FACT SHEET

Addressing Cybersecurity Risks to the U.S. Securities Markets

The Securities and Exchange Commission proposed a new rule, form, and related amendments to require entities that perform critical services to support the fair, orderly, and efficient operations of the U.S. securities markets to address their cybersecurity risks. The new requirements would apply to broker-dealers, the Municipal Securities Rulemaking Board, clearing agencies, major security-based swap participants, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents (collectively, "Market Entities").

Why This Matters

The U.S. securities markets are part of the Financial Services Sector, one of the sixteen critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof," according to the Cybersecurity and Infrastructure Security Agency. The Financial Services Sector increasingly is being attacked by cyber threat actors who use constantly evolving and sophisticated tactics, techniques, and procedures to cause harmful cybersecurity incidents. This poses a serious risk to the U.S. securities markets. The proposal is designed to address and mitigate this risk by requiring Market Entities to take measures to protect themselves and investors from the harmful impacts of cybersecurity incidents.

How This New Rule and Form Would Apply

Proposed new Rule 10 would require all Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks. All Market Entities also, at least annually, would be required to 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. All Market Entities also would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident had occurred or is occurring.

Market Entities—other than certain types of small broker-dealers—would be subject to additional requirements under proposed new Rule 10 as "Covered Entities."

First, the proposed rule would require Covered Entities to adopt policies and procedures to address cybersecurity risks would need to specifically include the following:

- Periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems;
- Measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversee service providers that receive, maintain, or process information or are otherwise permitted to access the Covered Entity's information systems;
- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and
- Measures to detect, respond to, and recover from a cybersecurity incident and procedures to create written documentation of any cybersecurity incident and the response to and recovery from the incident.

Second, after providing immediate written electronic notice of a significant cybersecurity incident, Covered Entities would need to report to the Commission and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR. The form would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to and recover from the incident.

Third, the proposal would require Covered Entities to publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR. A Covered Entity would need to file the form with the Commission and post it on its website. Covered Entities that are carrying or introducing broker-dealers would also need to provide the form to customers at account opening, when information on the form is updated, and annually.

Additional Information:

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