Published on *The National Law Review* https://natlawreview.com

For Limited Use Only: Guidance on National Security Delay Determinations under the SEC Cyber Reporting Rule

Article By:

Townsend L. Bourne

Nikole Snyder

On December 12, 2023, the Department of Justice ("DOJ") issued guidance related to the process by which companies may request the United States Attorney General authorize delays of cyber incident disclosures, pursuant to a new Securities and Exchange Commission ("SEC") rule. As a reminder, the SEC rule (which went into effect on Dec. 18, 2023) requires companies to disclose material cyber incidents via Form 8-K within four days of making a materiality determination. Our colleagues previously discussed the SEC rule and its new cyber reporting requirements here.

Notably, the SEC rule includes an exception that the registrant may delay providing the disclosure "if the United States Attorney General determines that disclosure [. . .] poses a substantial risk to national security or public safety [. . .]." This language exception piqued the interest of many federal contractors, who anticipated the national security exception might readily apply broadly to cyber incidents related to their federal – and particularly defense – contract work. The new guidance from DOJ, however, largely puts an end to that interpretation.

The DOJ guidance clarifies that the exception is to be used only in limited circumstances. In particular, DOJ provides four categories of "limited circumstances for finding a substantial risk to national security or public safety," including:

1. the illicit cyber activities were reasonably suspected to have involved a technique for which there is not yet well-known mitigation;
2. the incident primarily impacts a system that contains sensitive U.S. Government information and public disclosure would make that information and/or system vulnerable to further exploitation by illicit cyber activity;
3. the registrant is conducting remediation efforts for any critical infrastructure or critical system and disclosure would undermine those efforts; or
4. where the Government (rather than the registrant) has made the registrant aware that disclosure would pose a substantial risk to national security or public safety, including where:
    - disclosure of the incident would risk revealing a confidential source, information relating to U.S. national security, or law enforcement sensitive information;
    - disclosure of the incident would pose a demonstrable threat/impediment to the

Government's operation to disrupt ongoing illicit cyber activity that poses a risk to national security or public safety (e.g., freezing/seizing information or assets; arresting individuals; etc.); or
- revealing the registrant is aware of an incident would undermine the Government's remediation efforts for a critical infrastructure system and thus pose a substantial risk to national security or public safety.

The guidance also clarifies "the primary inquiry for the Department 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." As such, the focus is on the information to be included in the disclosure of the incident rather than the incident (or the systems or sensitive information at issue) itself. During meetings with industry, agency officials suggested that in most cases the disclosure can be written to avoid providing information that would necessitate a national security or public safety delay.

In parallel, the Federal Bureau of Investigation ("FBI") released its own guidance that provides more information on requesting a national security delay. Unlike the DOJ guidance, which (among other things) focuses on the circumstances under which a delay may be provided, the FBI provides the method for submitting a request and a list of 10 items that must be included in any request for a disclosure delay. Requests may be emailed directly to the FBI via the following address – cyber_sec_disclosure_delay_referrals@fbi.gov – or submitted through the U.S. Secret Service, the Cybersecurity and Infrastructure Security Agency, the Department of Defense, or another sector risk management agency. Importantly, the FBI guidance asks when the registrant made the determination to disclose the incident on the Form 8-K, and states (in bold!) that "Failure to report this information immediately upon determination will cause your delay-referral request to be denied." As such, this makes clear that, at the same time companies make the materiality determination, they also will need to assess and decide whether the incident may fall into one of the four limited categories outlined above.

Overall, the DOJ guidance confirms that delays will be granted only in very limited circumstances. However, if a company is planning to request a delay based on one of the limited exceptions, it must do so immediately upon determining the incident was "material." It remains to be seen whether the Attorney General will be able to make the delay determination before the expiration of the 4-day deadline for the company to make its report via the Form 8-K, or if companies will be given a grace period while the determination is pending.

National Law Review, Volume XIV, Number 19