Press Release

SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets

FOR IMMEDIATE RELEASE
2023-52

Washington D.C., March 15, 2023 — The Securities and Exchange Commission today proposed requirements for broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents (collectively, "Market Entities") to address their cybersecurity risks.

"I am pleased to support this proposal because, if adopted, it would set standards for Market Entities' cybersecurity practices," said SEC Chair Gary Gensler. "The nature, scale, and impact of cybersecurity risks have grown significantly in recent decades. Investors, issuers, and market participants alike would benefit from knowing that these entities have in place protections fit for a digital age. This proposal would help promote every part of our mission, particularly regarding investor protection and orderly markets."

Market Entities increasingly rely on information systems to perform their functions and provide their services and thus are targets for threat actors who may seek to disrupt their functions or gain access to the data stored on the information systems for financial gain. Cybersecurity risk also can be caused by the errors of employees, service providers, or business partners. The interconnectedness of Market Entities increases the risk that a significant cybersecurity incident can simultaneously impact multiple Market Entities causing systemic harm to the U.S. securities markets.

The proposal would require all Market Entities to implement policies and procedures that are reasonably designed to address their cybersecurity risks and, at least annually, review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether they reflect changes in cybersecurity risk over the time period covered by the review. The proposal — through new notification requirements applicable to all Market Entities and additional reporting requirements applicable to Market Entities other than certain types of small broker-dealers (collectively, "Covered Entities") — would improve the Commission's ability to obtain information about significant cybersecurity incidents affecting these entities. Further, new public disclosure requirements for Covered Entities would improve transparency about the cybersecurity risks that can cause adverse impacts to the U.S. securities markets.

The proposing release will be published in the Federal Register. The public comment period will remain open until 60 days after the date of publication of the proposing release in the Federal Register.

###

Related Materials

- Proposed Rule
- Fact Sheet