

United States Senate

WASHINGTON, DC 20510

January 11, 2024

The Honorable Deborah J. Jeffrey
Inspector General
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Ms. Jeffrey:

We write to request that your office open an investigation into the recent hack of the U.S. Securities and Exchange Commission's (SEC) social media account, and the SEC's apparent failure to follow cybersecurity best practices.

On January 9, 2024, the SEC revealed that an unknown party had hacked its official account on the social media platform X, formerly known as Twitter. Later that day, X released a statement that the hack involved "an unidentified individual obtaining control over a phone number associated with the @SECGov account through a third party." X also said that the SEC's official account did not have multi-factor authentication (MFA) enabled at the time the account was compromised.

Given the obvious potential for market manipulation, if X's statement is correct, the SEC's social media accounts should have been secured using industry best practices. Not only should the agency have enabled MFA, but it should have secured its accounts with phishing-resistant hardware tokens, commonly known as security keys, which are the gold standard for account cybersecurity. X has permitted users to restrict access to their accounts exclusively using security keys and to remove phone numbers, which can be easily hijacked by fraudsters, since 2021.

Indeed, on January 26, 2022, the Office of Management and Budget (OMB) issued policy memo M-22-09, requiring agencies to use phishing-resistant MFA, including security keys. Although the OMB policy only applies to agency-hosted systems, and not social media websites, OMB's guidance is clear that such security keys and other forms of phishing-resistant MFA are necessary to protect "personnel from sophisticated online attacks." In addition to this OMB policy, the Cybersecurity and Infrastructure Security Agency specifically recommends security keys, noting in an April, 2023 blog post that "while it's true that any form of MFA is better than no MFA, we need to be clear that the time has come for all enterprises to roll out security keys to their staff."

Management of the SEC has received ample warning of the dangers of poor cybersecurity practices from your office. In FY 2023, an independent evaluation overseen by your office of the SEC's Implementation of the Federal Information Security and Modernization Act of 2014 determined that "the SEC's information security program and practices were not effective." The SEC was found to need improvements in adopting plans of action, designing controls for SEC systems, and complying with requirements for logging events. A 2018 report from an evaluation of EDGAR System's Governance and Incident Handling Processes found that "certain

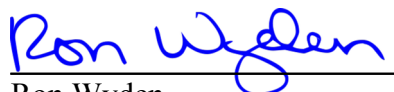
preventative controls either did not exist or operate as designed” and that the public-facing system “lacked adequate governance commensurate with the system’s importance to the SEC’s mission.”

The SEC’s failure to follow cybersecurity best practices is inexcusable, particularly given the agency’s new requirements for cybersecurity disclosure. Additionally, a hack resulting in the publication of material information for investors could have significant impacts on the stability of the financial system and trust in public markets, including potential market manipulation. We urge you to investigate the agency’s practices related to the use of MFA, and in particular, phishing-resistant MFA, to identify any remaining security gaps that must be addressed.

We request you provide us an update on your investigation and the SEC’s remediation no later than February 12, 2024.

Thank you for your attention to this important matter.

Sincerely,



Ron Wyden
United States Senator



Cynthia M. Lummis
United States Senator