December 20, 2023

The DOJ, FBI Release Guidance Regarding New Form 8-K Cybersecurity Incident Reporting Requirements

On July 26, 2023, the Securities and Exchange Commission adopted amendments to Form 8-K to add new Item 1.05, which requires public companies to disclose certain information regarding any material cybersecurity incident within four business days of an assessment that the incident is material.[1] New Item 1.05 of Form 8-K took effect for most public companies on December 18, 2023 (smaller reporting companies have until June 15, 2024 to comply). Item 1.05(c) permits affected entities to delay making the Form 8-K filing where the U.S. Attorney General determines that disclosure of the event would pose a "significant threat to public safety or national security." On December 12, 2023, the Department of Justice released a memorandum that outlines the approach the DOJ will take in determining whether a required disclosure poses such a risk, highlighting the "[l]imited circumstances for finding a substantial risk to national security or public safety" (the "DOJ Memo").[2] The DOJ Memo followed separate guidance released by the Federal Bureau of Investigation on December 6, 2023, regarding the process by which victim companies can request a determination whether delayed disclosure is appropriate (the "FBI Guidance").[3] As we explain in more detail below, the DOJ Memo makes clear that entities that are victims of a cybersecurity incident which they believe may qualify for delayed disclosure should act promptly to request delayed disclosure, as neither the request nor the government's consideration of the request will toll the four business day period for the Form 8-K filing.

Overview of Item 1.05 of Form 8-K

Companies must now make a filing pursuant to Item 1.05 of Form 8-K within four business days of a determination that the entity has experienced a "material" cybersecurity incident. A cybersecurity incident 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," and any uncertainty regarding the materiality of an incident should be resolved with the interests of investors in mind. Companies are not required to disclose whether the incident has been remediated, whether the incident is ongoing or whether any data was compromised.

Under Item 1.05(c), should the DOJ determine that the disclosure of a cybersecurity event "poses a substantial risk to national security or public safety," the Attorney General may grant an extension of 30 days for the company's Form 8-K filing, with an option for an additional 30 day delay. A further 60-day extension may be granted—for a total delay of 120 days—where the DOJ determines that disclosure of the cybersecurity event continues to pose a substantial national security threat (but not a public safety risk). Further delays can be granted through an SEC exemptive order. Per Compliance and Disclosure Interpretations

1 Securities and Exchange Comm'n, Fed. Reg. 51896, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, available here. See our prior memorandum describing these amendments here.

2 Dep't of Justice, *Department of Justice Material Cybersecurity Incident Delay Determinations* (Dec. 12, 2023), available here.

3 Federal Bureau of Investigation, *Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Policy Notice 1297N* (Dec. 6, 2023), available here.

issued by the SEC on December 14, 2023 (the "SEC C&DIs"), the mere filing of a request for a delay does not alter the four business day filing deadline: only after the DOJ issues a determination granting a delay is the requesting entity's filing deadline changed. The DOJ may revise its determination that a disclosure delay under Item 1.05(c) is warranted during the pendency of a delay period; should it do so, the affected entity has four business days to then make the Item 1.05 Form 8-Kfiling.

DOJ Memo

The DOJ Memo describes the guidelines used by the DOJ to evaluate requests for delays of Item 1.05 disclosures. The DOJ Memo emphasizes that the "primary inquiry" in determining whether a delay under Item 1.05(c) is appropriate is "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." Circumstances in which the disclosure of a cybersecurity incident could pose such a threat include where:

- disclosure would "risk revealing a confidential source, information relating to U.S. national security, or law enforcement sensitive information," particularly where "the registrant learned of the cybersecurity incident only because" a government agency alerted the registrant to the incident or the risk of such an incident;

- the U.S. Government is contemplating or initiating an operation to disrupt illegal cyber activity, and disclosure of the cyber incident would imperil the operation; and

- the U.S. Government is remediating vulnerabilities in critical infrastructure or critical systems, and disclosure of the cyber incident would undermine those remediation efforts.

The DOJ "has sole discretionary authority" to determine whether a substantial threat to national security or public safety exists, and how long the threat persists, for the purposes of delays under Item 1.05(c). In assessing a request under Item 1.05(c), the DOJ may consult with other government agencies, including the U.S. Secret Service, the FBI and relevant Sector Risk Management Agencies. Attorney General decisions regarding requests for Item 1.05 filing delays are conveyed to the SEC, the affected entity and any government agency that recommended the delay.

FBI Guidance

The FBI Guidance provides companies with a mechanism to request a delay in making an Item 1.05 Form 8-K filing, as described by Item 1.05(c). Per the FBI Guidance, the FBI is responsible for intaking requests for delays to Item 1.05 disclosure delays. The FBI may receive such requests from the affected entity itself, the Cybersecurity and Infrastructure Security Agency ("CISA") or other government agencies. After reviewing information associated with the cybersecurity incident, including: (i) the time of the incident and the materiality determination; (ii) the type of incident that occurred; (iii) any suspected or known vulnerabilities leveraged by the intruder; (iv) confirmed or suspected attribution of the responsible cyber actors; and (v) remediation status, the FBI will determine whether a timely Form 8-K filing would pose a credible threat to either public safety or national security. If the FBI makes such a finding, it can refer the request to the DOJ, where the Attorney General would issue a final determination regarding whether the company may delay disclosing the material cybersecurity incident on Form 8-K.

Takeaways

- A determination that a company may delay public disclosure of a material cybersecurity incident will be rare, absent facts that fall within the narrow circumstances implicating national security or public safety described in the DOJ Memo and FBI Guidance. Although the exemption is narrow, there will be circumstances such as incidents involving zero day vulnerabilities where delay may be appropriate, but companies will need to work quickly and in close coordination with the FBI for such delay to be available.

- The FBI Guidance underscores the benefits of early outreach to the FBI before a company determines that an incident is material. Merely consulting with the FBI will not result in a determination that an incident is material. In addition to other

support that law enforcement can provide to victim organizations, early engagement allows the FBI to familiarize itself with the facts and circumstances of an incident and may enable it to more quickly review a later request for disclosure delay.

- Requests for delay may also be routed through other federal agencies. Although companies may initially contact CISA, the U.S. Secret Service or other law enforcement agencies—and these agencies may have other unique support to offer victims—all requests for delayed Item 1.05 Form 8-K disclosure will ultimately be routed through the FBI for assessment and a determination by the Attorney General.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Luke Jennings
+1-212-373-3591
ljennings@paulweiss.com

Christodoulos Kaoutzanis
+1-212-373-3445
ckaoutzanis@paulweiss.com

John C. Kennedy
+1-212-373-3025
jkennedy@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Raphael M. Russo
+1-212-373-3309
rrusso@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associate Neil Chitrao contributed to this Client Memorandum.