wiley

ALERT

Cyber Incident Reporting Guidance: DOJ Explains How It Will Determine if a Public Disclosure Poses Substantial National Security or Public Safety Risk

December 13, 2023

The cyber reporting landscape is rapidly shifting. Many agencies are developing rules, and a major player has been the U.S. Securities and Exchange Commission (SEC), with important questions arising about implementation of its narrow mechanism for delaying public reporting. As compliance deadlines loom, we have seen a flurry of activity. We now have new insights into how companies can try to delay public disclosure of a cybersecurity incident for national security and public safety reasons.

Both the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) have now issued guidance explaining the process companies can use to request a determination, by the U.S. Attorney General, that publicly disclosing a material cyber incident poses a substantial risk to national security and public safety justifying the delay of the public disclosure of the incident required on SEC Form 8-K Item 1.05(a).[1]

The day after the FBI published its *Guidance to Victims of Cyber Incidents on SEC Reporting Requirements* and internal Policy Notice on *Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure* explaining how to request a public disclosure reporting delay, DOJ issued its own guidelines explaining how DOJ will review and adjudicate delay requests. In *Department of Justice Material Cybersecurity Incident Delay Determinations*, DOJ outlines the limited circumstances in which the Department may find a substantial risk to national security or public safety posed by the

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

National Security

Privacy, Cyber & Data Governance

public disclosure of a cybersecurity incident. The new DOJ guidelines also outline procedures for U.S. government agencies to request notification delays in coordination with registrants.

We covered the FBI's December 11 guidance and policy notice about the process for seeking delays, and we share below insights into this even more recent development from DOJ. Both sets of guidelines highlight the importance of timing – delay public disclosure notification requests must be made immediately after a company makes a materiality decision. While the FBI has put in place internal procedures to promptly process delay requests, the four (4) day public disclosure clock set by the SEC continues to tick.

Our review of the DOJ request adjudication guidelines indicate that DOJ contemplates granting those requests only in limited circumstances. This means that for most cybersecurity incidents, companies will likely be unable to delay reporting and will need to move forward with public reporting of the cyber incident within four (4) business days of determining that the incident is material.

FBI and DOJ Guidance Describe a Multi-Step Process for Seeking a Delay of Public Disclosures, But Prospects of Having a Request Granted Seem Narrow

Taken together, the FBI and DOJ guidelines contemplate a multi-step process that companies should be aware of:

1. Companies should contact the FBI either directly or through the U.S. Secret Service, the Cybersecurity and Infrastructure Security Agency (CISA) or another sector risk management agency (SRMA) as soon as the registrant believes disclosure of a newly discovered cybersecurity incident may pose a substantial threat to national security or public safety. Timing is critical here because the FBI says it won't process delay requests unless they are received by the FBI immediately upon a company's determination to disclose a cyber incident via Form 8-K.
2. The company will need to provide the FBI with ***all*** the information it needs to request a delay as set forth in the FBI's Guidance to Victims of Cyber Incidents on SEC Reporting Requirements: Request a Delay.
3. The FBI will process delay requests on behalf of DOJ, check with other U.S. government agencies about national security and public safety equities, and refer the delay request to DOJ as indicated by the FBI Policy Notice.
4. DOJ will then review the delay notification request in accordance with delay determination guidance the Department issued on December 12, 2023.
5. In limited circumstances, DOJ will find that the public disclosure of a cybersecurity incident threatens national security and public safety and will notify the SEC of that determination in writing, which will delay the notification period for up to 30 days, with subsequent periods of delay available for limited durations.

Here's what you need to know about DOJ's delay request adjudication process:

When Will DOJ Find a Substantial Risk to National Security or Public Safety to Justify Delayed Public Disclosure of a Material Cyber Incident?

The new guidelines make clear that the primary inquiry for DOJ 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 or national security. While cybersecurity incidents themselves frequently threaten public safety and national security, DOJ maintains that the disclosure to the public of these incidents poses a threat less often. In many circumstances, DOJ says that the prompt disclosure of relevant information about a cybersecurity incident provides an overall benefit for investors, public safety, and national security.

What Should a Public Company Registrant Consider in Deciding Whether This Delay Mechanism Could be Helpful?

Form 8-K Item 1.05 requires registrants to "describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."

Per DOJ, a registrant should consider seeking a notification delay in the following circumstances:

- The cybersecurity incident occurred because the illicit cyber activities were reasonably suspected to have involved a technique with a not yet well-known mitigation measure (e.g., software vulnerability with no patch) or the required disclosure could lead to more incidents, thereby posing a substantial risk to national security or public safety.
- The cybersecurity incident primarily impacts a system containing sensitive U.S. government information and public disclosure would make that information and/or system vulnerable to further exploitation by illicit cyber activity, thereby posing a substantial risk to national security or public safety. This category includes systems operated or maintained for the government as well as systems not specifically operated or maintained for the government that contain information the government would view as sensitive, such as that regarding national defense or research and development performed under government contracts.
- The registrant is conducting remediation efforts for any critical infrastructure or critical system, and any required disclosure that reveals that the registrant is aware of the incident would undermine those remediation efforts and thus pose a substantial risk to national security or public safety. This does not contemplate delay to prevent further harm to the victim's operations or business, which suggests delay will be available in a relatively narrow set of circumstances.
- When a government agency has made the registrant aware that circumstances exist that require delaying disclosure.

What Should a Public Company Registrant do in Light of These Developments?

Organizations under cyberattack face an array of considerations and decisions, including when and how to work with the FBI and other government agencies. Several hard questions can arise related to public and government disclosure of cyber incidents. Disclosures before key facts are known, before data or system analysis is complete, or before remediations have been done, can expose organizations, their customers, and employees to further victimization. Premature disclosures also can interfere with ongoing internal and criminal investigations that the victim is cooperating with. But the SEC appears unconcerned with these impacts, and DOJ's new guidelines suggest that it will only authorize delays of material cyber incidents in narrow circumstances.

In light of the new SEC rule and this DOJ guidance, when a registrant discovers a cybersecurity incident and believes that public disclosure may pose a substantial risk to national security or public safety, the registrant should immediately contact the FBI in accordance with the FBI's reporting instructions. The registrant may contact the FBI directly or through another agency (e.g., the U.S. Secret Service, another federal law enforcement agency, the Cybersecurity & Infrastructure Security Agency (CISA), or another sector risk management agency (SRMA)).

The registrant should convey a concise description of the facts and why it believes that disclosure may pose a substantial risk to national security or public safety. DOJ says that the most relevant facts will pertain to the potential consequences to national security or public safety that would results from a disclosure.

DOJ recommends that registrants contact the FBI about delayed notification as soon as possible, even before the registrant has completed its materiality analysis or its investigation into the incident.

What Happens Once a Registrant Asks for Delayed Notification to the SEC?

The FBI's referral of a delay request to DOJ will include an evaluation of whether the public disclosure required by Form 8-K Item 1.05, within the prescribed time frame, would pose a substantial risk to national security or public safety.

The DOJ will then review the submitted information. The Attorney General must invoke the provision in the SEC rules permitting a delay in disclosing an incident within four (4) business days of a determination by the registrant that the registrant has experienced a material cybersecurity incident.

A U.S. Government Agency May Also Seek a Delay of Public Reporting in Coordination With a Registrant

When any U.S. government agency becomes aware of a cybersecurity incident pertaining to a registrant's information system and believes the available facts show that a disclosure is potentially required poses a substantial risk to national security or public safety, the DOJ guidelines provide that the agency should, in consultation with the FBI and other agencies as appropriate, determine whether the U.S. government should notify and coordinate with the registrant to determine the timing and content of the information to be disclosed. Once a U.S. government agency determines that a delay in public disclosure is warranted and

agreed to by the registrant, the DOJ guidelines mandate that the agency immediately contact DOJ through the FBI.

DOJ anticipates that a U.S. government agency, rather than a registrant, may be aware of a substantial risk to national security or public safety in the following circumstances:

- Disclosure to the public of the cybersecurity incident would risk revealing a confidential source, information relating to U.S. national security, or law enforcement sensitive information and thereby pose a substantial threat to national security or public safety. DOJ believes the risk that disclosure will pose a substantial threat to national security or public safety is higher where the registrant learned of the cybersecurity incident only because a U.S. government agency alerted the registrant to the cybersecurity incident or its possible occurrence.
- The U.S. government is preparing to execute an operation to disrupt ongoing illicit cyber activity that poses a substantial risk to national security or public safety, such as freezing or seizing information, assets, or infrastructure involved in illicit cyber activity, or by effecting the arrest of an individual(s) for illicit cyber activity, and public disclosure of the cybersecurity incident would pose a demonstrable threat or impediment ot the success of such an operation.
- The U.S. government is aware of or conducting remediation efforts for any critical infrastructure or critical system, and any disclosure revealing that the registrant is aware of the incident would undermine those remediation efforts and pose a substantial risk to national security or public safety.

What Happens After the Public Company Registrant's Delay Notification Request Gets to DOJ?

When the Attorney general determines that disclosure poses a substantial risk to national security or public safety, DOJ will notify the SEC in writing. DOJ will also notify the recommending agency and the registrant of its determination. DOJ will also notify both if it decides that the standard for a disclosure delay is not warranted.

How Do These New Guidelines Affect Information Sharing or Cyber Regulatory Deconfliction?

The new DOJ guidelines are limited to the public disclosure requirements contained in Item 1.05 and do not affect other statutory or regulatory reporting requirements that may be legally required or prudentially advisable.

DOJ was also careful to note that future rulemaking under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) or the Cyber Incident Reporting Council's directive to harmonize mandatory cyber incident reporting under CIRCIA may affect these guidelines. DOJ noted that it will reassess these guidelines after the CIRCIA rulemaking is complete.

What Are the Implications for Affected Companies?

DOJ's guidelines highlight the importance of reaching out to and coordinating with law enforcement when a cybersecurity incident first occurs, if the company anticipates the incident may end up being deemed material. Companies should keep in mind that they need to report a cybersecurity incident to the SEC under its new rules within four (4) days of making a materiality determination. Prompt coordination with law enforcement can facilitate seeking a delay in the required notification for national security or public safety reasons, but the burden is generally on the company to determine that this exception may be applicable.

Cybersecurity incidents involving novel vulnerabilities, sensitive U.S. government information, or critical infrastructure are the types of incidents that DOJ is most likely to seek delayed notification for. It's also interesting to note that the U.S. government may determine on its own that delayed notification may be appropriate and then seek the concurrence of the victim company.

Public companies may want to review their incident response plans to build in early consideration of law enforcement outreach that includes evaluation of whether and when to seek a delay based on threats to public safety or national security. Companies may also want to invest in working relationships with trusted counsel and internal security stakeholders, including in-house counsel, who can interact with the FBI and DOJ early in an incident, where it becomes appropriate.

[1] When a registrant "experiences a cybersecurity incident that is determined by the registrant to be material," requires the registrant to disclose within four (4) business days "the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations." There is an important exception to the general disclosure requirement if the Attorney General determines that disclosure poses a substantial risk to national security or public safety and notifies the SEC in writing. If that happens, then the registrant may delay providing the required public disclosure for up to 30 days subject to limited extensions. It is that Attorney General's determination that is the subject of DOJ's recent guidance.