Statement on Proposal for Mandatory Cybersecurity Disclosures

Chair Gary Gensler

March 9, 2022

Today, the Commission is considering a proposal to mandate cybersecurity disclosures by public companies. I am pleased to support this proposal because, if adopted, it would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting.

We've been requiring disclosure of important information from companies since the Great Depression. The basic bargain is this: Investors get to decide what risks they wish to take. Companies that are raising money from the public have an obligation to share information with investors on a regular basis.

Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs.

Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. The interconnectedness of our networks, the use of predictive data analytics, and the insatiable desire for data are only accelerating, putting our financial accounts, investments, and private information at risk. Investors want to know more about how issuers are managing those growing risks.

Cybersecurity incidents, unfortunately, happen a lot. They can have significant financial, operational, legal, and reputational impacts on public issuers. Thus, investors increasingly seek information about cybersecurity risks, which can affect their investment decisions and returns.

A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner.

Today's release would enhance issuers' cybersecurity disclosures in two key ways:

First, it would require mandatory, ongoing disclosures on companies' governance, risk management, and strategy with respect to cybersecurity risks. This would allow investors to assess these risks more effectively. For example, under the proposed rules, companies would disclose information such as:

- management's and the board's role and oversight of cybersecurity risks;
- whether companies have cybersecurity policies and procedures; and
- how cybersecurity risks and incidents are likely to impact the company's financials.

Second, it would require mandatory, material cybersecurity incident reporting. This is critical because such material cybersecurity incidents could affect investors' decision-making.

When companies have an obligation to disclose material information to investors, they must be complete and accurate. Their disclosures also should be timely. Today's proposal would specify when and what information about cybersecurity incidents companies must disclose in a current report, such as on Form 8-K. It also would

require updates in periodic reports to give investors more complete information on previously disclosed, material cybersecurity incidents.

This is the third rulemaking project we have proposed that implicates cybersecurity. Earlier this winter, the Commission voted to propose expanding Regulation Systems Compliance and Integrity (SCI) to certain government securities trading platforms. In February, we voted to propose new obligations for registered investment advisers and funds with respect to cybersecurity.

Going forward, I've also asked staff to make additional recommendations for the Commission's consideration with respect to broker-dealers, Regulation SCI, and intermediaries' requirements regarding customer notices (Regulation S-P).

I am pleased to support today's proposal and, subject to Commission approval, look forward to the public's feedback. I'd like to thank the members of the SEC staff who worked on this rule, including:

- Renee Jones, Erik Gerding, Betsy Murphy, Luna Bloom, Ian Greber-Raines, Charles Kwon, Michael Seaman, Lindsay McCord, Deanna Virginio, Michael Coco, Matt McNair, Shelly Luisi, Catherine Brown, Kim McManus, Rolaine Bancroft, Katherine Hsu, Arthur Sandel, Chris Windsor, Rushabh Soni, and Sam Serfaty in the Division of Corporation Finance;
- Brian Johnson, David Joire, Amanda Wagner, Christopher Staley, and Rachel Kuo in the Division of Investment Management;
- Dan Berkovitz, Megan Barbero, Bryant Morris, Dorothy McCuaig, David Lisitza, and Joseph Valerio in the Office of the General Counsel;
- Jessica Wachter, Oliver Richard, Vlad Ivanov, Lauren Moore, Charles Woodworth, Qiao Kapadia, Connor Hurley, Mike Willis, Julie Marlowe, PJ Hamidi, Gregory Scopino, Hamilton Martin, Mariesa Ho, Xanthi Gkougkousi, Sejal Naik, Michael Pessin, Lakin Brown, Justin Myalil, Syed Husain, Nicholas Acosta, Benjamin Stoner, Reevu Adakroy, Gideon Brown, Ian Black, Justin Soll, and Wanli Zhao in the Division of Economic and Risk Analysis;
- Shaz Niazi in the Office of the Chief Accountant;
- Ted Shelkey in the Office of Information Technology;
- Arsen Ablaev in the Division of Enforcement;
- Laurita Finch, Rosemary Filou in the EDGAR Business Office; and
- Dan DeWaal and Nancy Sumption in the Division of Examinations.

I'd also like to thank the Department of Justice, the Federal Bureau of Investigation, and the Cybersecurity and Infrastructure Security Agency for their valuable input as we developed this proposal.