




REDACTED FOR PUBLIC RELEASE

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

September 27, 2023

TO: Kenneth Johnson, Chief Operating Officer

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

SUBJECT: *Final Management Letter: Readiness Review – The SEC’s Progress Toward Implementing Zero Trust Cybersecurity Principles*

A zero trust approach to cybersecurity focuses on preventing and limiting damage in the event that a malicious actor gains access to a network. Unlike traditional models, zero trust operates on the principle “never trust, always verify,” continuously authenticating and authorizing users and devices that seek to obtain and maintain access to systems and data.

In 2022, the Office of Management and Budget (OMB) directed all agencies to begin implementing a zero trust framework to secure their data and information systems. Subsequently, in May 2023, the U.S. Securities and Exchange Commission’s (SEC or Agency) Office of Inspector General (OIG) initiated a review of the SEC’s progress toward implementing new Federal zero trust cybersecurity principles. This management letter presents our results and requests additional information to help us determine whether further action by the OIG is warranted. We redacted non-public information to create this public version of our letter.

Executive Summary

Overall, the SEC has made progress toward implementing Government-wide zero trust architecture strategy and cybersecurity standards and objectives established in OMB Memorandum M-22-09 (referred to here after as “Memorandum” or OMB M-22-09).¹ The Memorandum specifies 19 tasks, 9 of which were to be accomplished in the first year (*i.e.*, by January 27, 2023).

The SEC has completed six of the nine actions required to be implemented within the first year. Among other actions taken, the SEC has:

- Appointed a zero trust strategy implementation lead,
- Ensured certain tools met Cybersecurity and Infrastructure Security Agency (CISA) technical requirements, and
- Provided OMB and CISA a zero trust strategy implementation plan and estimates of budgetary resources needed to implement zero trust in fiscal year (FY) 2023 and FY 2024.

¹ Office of Management and Budget, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*; January 26, 2022.

REDACTED FOR PUBLIC RELEASE

However, at the time of our review, three of the nine tasks had not been completed. Specifically, the SEC's Office of Information Technology (OIT) has not:

- Made necessary changes to one of the SEC's public-facing systems,
- Removed from all systems password policies that require special characters, and
- Established a goal for monitoring and restricting sensitive electronic documents.

The SEC appears to be on track to meet the longer term zero trust requirements by OMB's September 30, 2024, deadline; however, actions are needed to address outstanding tasks and prevent delaying the SEC's achievement of specific zero trust security goals and extending implementation beyond FY 2024.

Background

Increasingly sophisticated and persistent threat campaigns against the Federal Government's information technology architecture demonstrate that conventional perimeter-based defenses often do not effectively protect critical systems and data. These threats have necessitated a Government-wide paradigm shift towards a "zero trust" approach to cybersecurity based on continual verification of each user, device, application, and transaction.² Accordingly, on May 12, 2021, the President issued Executive Order 14028, *Improving the Nation's Cybersecurity*, initiating a Government-wide effort to ensure that baseline security practices are in place and to migrate the Federal Government to a zero trust architecture, among other things. To fulfill requirements established in Executive Order 14028, help reinforce the Government's defenses, and implement a zero trust architecture, on January 26, 2022, OMB issued M-22-09.

OMB M-22-09 requires Federal agencies to achieve specific zero trust security goals by the end of FY 2024 (that is, September 30, 2024). To do so, agencies must appoint a zero trust strategy implementation lead and complete 19 specific tasks. Nine of those tasks were to be completed within 60 days to one year after the issuance of OMB M-22-09.³

The SEC appointed its Chief Information Security Officer as its zero trust strategy implementation lead.⁴ Thereafter, on May 24, 2022, the SEC submitted to OMB and CISA the first version of its zero trust strategy implementation plan and required budget estimates. According to SEC's May 2022 implementation plan, OIT estimated requiring a total of about (b)(5) for FY 2023 and FY 2024 to implement a zero trust strategy. Following the release of additional guidance from CISA in April 2023, the SEC revised its plan, stating that the Agency would require additional funding from its FY 2024 appropriation to develop and staff

² As described in National Institute of Standards and Technology Special Publication 800-207, *Zero Trust Architecture* (August 2020), "Zero trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different—or no more trustworthy—than any nonenterprise-owned environment. In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks. In zero trust, these protections usually involve minimizing access to resources . . . as well as continually authenticating and authorizing the identity and security posture of each access request."

³ Required tasks and corresponding deadlines are attached to this document.

⁴ The zero trust strategy implementation lead was appointed 19 days beyond the required 30 days set forth in OMB M-22-09 because the previously responsible official left the Agency.

required functions and capabilities and fully comply with OMB M-22-09.⁵ The revised plan also highlighted the SEC's efforts to implement zero trust, including:

- Establishing a Zero Trust Governance Committee as part of the SEC's Risk Management Oversight Committee.
- Implementing a cloud architecture model that combines network and security functions into a single service with the goal of accelerating Agency efforts to implement a zero trust architecture.
- Making progress on strategic goals that address requirements for the successful adoption and implementation of zero trust.

Objective, Scope, and Methodology

Our objective was to review the SEC's progress toward implementing the Federal zero trust architecture strategy and specific cybersecurity standards and objectives required by OMB M-22-09. To accomplish our objective, among other work performed, we:

- Met with the contractor conducting the OIG's FY 2023 independent evaluation of the SEC's implementation of the Federal Information Security Modernization Act of 2014 (FISMA) to identify overlaps between FISMA metrics and OMB M-22-09 requirements,⁶
- Selected and tested tasks required to be implemented within 60 days to one year of the issuance of OMB M-22-09 that were not tested by the OIG's FISMA contractor, and
- Met with OIT management to understand how the SEC prepared and revised its zero trust strategy implementation plan.

We conducted our work between May and September 2023 and in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspector General* (Silver Book) and guidance for OIG agile work products. Our work adhered to the professional standards of independence, due professional care, and quality assurance, and followed procedures to ensure accuracy of the information presented.

Results

The SEC has made progress toward implementing Government-wide zero trust architecture strategy and specific cybersecurity standards and objectives. As of March 16, 2022, the Agency had appointed a zero trust strategy implementation lead⁷ and had either completed or was working to implement 16 of the 19 tasks specified in OMB M-22-09. Actions taken to comply with those requirements due on or before January 2023 (within one year's of the Memorandum's issuance) are further described below.

⁵ As of August 15, 2023, when we drafted this letter, the exact amount of additional funding that may be needed was unknown.

⁶ To meet many OMB M-22-09 requirements at this time, agencies need only to address certain topics in their zero trust implementation plans. Relevant FISMA metrics may include additional requirements.

⁷ Since the issuance of OMB M-22-09, two individuals have served as the SEC's Chief Information Security Officer and, therefore, its zero trust strategy implementation lead.

The SEC Submitted a Zero Trust Strategy Implementation Plan and Budget Estimates. Agencies were given 60 days to submit to OMB and CISA a zero trust strategy implementation plan for FY 2022 through FY 2024 and estimates of the budgetary resources needed to implement zero trust in FY 2023 and FY 2024. Although delayed, as previously stated, the SEC submitted to OMB and CISA its zero trust implementation plan and budget estimates.⁸

OIT Ensured the SEC's Endpoint Detection and Response Tools Met CISA's Technical Requirements. Endpoint detection and response tools allow agencies to gather and analyze security threat information to find security breaches and respond to threats. Agencies must ensure such tools meet CISA's technical requirements and are deployed and operated in accordance with OMB guidance.⁹ Communications between OIT and CISA demonstrated completion of this task.

The SEC Coordinated with CISA to Improve Detection of Cybersecurity Vulnerabilities. The adoption of an endpoint detection and response solution requires agencies to share information with CISA. The SEC has implemented dashboards that provide internal and external stakeholders (including CISA) a portfolio view of cybersecurity risks across the Agency.

The SEC Welcomes Vulnerability Reports. To fully implement zero trust strategies, by September 2022 agencies should have begun welcoming external vulnerability reports for their internet-accessible systems. The SEC's vulnerability disclosure policy, which is posted to the Agency's public website, accomplishes this by encouraging security researchers to contact the Agency to report potential vulnerabilities identified in SEC systems. The policy specifies how to submit a vulnerability report and the information that should be included.¹⁰

The SEC Implemented a FISMA Moderate System. Within one year of the issuance of OMB M-22-09, agencies were to select at least one information technology system rated under FISMA as posing moderate risks if compromised¹¹ that was not internet-accessible and that required authentication, and take necessary actions to allow secure, full-featured operation of that system over the internet. To fulfill this requirement, the SEC selected a legal-based document retrieval system that was categorized as "FISMA moderate." Within the one-year timeframe, that system was fully operational and accessible by SEC staff over the internet.

OIT Submitted a Non-.gov Hostname. Agencies were given 60 days to begin providing CISA and the U.S. General Services Administration any non-.gov hostnames used by agencies' internet-accessible information systems. Accordingly, OIT submitted a .com host

⁸ The SEC was about two months late submitting its zero trust strategy implementation plan and required budget estimates for FY 2023 and FY 2024.

⁹ Relevant OMB guidance is established in OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*; October 8, 2021.

¹⁰ See "Vulnerability Disclosure Policy" at <https://www.sec.gov/vulnerability-disclosure-policy> (accessed by the OIG on August 9, 2023, and last modified by the SEC on October 21, 2021).

¹¹ A system may be considered "FISMA moderate" if a breach of system security could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

name that the SEC uses. We verified that, as of May 22, 2023, the host name appeared on the U.S. General Services Administration's list of non-.gov and non-.mil government domains.

Three of the nine zero trust implementation tasks due by January 2023 remained outstanding at the time of our review. These tasks and the SEC's actions and/or needed actions are further described below.

OIT Did Not Fully Comply with a Requirement Related to Certain Public-facing Systems. To fully implement zero trust strategies, within one year of issuance of OMB M-22-09 agencies were required to configure all public-facing systems that support multi-factor authentication to give users the option of using phishing-resistant authentication.¹² According to CISA, multi-factor authentication makes it difficult for cyber threat actors to gain access to networks and information systems, including through phishing. Moreover, CISA considers phishing-resistant authentication to be the "gold standard." However, OIT did not fully comply with this requirement and has accepted the risk. The risk acceptance form (approved by the then Acting Chief Information Security Officer and dated January 30, 2023) states that, with the exception of one system,¹³ OIT has generally met this requirement by migrating the Agency's public-facing systems capable of multifactor authentication to use *login.gov*.¹⁴ According to Agency personnel, there is limited risk because the system in question has compensating authentication controls. We note, however, that phishing-resistant authentication is needed to prevent cyber threat actors from using social engineering to gain access to the SEC's network.

OIT Did Not Remove Password Policies That Require Special Characters. As part of zero trust implementation, OMB requires agencies to remove from all systems password policies that require special characters and regular password rotation, because these requirements have long been known to lead to weaker passwords and should not be employed by the Federal Government.¹⁵ Although OIT discontinued requiring periodic password rotation, it continues to require that passwords contain special characters. The risk acceptance form (approved by the Chief Information Security Officer and dated January 4, 2023) states that OIT will delay compliance until the SEC implements essential elements of the zero trust architecture, including multi-factor authentication, sufficient to eliminate the use of single-factor passwords as a means for authentication. OIT officials informed us that the temporary delay (1) will ensure that the policy change is coordinated both technically and procedurally and will occur at a time that does not conflict with other OIT initiatives; and (2) will have little impact due to existing password controls and ongoing network monitoring and account maintenance procedures. We note, however, that OMB M-22-09 makes clear

¹² Phishing-resistant multi-factor authentication protects personnel from sophisticated online attacks. According to OMB M-22-09, "phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

¹³ The Agency expects to migrate this system to *login.gov* by January 30, 2024, given that this is the requested expiration date of the risk acceptance.

¹⁴ *Login.gov* is a secure service used by the public to sign in to participating government agencies. The service requires both passwords and a second authentication method (such as a one-time code) to protect user information.

¹⁵ See OMB M-22-09, page 8.

that removal of the password policies in question should be completed “as soon as is practical and should not be contingent on adopting other protections.”

The Office of the Chief Data Officer and OIT Did Not Establish a Goal for Monitoring and Restricting Sensitive Electronic Documents. Within 120 days of the issuance of OMB M-22-09, agencies were to develop a set of initial categories for sensitive electronic documents within their enterprise, with the goal of automatically monitoring and potentially restricting how such documents are shared. While the Office of the Chief Data Officer developed data categories defined in the SEC Regulation 2-1 *Data Access, Use, and Internal Sharing Policy*, it did not include a goal for monitoring and restricting sensitive electronic documents. According to OIT personnel, development of automated controls for document monitoring is in progress and the SEC expects to complete this effort by FY 2024. Moreover, OIT personnel believe that only initial categories were required within 120 days of the issuance of OMB M-22-09. However, we consider monitoring and potentially restricting how sensitive electronic documents are shared to be an integral part of the OMB M-22-09 requirement for protecting the Agency’s data and systems.

The SEC appears on track to meet the remaining zero trust requirements by OMB’s September 30, 2024, deadline; however, actions are needed to address outstanding tasks and prevent delaying the SEC’s achievement of specific zero trust security goals and extending implementation beyond FY 2024.

Conclusion

On September 11, 2023, we provided SEC management with a draft of our management letter for review and comment. On September 22, 2023, the SEC indicated it would not be providing a written response.

To help us determine whether further action by the OIG is warranted, we request that management provide the OIG, no later than November 13, 2023, a description of actions the SEC has taken or plans to take to:

1. Configure all SEC public-facing systems that support multi-factor authentication to give users the option of using phishing-resistant authentication.
2. Remove password policies that require special characters.
3. Establish a goal for monitoring and potentially restricting how sensitive electronic documents are shared.

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

Attachment

cc: Gary Gensler, Chair
Amanda Fischer, Chief of Staff, Office of Chair Gensler
Heather Slavkin Corzo, Policy Director, Office of Chair Gensler

Kevin R. Burris, Counselor to the Chair and Director of Legislative and Intergovernmental Affairs
Scott E. Schneider, Counselor to the Chair and Director of Public Affairs
Philipp Havenstein, Operations Counsel, Office of Chair Gensler
Ajay Sutaria, Legal Counsel, Office of Chair Gensler
Hester M. Peirce, Commissioner
Benjamin Vetter, Counsel, Office of Commissioner Peirce
Caroline A. Crenshaw, Commissioner
Malgorzata Spangenberg, Counsel, Office of Commissioner Crenshaw
Mark T. Uyeda, Commissinoer
Holly Hunter-Ceci, Counsel, Office of Commissioner Uyeda
Jaime Lizárraga, Commissioner
Laura D'Allaird, Counsel, Office of Commissioner Lizárraga
Parisa Haghshenas, Counsel, Office of Commissioner Lizárraga
Megan Barbero, General Counsel
Elizabeth McFadden, Deputy General Counsel General Litigation/Managing Executive, Office of the General Counsel
Lisa Helvin, Principal Deputy General Counsel for Adjudication and Oversight, Office of the General Counsel
David Leviss, Associate General Counsel for Oversight and Investigations, Office of the General Counsel
Stephen Jung, Assistant General Counsel for Intragovernmental and Congressional Affairs, Office of the General Counsel
Shelly Luisi, Chief Risk Officer
Jim Lloyd, Assistant Chief Risk Officer/Audit Coordinator, Office of the Chief Risk Officer
Austin Gerig, Chief Data Officer
David Bottom, Director/Chief Information Officer, Office of Information Technology
James Scobey, Associate Director/Chief Information Security Officer, Information Security, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology
Deborah J. Jeffrey, Inspector General

Attachment. The SEC's Progress to Date Toward Completing Tasks Prescribed in OMB M-22-09

	Task	Agency Action Timeline (Measured from OMB M-22-09 Issuance Date)	Requirement Met?	OIG Comments
1	Agencies must submit to OMB and CISA an implementation plan for FY 2022-2024 and a budget estimate for FY 2023-2024.	Within 60 days	Yes	The SEC's submission was about two months late.
2	Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan and assessed as part of the OIG's FY 2023 FISMA evaluation.
3	Agencies must require their users to use a phishing-resistant method to access agency-hosted accounts.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan and assessed as part of the OIG's FY 2023 FISMA evaluation.
4	Public-facing agency systems that support multi-factor authentication must give users the option of using phishing-resistant authentication.	Within 1 year	No	OIT issued a risk acceptance document for one public-facing SEC system, acknowledging a lack of compliance with OMB M-22-09 requirements.
5	Agencies must remove password policies that require special characters and regular password rotation from all systems.	Within 1 year	No	OIT issued a risk acceptance document, acknowledging a lack of compliance with OMB M-22-09 requirements.
6	Agency authorization systems should work to incorporate at least one device-level signal alongside identity information about the authenticated user.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan.
7	Agencies must create ongoing, reliable, and complete asset inventories, including by leveraging the continuous diagnostics and mitigation program.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan and assessed as part of the OIG's FY 2023 FISMA evaluation.
8	Agencies must ensure their endpoint detection and response tools meet CISA's technical requirements and are deployed and operated across their agency.	February 2022, consistent with OMB M-22-01	Yes	Communications between OIT and CISA demonstrated completion of this task.
9	Agencies must work with CISA to identify gaps, coordinate on deployment, and establish information sharing capabilities with CISA, as described in OMB M-22-01.	January 2022, consistent with OMB M-22-01	Yes	Assessed as part of the OIG's FY 2023 FISMA evaluation.
10	Agencies must resolve Domain Name System queries using encrypted Domain Name System wherever it is technically supported.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan.
11	Agencies must enforce authenticated HTTPS for all production HTTP traffic, including traffic that does not cross the public internet.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan.
12	Agencies must work with the Dot.Gov program at CISA to "preload" agency-owned .gov domains as HTTPS-only in web browsers.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan.
13	Agencies must develop a zero trust architecture plan that describes how the agency plans to isolate its applications and environments, in consultation with CISA, and include it in the full implementation and investment plan required by OMB M-22-09.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan.

	Task	Agency Action Timeline (Measured from OMB M-22-09 Issuance Date)	Requirement Met?	OIG Comments
14	Agency system authorization processes must employ both automated analysis tools and manual expert analysis.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan.
15	Agencies must welcome external vulnerability reports for their internet-accessible systems.	September 2022, consistent with OMB M-20-32 and Department of Homeland Security Binding Operational Directive 20-01	Yes	Verified that the SEC established a public-facing vulnerability disclosure policy.
16	Agencies must select at least one FISMA moderate system that requires authentication and is not currently internet-accessible, and securely allow full-featured operation over the internet.	Within one year	Yes	Verified that the SEC selected and implemented a FISMA moderate system per the requirement.
17	Agencies must begin providing CISA and the U.S. General Services Administration any non-.gov hostnames used by their internet-accessible information systems.	Within 60 days	Yes	Verified that the SEC provided .com hostname to CISA and the U.S. General Services Administration as a non-.gov hostname used by the Agency.
18	Agencies should work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure.	Include in agency zero trust strategy implementation plan	Yes	Addressed in the SEC's plan.
19	Agency Chief Data Officers must work with key agency stakeholders to develop a set of initial categorizations for sensitive electronic documents within their enterprise, with the goal of automatically monitoring and potentially restricting how these documents are shared.	120 days	No	OIT did not establish a goal for monitoring and potentially restricting sensitive electronic documents as part of the initial categorization of these documents. OIT indicated that the automated controls for document monitoring is in progress and that the SEC expects to complete this effort by FY 2024.

Source: OIG-generated based on OMB M-22-09 and OIG results.