ALSTON & BIRD

WWW.ALSTON.COM

Capital Markets & Securities /
Privacy, Cyber & Data Strategy ADVISORY ■

DECEMBER 21, 2023

SEC's Cybersecurity Rules – SEC Issues Guidance and DOJ Establishes Processes for the National Security or Public Safety Exception

by ***Dave Brown***, ***Rebecca Valentino***, ***Kim Peretti***, ***Kate Hanniford***, ***Alysa Austin***, ***Kezia Osunsade*** **and** ***Baili Ebinger***

As the new cybersecurity disclosure rules for public companies adopted by the Securities and Exchange Commission (SEC) took effect on December 18, 2023, the SEC Division of Corporation Finance, U.S. Department of Justice (DOJ), and Federal Bureau of Investigation (FBI) have released guidance intended to aid public companies as they comply with the rules. Under the recently adopted rules, public companies, including foreign private issuers, must report material cybersecurity incidents on Forms 8-K and 6-K.

SEC Guidance on the Content and Timing of the Form 8-K Disclosure

In a statement on December 14, Director of the Division of Corporation Finance (Corp Fin) Erik Gerding provided clarification of two key points that together represent a potential softening of the SEC's position toward the content and timing of the Form 8-K report. First, he provided welcome assurance that a disclosing company "need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." Second, he reiterated that the four-day clock begins after the determination of materiality, not the discovery of the incident itself, and noted that "in many cases, a company will be unable to determine materiality the same day the incident is discovered." His remarks specifically acknowledged that "a public company may alert similarly situated companies as well as government actors at any point in its incident response, including immediately after discovering an incident and before determining materiality, so long as it does not unreasonably delay its internal processes for determining materiality."

DOJ, FBI, and SEC Guidance on the Process and Criteria for Seeking a Delay

Consistent with the SEC's final rules and guidance, the DOJ issued guidance that specifies its criteria and timing for assessing a request for a potential law enforcement delay. For its part, the FBI issued guidance that provides instructions for public companies to seek a law enforcement delay and the criteria and process for diligence and escalation by the FBI to the DOJ to make the ultimate decision to a delay request. To complete the coordination effort,

Corp Fin published four new compliance and disclosure interpretations (CD&Is) relating to the national security / public safety exception to the requirement to file a Form 8-K within four business days of a company determining that a cybersecurity incident is material.

DOJ criteria for a delay

The DOJ Material Cybersecurity Incident Delay Determination reinforced the DOJ's position that it may grant an exception to allow a company to delay a disclosure by up to 30 days after the disclosure would have otherwise been required upon a determination by the DOJ that all or part of a company's disclosure of a material cybersecurity incident would pose a substantial risk to national security or threat to public safety. The DOJ clarified that its primarily inquiry in deciding whether to approve a delay request will be "whether the *public disclosure* of a cybersecurity incident threatens public safety or national security, not whether the incident itself poses a substantial risk to public safety and national security."

The DOJ guidance further outlined the limited instances when delaying public disclosure may be warranted, which include among others:

- Incidents resulting from exploitation of a technique for which there is not yet well-known mitigation (e.g., exploiting a software vulnerability if there is no patch or other mitigation available) and when disclosure could lead to more incidents.
- Incidents primarily impacting a system containing sensitive U.S. government information and public disclosure could lead to further cyber exploitation.
- When a company is conducting remediation efforts for any critical infrastructure or critical system and disclosure of the incident could undermine those efforts.
- When a government agency has made the company aware of circumstances that require delaying disclosure, such as law enforcement operations to disrupt criminal activity or the potential compromise of confidential sources.

A delay may be further extended by an additional 30 days if, after the initial 30 days, the DOJ determines that the incident continues to pose a risk to national security or public safety. A further delay of 60 days may be granted in "extraordinary circumstances" if the Attorney General determines that the substantial national security (but not public safety) risk is ongoing.

FBI process to seek a delay

The FBI is tasked with processing delay requests on behalf of the DOJ and coordinating the involvement of other government agencies as appropriate. It has issued a Policy Notice that describes how incoming disclosure requests will be processed and provided summary guidance on its approach in FBI's Guidance to Victims of Cyber Incidents on SEC Reporting Requirements.

While the DOJ and FBI encourage companies to engage with their local FBI field office as soon as possible in the context of an incident—and well before the completion of any materiality analysis—companies must submit their delay request to the FBI no later than "concurrently with the materiality decision." Upon receipt of a company's delay request, the FBI, in coordination with other government agencies, must conduct checks of U.S. government national security and public safety equities and fact-finding procedures before referring the request to the DOJ within no more

than 32 hours. Once referred, the DOJ must issue a delay determination within four business days of the company's determination that a cybersecurity incident was material. Given the strict internal timeframes, the FBI encourages companies to engage in early communication to allow the FBI to familiarize itself with the facts and circumstances before it receives a company's delay request.

The DOJ will communicate its decision to the SEC and requesting public company simultaneously so that both would be aware of the materiality determination and the DOJ's approval or rejection of a law enforcement delay. Importantly, if the company requests a delay from the DOJ and it does not receive a response within four business days of the company determining that a cybersecurity incident was material, the company should still move forward with filing a Form 8-K because there is no tolling provision.

FBI guidance on requesting a delay outlines the specific information such requests must include:

- A detailed account of the incident (e.g., timing, location, suspected intrusion vectors and any known identified vulnerabilities, affected infrastructure or data, and operational impact if known, as well as the date and time (including time zone) of the company's materiality determination).
- Information on the cyber actors responsible.
- Status of any remediation efforts.

Notably, any request that fails to disclose the date, time, and time zone of the company's materiality determination or that is not filed "immediately" upon the determination of materiality will be automatically denied.

Requests may be made to the FBI directly via email at cyber_sec_disclosure_delay_referrals@fbi.gov or through the U.S. Secret Service, Cybersecurity and Infrastructure Security Agency, or another sector risk management agency.

Corp Fin guidance

Consistent with the process articulated by the DOJ and FBI, on December 12, 2023, Corp Fin concurrently published four new CD&Is relating to the national security / public safety exception to the requirement to file a Form 8-K within four business days of a company determining that a cybersecurity incident is material.

- Question 104B.01. If the Attorney General declines to make a determination or does not respond before the Form 8-K would otherwise be due, a company must file the 8-K within four business days of determining that the cybersecurity event was material. Requesting an exception from the Attorney General does not change the required filing timing. The exception must be granted to alter 8-K timing.
- Question 104B.02. If a company is granted an exception by the Attorney General for a limited time and then requests an additional delay and the Attorney General declines to make a determination or does not respond, a Form 8-K is due within four business days of the expiration of the original delay period.
- Question 104B.03. If a company is granted an exception by the Attorney General, but during the delay period the Attorney General determines that the disclosure of the incident no longer poses a substantial risk, a company must file a Form 8-K within four days of the new determination.
- Question 104B.04. A company consulting with the DOJ about the availability of a delay does not make the cybersecurity incident material.

Although this collection of guidances represents a coordinated interagency effort to facilitate requests for law enforcement delays to the SEC material cybersecurity incident disclosure timeline, given the nature of the information that is required to request a delay, the limited circumstances in which the DOJ appears to be amenable to granting a delay, the limited timeframe for which a delay would be granted, and the simultaneous communication of the decision to the SEC and victim company, it remains to be seen how willing companies may be to take advantage of this process. However, companies can enhance their level of preparedness by considering a range of proactive steps, including by proactively identifying local FBI field office contacts and by reviewing incident response plans to ensure a process for assessing materiality is specified and considers the compressed timeline for potential requests to the FBI and public disclosure via Form 8-K.

You can subscribe to future advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or anyone from our **Capital Markets & Securities** or **Privacy, Cyber & Data Strategy** Teams.

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ +1 404 881 7000 ■ Fax: +1 404 881 7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Rue Guimard 9 ■ Brussels, B-1040 ■ Belgium ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Vantage South End ■ 1120 South Tryon Street ■ Suite 300 ■ Charlotte, North Carolina, USA, 28203-6818 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
FORT WORTH: City Center Fort Worth ■ Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 682 354 2000 ■ Fax: +1 682 354 2299
LONDON: LDN:W ■ 6th Floor ■ 3 Noble Street ■ London ■ EC2V 7EE ■ United Kingdom ■ +44 20 8161 4000
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ +1 213 576 1000 ■ Fax: +1 213 576 1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ +1 212 210 9400 ■ Fax: +1 212 210 9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ +1 919 862 2200 ■ Fax: +1 919 862 2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ +1 415 243 1000 ■ Fax: +1 415 243 1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA, 94304 ■ +1 650 838 2000 ■ Fax: +1 650 838 2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ +1 202 239 3300 ■ Fax: +1 202 239 3333