] All SEC Capstone officials must complete this training annually.

The SEC's Four-Month Delay Before Notifying the OIG. On January 17, 2024, the SEC's CIO notified our office that Gensler's smartphone had been wiped and then factory reset, erasing his text messages spanning October 2022 to September 2023. This notification occurred more than four months after the agency first learned of the incident. Accounts of when the decision was made to notify our office, and by whom, vary. The Chief Operating Officer (COO) believed that he discussed the idea of referring the matter to our office with Gensler's Operations Counsel on January 9, 2024, just over a week before we were notified. Gensler's Operations Counsel largely agreed with this account, although details regarding the date of the actual meeting and its attendees are unclear.[31] The COO recalled that, after the meeting, he asked the CIO to put together a briefing package for the OIG. The CIO told us that he believed it was his decision to notify our office and the delay was due to the time it took his office to complete their review of the incident. Nonetheless, our review uncovered no evidence that the delay in notification resulted from an effort to conceal what had occurred from the OIG. Rather, the CIO noted that the smartphone wipe and subsequent reset was considered an information technology issue initially and not something that would rise to the level of an OIG referral.

Notification to NARA. The Federal Records Act requires federal agencies to notify NARA "of any actual, impending, or threatened unlawful . . . deletion of records in the custody of the agency . . . ."[32] During our review, ORMS told us that the SEC would not notify NARA of the lost records until after we concluded our review, noting that this stance was "in keeping with agency practice of not interfering with the work of [the] OIG." ORMS maintained that Gensler's office was aware of this stance and NARA had raised no concerns about this practice in the past. On June 23, 2025, we briefed Chairman Atkins regarding our findings in this matter, and we issued a discussion draft report on June 24, 2025. On June 27, 2025, the SEC notified NARA of the lost records.

[30] 2024-05-28 Capstone Training (sec.gov)

[31] Gensler told us he did not participate in any discussions regarding OIG notification.

[32] 44 U.S.C. § 3106(a). *See also* applicable federal regulations requiring agencies to "report promptly any unlawful or accidental removal, defacing, alteration, or destruction of records in the custody of that agency to NARA . . . ." 36 C.F.R. § 1230.14.

Other Matters of Interest

During our review, we identified additional matters regarding (1) the SEC's process for responding to FOIA requests that may include text messages, and (2) risk that may be introduced by removing the texting application from SEC devices. Although we are not making recommendations, we discussed these matters with SEC management and encourage management to consider taking actions to resolve these concerns.

Potential Impact of Lost Text Messages on FOIA Requests

On April 22, 2024—seven months after Gensler's text messages were erased—the Office of the COO informed FOIA Services of the deleted text messages and the SEC's efforts to recover them. On June 4, 2024, OIT provided FOIA Services access to the deleted text messages that had been recovered so that FOIA Services could determine whether the text messages were responsive to any FOIA requests. We reviewed FOIA requests for which Gensler's lost texts could have been responsive. Of the requests we reviewed, six percent remained open as of June 2025. We also assessed the circumstances under which searches of Gensler's text messages occurred in response to FOIA requests and the roles of the various offices involved. We observed the following:

- Before removing the texting application from SEC devices, OIT and/or Gensler's office searched Gensler's text messages in response to applicable FOIA requests. Now that the application has been removed, only OIT performs these searches.
- OIT only searches text messages when FOIA Services specifies that texts should be searched. Therefore, although FOIA requests are to be interpreted broadly,[33] whether OIT performs these searches could depend on a FOIA specialist's determination of whether "all emails or other communications" or similar request language includes text messages.
- Internal FOIA guidance did not clearly state how to interpret a request for a broad term such as "communications." We identified one matter where a FOIA specialist interpreted a request for "all emails or other communications" as *not* to include text messages, so OIT did not search for responsive texts.
- We reviewed closed FOIA requests submitted after September 6, 2023, to which Gensler's lost text messages could have been responsive. OIT confirmed that his text messages were not searched in these instances, and they found no record that FOIA Services requested such a search. This was true even though "all emails or other communications" and "any communications" were requested.
- Federal regulations require that FOIA Services notify a requester of an adverse determination in response to a FOIA request, including if "the requested record does not exist . . . cannot be

[33] *See, e.g., Coffey v. BLM*, 277 F. Supp. 3d 1, 8 (D.D.C. 2017) ("[T]he Court notes that an agency has a duty to construe FOIA requests liberally . . . ."), citing *Nation Magazine v. United States Customs Service*, 71 F.3d 885, 890 (D.C. Cir. 1995).

located, or has previously been destroyed . . . ."[34] Because no text message searches were performed for the closed matters we reviewed, there was no adverse determination triggering the requirement to notify requesters.

Although the SEC has removed the texting application from its government-issued devices, past text messages and any exceptions granted to its prohibition on texting could still yield messages that are responsive to FOIA requests. The SEC's FOIA Services should consider providing guidance to its FOIA specialists to ensure they consistently interpret whether requests for "communications" include searching text messages. Furthermore, for FOIA requests that remain open and as federal regulations require, requesters should be appropriately notified of lost text messages whenever those messages would have been searched in response to the request.

OIT's Removal of the Texting Application from SEC Devices May Introduce New Risk to Records Management

As previously stated, OIT removed the texting application from SEC devices in March 2024. The agency encouraged employees to use an alternative instant messaging application installed on SEC devices instead. The CIO stated that doing so promotes better recordkeeping practices and enhances protections around nonpublic, confidential information. However, the instant messaging application has some limitations, including only allowing messaging between SEC devices. NARA recommends that agencies provide employees with appropriate tools to complete their work, adding that simply prohibiting the use of electronic messaging (including text messaging) to conduct agency business "is difficult to enforce and does not acknowledge the ways employees communicate."[35] Furthermore, NARA states that "[a]gencies run the risk of employees conducting business on personal accounts when they do not provide these tools."

We encourage OIT and ORMS to consider whether prohibiting the use of text messaging (except in very limited circumstances) and removing the texting application from SEC devices has unintentionally introduced new risk of agency personnel conducting business through unauthorized channels, as described by NARA. OIT and ORMS should also consider determining whether compensating controls effectively minimize this risk.

[34] 17 C.F.R. § 200.80(e)(2)(iii).

[35] National Archives and Records Administration, *Guidance on Managing Electronic Messages* (Bulletin 2015-02; July 29, 2015).

Appendix I. Scope and Methodology

We performed our fieldwork between January and October 2024 pursuant to the Pandemic Response Accountability Committee's *Agile Products Toolkit* (November 2020) and the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspector General* (August 2012).

Objectives and Scope

Our review focused on Gensler's government-issued mobile device and actions taken by the SEC leading up to and in response to the September 6, 2023, factory reset of that device. We also reviewed Gensler's text messages from October 2022 through September 2023 that the SEC was able to recover or recreate. We undertook this review to determine what happened and why, how the SEC responded, and any implications for federal records management.

Methodology

To address our objectives, among other work performed, we (1) reviewed actions taken leading up to and in response to the September 6, 2023, factory reset of Gensler's mobile device; (2) interviewed SEC and contractor personnel from OIT, ORMS, FOIA Services, the Office of the COO, and Gensler's office, including Gensler; and (3) collected and assessed over 110 relevant documents and about 1,500 recovered or re-created text messages. We also reviewed the SEC's efforts to recover data missing from Gensler's mobile device before it was returned to the vendor.

Prior Coverage

In 2020, we issued the following report of particular relevance to this review:

- *Opportunities Exist To Improve the SEC's Management of Mobile Devices and Services, Report No. 562* (September 30, 2020).

This report can be accessed at https://www.sec.gov/oig.

Appendix II. 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: Dave Bottom, Chief Information Officer DAVID BOTTOM Digitally signed by DAVID BOTTOM Date: 2025.08.22 15:40:48 -04'00'

Date: August 22, 2025

Subject: Management Response to Draft OIG Special Review, *Avoidable Errors Led to the Loss of the Former SEC Chair's Text Messages*

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG)'s special review of the Securities and Exchange Commission's handling of some of the then Chair Gary Gensler's text messages on his agency-issued mobile device.

The SEC takes seriously its obligations to manage the mobile devices issued to agency officials and staff to conduct SEC business. The agency has taken proactive steps to prevent a recurrence of the missteps that led to the loss of records in 2024. Most notably, the SEC has disabled the use of the native texting application on all agency-issued mobile devices (with limited exceptions) and reaffirmed its policy prohibiting agency officials and staff from conducting SEC business on personal devices. The agency also no longer automatically removes content from a mobile device if it stops communicating with the agency's mobile device management (MDM) system for a length of time. Finally, the agency has established annual recordkeeping training for Capstone officials. These changes reflect the agency's commitment to safeguarding sensitive information and ensuring compliance with federal records management standards.

The SEC concurs with the report's five recommendations and will implement corrective actions as a key priority. Detailed responses on those recommendations are provided in Appendix A.

The OIG's report raises two additional matters of interest, the first of which pertains to the impact of the loss of text messages on FOIA requests. The Office of FOIA Services (OFS) will incorporate the OIG's suggestion to notify requesters of the former Chair's lost text messages whenever those messages would have been searched in response to a pending FOIA request. In addition, OFS will review internal FOIA guidance and if necessary, issue clarifications on when requests for "communications" must include searching text messages. The second matter relates to the potential records management-related risks that may result from disabling the use of the native texting application on SEC devices. The SEC's decision to disable the native texting application on agency-issued mobile devices—subject to limited exceptions—was driven by significant cybersecurity and recordkeeping concerns. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has advised federal agencies to disable SMS messaging on government-

issued devices due to persistent cyber threats.[1] Text messaging also presents substantial challenges for meeting federal recordkeeping obligations. Guidance from the National Archives and Records Administration (NARA) cited by the OIG acknowledges the recordkeeping limitations of text messaging and recommends that agencies adopt secure communication tools that support both information protection and archival requirements. Consistent with this guidance, the SEC has implemented secure, compliant alternatives—including encrypted email and mobile collaboration platforms—that are easier to manage, audit, and preserve.

We appreciate the professionalism and courtesy provided by the OIG during this review. We look forward to working with your office to confirm our actions fully address the recommendations in your report.

Enclosure: Appendix A

[1] *See, e.g.*, CISA, Mobile Communications Best Practice Guidance (Dec. 18, 2024), https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf.

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

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

Recommendation 1: Update policies and procedures to ensure that OIT (a) thoroughly documents and understands changes to the SEC's mobile device management system before such changes are implemented; (b) maintains an accurate inventory of mobile devices enrolled in the SEC's mobile device management system (including timely follow-up and removal of inactive devices); (c) reviews and escalates mobile device management system notifications involving Capstone officials' devices; and (d) regularly obtains and, as necessary, responds to information about technical risks from vendors whose products may impact the SEC's mobile devices.

Response: We concur. The SEC will update OIT policies and procedures to require that:

a. Changes to the SEC's MDM system are documented before changes are implemented;
b. An accurate inventory of mobile devices enrolled in the SEC's MDM system is maintained (including timely follow-up and removal of inactive devices);
c. MDM system notifications involving Capstone officials' devices are reviewed and escalated; and
d. Reviews of vendor release notes about the technical risks associated with products impacting SEC's mobile devices are performed, as necessary.

We will aim to complete these planned corrective actions by December 2025.

Recommendation 2: Ensure that all SEC Capstone officials' devices were backed up at the time OIT removed the texting application from SEC devices, and (for each device) document the date OIT verified that all electronic records, including text messages, were successfully saved (as of the October 2022 Capstone initiative and with each subsequent backup). If text messages from any Capstone officials' devices were not successfully saved, work with ORMS to determine if NARA notification is required.

Response: We concur. At the time OIT disabled texting on SEC-issued devices, OIT stored backups in an SEC SharePoint repository. OIT will review its records to confirm that all Capstone devices were backed up, the date on which this occurred, and that texts from these backups are accessible. In addition, in response to OIG's inquiries concerning the potential loss of text messages from 50 particular Capstone devices, OIT and other agency staff investigated the history of each device and concluded that 21 devices needed to be reported to NARA. (The other 29 devices did not involve the potential loss of Federal records.) On July 29, 2025, following OIT's investigation, the SEC reported to NARA the potential loss of Federal records on 21 devices.

We will aim to complete this planned corrective action by December 2025.

Recommendation 3: Update the applicable system security plan(s) to accurately reflect the mobile device management system audit events and logs that should be forwarded to the SEC's security information and event management tool and ensure that those logs support after-the-fact investigations of incidents.

Response: We concur. The SEC will update the applicable system security plans to identify auditable events and logs that should be forwarded to the SEC's security information and event management tool to support after-the-fact investigations of incidents.

We will aim to complete this planned corrective action by March 2026.

Recommendation 4: Develop procedures to periodically verify that the mobile device management system audit events and logs identified in the applicable system security plan(s) are successfully retained in the SEC's security information and event management tool.

Response: We concur. The SEC will update its procedures to include processes for reviewing and retaining MDM audit events and logs identified in Recommendation 3.

We will aim to complete this planned corrective action by March 2026.

Recommendation 5: Update policies and procedures to require OIT management's approval of commands during troubleshooting activities that result in a factory reset of Capstone user devices, and verification that appropriate device logs and forensic data have been collected and retained beforehand.

Response: We concur. The SEC will update its policies and procedures to require OIT management's approval of commands during troubleshooting activities that result in a factory reset of Capstone user devices and verify that appropriate device logs and forensic data have been collected and retained beforehand.

We will aim to complete this planned corrective action by November 2025.

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