

SEC Cybersecurity Rules: FBI, DOJ and SEC Publish Guidance on Disclosure Delays

December 18, 2023

The SEC's [new cybersecurity rules](#) for public companies became effective on December 18, 2023. The rules require disclosure of a cybersecurity event within four business days of a [determination that it is material](#). They also provide that such disclosure may be delayed for up to 30 days if the United States Attorney General (or per DOJ guidelines, the Attorney General's authorized designees) determines that immediate disclosure would pose "a substantial risk to national security or public safety, and notifies the SEC of such determination in writing." Two subsequent delay periods of 30 days and 60 days (in extraordinary circumstances) may also be sought.

The FBI and the DOJ recently issued guidelines for companies seeking such delays. In this post, we discuss the logistics of making a delay request and offer [several tips](#) for companies to prepare for potentially material cybersecurity incidents that may involve making such a request.

FBI's Guidance and Policy Notice. On December 6, the FBI, in coordination with the DOJ, published [guidance](#) and a [Policy Notice](#) on how victimized companies can request disclosure delays for national security or public safety reasons. First, the FBI recommends that public companies establish a relationship with the cyber squad at their local FBI field office before any potentially material cyber incident occurs. Second, during an incident, the FBI "strongly encourages" victims to engage with the FBI directly (or through U.S. Secret Service (the "USSS"), the Cybersecurity and Infrastructure Security Agency (the "CISA") or another sector risk management agency ("SRMA")) *prior* to making a materiality determination. Third, the FBI warns that if it does not receive a delay request "concurrently" with the materiality determination, it will not process the request.

As outlined in the Policy Notice, the FBI is responsible for: (1) intaking delay requests on behalf of the DOJ, (2) documenting those requests; (3) coordinating checks of U.S. government national security and public safety equities, including consulting with the USSS, CISA and SRMAs as appropriate; (4) referring the request forms to the DOJ; (5) conducting follow-up victim engagement, as appropriate; and (6) coordinating and

documenting requests for additional delay referrals. The FBI will also soon provide a dedicated email address for initial reporting delay requests and delay extension requests.

The FBI's guidance lists 10 items that must be included in each delay request:

- The name of the company;
- The date when the cyber incident occurred;
- Details (date, time and time zone) regarding when the victim company determined that the cyber incident was material such that it would require disclosure on Form 8-K or Form 6-K under the SEC's final cyber disclosure rules. *The FBI explains that failure to report this information immediately upon determination will cause a delay-referral request to be denied.*
- Whether the victim company is already in contact with the FBI or another U.S. government agency regarding this incident (and, if so, the names and field offices of the FBI points of contact or information regarding the applicable U.S. government agency);
- A description of the cyber incident in detail that includes, at a 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 they were affected;
 - What the operational impact on the company is, if known;
- Whether there is any confirmed or suspected attribution of the cyber actors responsible;
- The current status of any remediation or mitigation efforts;
- The location where the cyber incident occurred (including street address, city and state);
- The company's points of contact for the matter (including name, phone number and email address of personnel the company wants the FBI to contact to discuss the request); and

-
- Whether the company has previously submitted a delay referral request or if this is the first time. If the company has previously submitted a delay request, the victim company should include details about when the DOJ made its last determination(s), on what grounds and for how long the DOJ granted a delay (if applicable).

DOJ's Guidelines. On December 12, the DOJ [issued](#) its [departmental guidelines](#) for material cybersecurity incident delay determinations. The guidelines explain that the “primary inquiry” for the DOJ is “whether the *public disclosure* of a cybersecurity incident threatens public safety and national security, not whether the incident itself poses a substantial risk to public safety and national security.” The guidelines outline four categories of “limited circumstances” in which the DOJ believes the disclosure of some or all of the information required by new Item 1.05 of Form 8-K (“Item 1.05”) could pose a substantial risk to national security or public safety:

- A cybersecurity incident involves a technique for which there is not yet a well-known mitigation (*e.g.*, zero-day vulnerability), and the disclosure required by Item 1.05 could lead to more incidents.
- The cybersecurity incident primarily impacts a system operated or maintained by a registrant that contains sensitive U.S. government information (*e.g.*, information regarding national defense or research and development performed pursuant to government contracts), and public disclosure required by Item 1.05 would increase vulnerability to further exploitation by illicit cyber activity.
- The registrant is conducting remediation efforts, and any disclosure required by Item 1.05(a) revealing that the registrant is aware of the incident would undermine those remediation efforts.
- Circumstances in which the U.S. government, rather than a registrant, is likely to be aware of a substantial risk to national security or public safety and in which the government has made the registrant aware of the circumstances.

For the fourth category, the DOJ anticipates that relevant scenarios may be those: (i) where disclosure would risk revealing a confidential source, information relating to U.S. national security or law enforcement sensitive information; (ii) where the U.S. government is prepared to execute, or is aware of, an operation to disrupt ongoing illicit cyber activity; and (iii) where the U.S. government is aware of or conducting remediation efforts for any critical infrastructure or critical system. In these instances, the government might try to obtain the registrant's agreement to delay a disclosure.

Steps to Consider. Given the publication of these resources, as well as the FBI's and the DOJ's comments at the recent [2023 Aspen Institute Cyber Summit](#), companies should consider the steps outlined below.

- **Consider updating incident response plans to incorporate relevant factual predicates from, and ensure timely compliance with, the guidelines.** It is important to confirm that cyber incident response plans and procedures ensure timely assessment of whether the disclosure of an incident may present substantial risks to national security or public safety, and therefore be considered for a notification delay from the DOJ. Such plans and procedures should favor early reporting to law enforcement in any situation where these issues have the potential to be relevant in the incident. The guidelines include several examples of cybersecurity incidents (*e.g.*, zero-day vulnerability exploits) and key factual questions that companies should include in their plans in order to inform their analysis.
- **Consider enhancing relationships with applicable FBI local field offices, including points of contact on the FBI cyber squads.** The FBI will play a central role in the DOJ's determinations regarding disclosure delay requests. Having established direct or indirect (*e.g.*, through cyber counsel) relationships with FBI contacts and promptly initiating contact with the FBI about an incident will be critical, as a failure to report a cyber incident immediately upon determination of materiality will cause a delay-referral request to be denied. Additionally, the FBI's guidance emphasizes reporting to the FBI early is important in order to manage the lead time necessary to make a disclosure delay determination.
- **Consider reviewing and updating disclosure analysis and escalation procedures to incorporate the FBI and the DOJ guidelines, as well as interpretations recently issued by the SEC.** The SEC made clear in recently issued [compliance and disclosure interpretations](#) that requesting a delay alone does not toll the registrant's filing obligation. Importantly, the SEC confirmed that if the Attorney General declines to make a determination whether disclosure of the incident poses a substantial risk to national security or public safety or does not respond before the Form 8-K otherwise would be due, the registrant must file the Item 1.05 Form 8-K within four business days of its determination that the incident is material (or within four business days of end of the initial delay period, if the request relates to a delay extension). Registrants should therefore ensure that their disclosure analysis and escalation procedures align with best practices from the guidelines and ensure timely outreach to the FBI and the DOJ. The director of the SEC's Division of Corporation Finance also reiterated, in a [recent speech](#), that a decision to contact the FBI or the DOJ about a cybersecurity incident does not trigger a materiality determination. However, this will only be relevant prior to submitting a request for delay, as the

request form requires an indication of when the incident was determined to be material.

* * *

Please do not hesitate to contact us with any questions.



Charu Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com



Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com



Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com



Benjamin R. Pedersen
Partner, New York
+1 212 909 6121
brpedersen@debevoise.com



Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com



Alice Gu
Associate, New York
+1 212 909 6057
agu@debevoise.com



Paul D. Lowry
Associate, New York
+1 212 909 6198
pdlowry@debevoise.com



Michael R. Roberts
Associate, New York
+1 212 909 6406
mrroberts@debevoise.com