GUNDERSON DETTMER

Public Companies Insight: DOJ, FBI and SEC Issue Guidance on Requesting National Security and Public Safety Delay for Reporting Material Cyber Incidents on Form 8-K

Insights
December 18, 2023

Current reporting about material cybersecurity incidents within four business days pursuant to new Item 1.05 of Form 8-K required beginning on December 18, 2023 for public companies other than smaller reporting companies (June 15, 2024 for smaller reporting companies)

On December 12, 2023, the U.S. Department of Justice (DOJ) published guidelines outlining the process public companies (or U.S. government agencies in coordination with such companies) must follow to invoke the limited national security and public safety reporting delay permitted under the new cybersecurity disclosure rules adopted by the U.S. Securities and Exchange Commission (SEC) last July. The guidelines also describe the procedures the U.S. Attorney General will use to evaluate whether a delay is warranted.

Background

Under the new SEC rules (discussed in-depth in our previous client alert), a company is required to disclose certain specified information about a material "cybersecurity incident" (namely, the material aspects of the nature, scope and timing of the incident, and the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations) ***within four***

business days after the company determines the incident is material (*not* four business days after the incident occurred or is discovered). The materiality determination must be made ***"without unreasonably delay" after discovery of the incident***. What constitutes "materiality" for purposes of cybersecurity incident disclosure is consistent with the U.S. Supreme Court definition of materiality—i.e., information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."

However, the rules expressly provide that the Form 8-K disclosure may be delayed, initially for up to 30 days, if the Attorney General (or authorized designees at DOJ) determines immediate disclosure would pose a ***"substantial risk to national security or public safety"*** and notifies the SEC of such determination in writing prior to the four-business-day Form 8-K filing deadline. The delay may be extended for an additional 30-day period and (in extraordinary circumstances) for a final additional 60-day period in a similar fashion. To extend the delay beyond 120 days, the SEC must grant relief through an exemptive order.

New Guidance

Pursuant to the new guidance, Federal Bureau of Investigation (FBI) field offices will be the primary points of contact for companies that have experienced cybersecurity incidents. **Companies seeking a reporting delay must submit a request to the FBI (either directly or indirectly through another U.S. government agency) concurrently with their materiality determination**. The FBI is responsible for (i) intaking delay requests on behalf of DOJ; (ii) documenting those requests; (iii) coordinating checks of U.S. government national security and public safety equities; and (iv) referring information to DOJ.

Key provisions of the DOJ and FBI guidance are summarized below. Links to the complete guidance documents appear at the end of this alert. On December 12 and December 14, 2023, the SEC's Division of Corporation Finance published four new Form 8-K Compliance and Disclosure Interpretations (C&DIs) addressing additional considerations related to the national security and public safety delay provision that is the subject of the new guidance. The C&DIs are set forth in their entirety and linked below.

Please reach out to your regular Gunderson Dettmer attorney or any member of our Public Companies team if you have questions or would like assistance in navigating the SEC's new cybersecurity disclosure requirements, including incorporating the new guidance discussed in this alert into your organization's cybersecurity incident response plan.

DOJ Approach to Making Delay Determinations

DOJ has sole discretionary authority to determine whether and how long a substantial risk to national security or public safety exists such that a delay in public disclosure is necessary. Senior DOJ and FBI officials have stated they do not expect that many cyber incidents will qualify for such a delay.

The DOJ guidelines emphasize that **the department's primary inquiry when evaluating delay requests is whether the *public disclosure* of a cybersecurity incident—not the incident itself—threatens national security or public safety**: "While cybersecurity incidents themselves frequently threaten public safety and national security, the disclosure to the public that those incidents have occurred poses threats less often," and in many circumstances can even be beneficial.

The guidelines state that, in most cases, companies will be able to publicly disclose material information "at a level of generality" that does not pose a substantial risk to national security or public safety. However, **a delay in public disclosure would be appropriate in the following limited circumstances**:

- **When the incident involved a technique for which there is not yet well-known mitigation** (e.g., exploiting a software vulnerability for which there is no patch or other reasonably available mitigation), and public disclosure of the incident could lead to more incidents.
- **When the incident primarily impacts a system operated or maintained by the company containing sensitive U.S. government information** (e.g., regarding national defense or research and development performed pursuant to government contracts), and public disclosure of the incident would make that information or system vulnerable to further exploitation.
- **When the company is conducting remediation efforts for any critical infrastructure or critical system**, and public disclosure of the incident would undermine those efforts.

The guidelines also identify scenarios in which, at least initially, the government is more likely to be aware of a substantial threat to national security or public safety than the company and might seek the company's agreement to delayed disclosure, such as **when public disclosure of the incident would risk compromising government interests**—for instance, confidential sources, information relating to U.S. national security or law enforcement-sensitive information; operations to disrupt ongoing illicit cyber activity (e.g., through freezing or seizing information, assets or infrastructure involved in illicit cyber activity or by effecting the arrest of individuals for

illicit cyber activity); or the government's own remediation efforts targeted at critical infrastructure and systems.

If the Attorney General determines that a disclosure delay is justified based on one or more of the categories described above, the guidelines note that such determination might pertain to only part of the information that Item 1.05 of Form 8-K requires—for example, that disclosure of the timing of the incident would not pose a substantial risk to national security or public safety, but disclosure of the nature or scope of the incident would pose such a risk.

FBI Contact Instructions

The DOJ guidelines advise that, when a company discovers a cybersecurity incident and believes that disclosure may pose a substantial risk to national security or public safety, the company should (either directly or indirectly through another U.S. government agency) immediately contact the FBI consistent with the reporting procedures described in an FBI Policy Notice dated December 6, 2023 and related guidance documents posted on the FBI's website. In summary:

- The FBI recommends that all publicly traded companies establish a relationship with the cyber squad at their local FBI field office.
- The guidance strongly encourages companies to engage with the FBI *prior to* making a materiality determination about a newly discovered cybersecurity incident whose disclosure may pose a substantial risk to national security or public safety so that agency officials can help them understand whether the incident is material. The DOJ guidelines underscore the importance of providing all relevant facts to the FBI "as soon as possible, even beginning well before the [company] has completed its materiality analysis or its investigation into the incident."
- The guidance explicitly states that **engaging with the FBI or another U.S. government agency does not, by itself, constitute a determination of materiality triggering an 8-K disclosure obligation**. Rather, early outreach "could assist with the FBI's review if the company determines that a cyber incident is material and seeks a disclosure delay."

- In remarks about the SEC's new cybersecurity disclosure rules delivered on December 14, 2023, the agency's Director of the Division of Corporation Finance Erik Gerding reiterated this point, emphasizing that **the rules do not create a disincentive for public companies to consult with law enforcement or national security agencies about cybersecurity incidents**: "Indeed, I would

encourage public companies to work with the FBI, [the Cybersecurity and Infrastructure Security Agency], and other law enforcement and national security agencies at the earliest possible moment after cybersecurity incidents occur…. [C]ompanies and government agencies may find that such timely engagement could assist them in a later determination of whether to seek a delay from the DOJ."

  - Gerding also cautioned that, while consultations with national security and law enforcement agencies may help companies to better understand the impact or severity of a particular incident and thus to assess whether the incident is material, analyses of cyber incidents by these other agencies may take into account factors other than a focus on a reasonable investor, and thus "**ultimately it is the company's responsibility to make a materiality determination based on a consideration of all relevant facts and circumstances**."

- To request a reporting delay, **companies must contact the FBI directly at cyber_sec_disclosure_delay_referrals@fbi.gov** (or indirectly through the U.S. Secret Service, another federal law enforcement agency, the Cybersecurity and Infrastructure Security Agency, the Department of Defense or another sector risk management agency).
- **The FBI will not process delay requests unless they are received from the company immediately upon the company's materiality determination**.
- Each delay request must contain all of the following information:
  - What is the name of your company?
  - When did the cyber incident occur?
  - When did you determine the cyber incident is material? Include the date, time and time zone. ***(Note: Failure to report this information immediately upon determination will cause your delay referral request to be denied.)***

- Are you already in contact with the FBI or another U.S. government agency regarding this incident? If so, provide the names and field offices of the FBI points of contact or information regarding the U.S. government agency with whom you're in contact.

- Describe the incident in detail. Include the following details, at minimum:
    - What type of incident occurred?
    - What are the known or suspected intrusion vectors, including any identified vulnerabilities if known?
    - What infrastructure or data were affected (if any) and how were they affected?
    - What is the operational impact on the company, if known?

- Is there confirmed or suspected attribution of the cyber actors responsible?

- What is the current status of any remediation or mitigation efforts?

- Where did the incident occur? Provide the street address, city and state where the incident occurred.

- Who are your company's points of contact for this matter? Provide the name, phone number and email address of personnel you want the FBI to contact to discuss this request.

- Has your company previously submitted a delay referral request or is this the first time? If you have previously submitted a delay request, please include details about when DOJ made its last delay determination(s), on what grounds and for how long it granted the delay (if applicable).

- The FBI will begin investigating the potential national security or public safety implications surrounding the disclosure of a reported incident within two hours of receiving a delay request.
- After the FBI makes a referral based on national security and public safety equities checks and fact-finding procedures, DOJ will issue a delay determination, which will be communicated in writing concurrently to the company and the SEC.
- If DOJ approves the delay request, the FBI should invite the company to submit any subsequent requests for extensions beyond the initial delay period. **A request for an additional period of delay should be made to the FBI at least five business days before the end of the initial period of delay**, and include a description of the continued substantial risk that public disclosure poses to national security or public safety and an estimate of the duration that such risk may last.
- Companies should keep the FBI apprised of any new or changed circumstances relevant to the national security or public safety risks of public disclosure that arise during the delay period.

Related Materials

- Department of Justice Guidelines on Material Cybersecurity Incident Delay Determinations (and related Announcement)
- FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements
- Request a Delay
- FBI Policy Notice (and related Summary)

SEC Staff Compliance and Disclosure Interpretations

On December 12 and December 14, 2023, the SEC's Division of Corporation Finance released the following four Form 8-K C&DIs addressing additional considerations related to the national security and public safety delay provision that is the subject of the new DOJ and FBI guidance summarized above:

Exchange Act Form 8-K

Section 104B. Item 1.05 Material Cybersecurity Incidents.

Question 104B.01

[Initial Delay Requests]

Question: A registrant experiences a material cybersecurity incident, and requests that the Attorney General determine that disclosure of the incident on Form 8-K poses a substantial risk to national security or public safety. The Attorney General declines to make such determination or does not respond before the Form 8-K otherwise would be due. What is the deadline for the registrant to file an Item 1.05 Form 8-K disclosing the incident?

Answer: The registrant must file the Item 1.05 Form 8-K within four business days of its determination that the incident is material. Requesting a delay does not change the registrant's filing obligation. The registrant may delay providing the Item 1.05 Form 8-K disclosure only if the Attorney General determines that disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing before the Form 8-K otherwise would be due. For further information on the Department of Justice's procedures with respect to Item 1.05(c) of Form 8-K, please see *Department of Justice Material Cybersecurity Incident Delay Determinations*, Department of Justice (2023), *at* https://www.justice.gov/media/1328226/dl?inline [December 12, 2023]

Question 104B.02

[Subsequent Delay Requests]

Question: A registrant experiences a material cybersecurity incident, and requests that the Attorney General determine that disclosure of the incident on Form 8-K poses a substantial risk to national security or public safety. The Attorney General makes such determination and notifies the Commission that disclosure should be delayed for a time period as provided for in Form 8-K Item 1.05(c). The registrant subsequently requests that the Attorney General determine that disclosure should be delayed for an additional time period. The Attorney General declines to make such determination or does not respond before the expiration of the current delay period. What is the deadline for the registrant to file an Item 1.05 Form 8-K disclosing the incident?

Answer: The registrant must file the Item 1.05 Form 8-K within four business days of the expiration of the delay period provided by the Attorney General. For further information on the Department of Justice's procedures with respect to Item 1.05(c) of Form 8-K, please see *Department of Justice Material Cybersecurity Incident Delay Determinations*, Department of Justice (2023), *at* https://www.justice.gov/media/1328226/dl?inline [December 12, 2023]

Question 104B.03

[Shortened Delay Periods]

Question: A registrant experiences a material cybersecurity incident and disclosure of the incident on Form 8-K is delayed pursuant to Form 8-K Item 1.05(c) for a time period of up to 30 days, as specified by the Attorney General. Subsequently, during the pendency of the delay period, the Attorney General determines that disclosure of the incident no longer poses a substantial risk to national security or public safety. The Attorney General notifies the Commission and the registrant of this new determination. What is the deadline for the registrant to file an Item 1.05 Form 8-K disclosing the incident?

Answer: The registrant must file the Item 1.05 Form 8-K within four business days of the Attorney General's notification to the Commission and the registrant that disclosure of the incident no longer poses a substantial risk to national security or public safety. *See also* "Changes in circumstances during a delay period" in *Department of Justice Material Cybersecurity Incident Delay Determinations*, Department of Justice (2023), *at* https://www.justice.gov/media/1328226/dl?inline [December 12, 2023]

Question 104B.04

[Consulting Law Enforcement]

Question: Would the sole fact that a registrant consults with the Department of Justice regarding the availability of a delay under Item 1.05(c) necessarily result in the determination that the incident is material and therefore subject to the requirements of Item 1.05(a)?

Answer: No. As the Commission stated in the adopting release, the determination of whether an incident is material is based on all relevant facts and circumstances surrounding the incident, including both quantitative and qualitative factors, and should focus on the traditional notion of materiality as articulated by the Supreme Court.

Furthermore, the requirements of Item 1.05 do not preclude a registrant from consulting with the Department of Justice, including the FBI, the Cybersecurity & Infrastructure Security Agency, or any other law enforcement or national security agency at any point regarding the incident, including before a materiality assessment is completed. [December 14, 2023]

Related Services

Public Companies/Public Offerings

Featured Insights

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding

INSIGHTS

Legal 500 Country Comparative Guides 2025: Venture Capital (Singapore)