DOJ, FBI, AND SEC PROVIDE GUIDANCE FOR DELAY REQUESTS RELATING TO DISCLOSURE OF CYBERSECURITY INCIDENTS UNDER FORM 8-K

Date: 3 January 2024

US Corporate Alert

By: Patrick J. Rogers, David A. Bartz, Guillermo S. Christensen, Hillary Pellerin O'Rourke

On 18 December 2023, the new rules[1] of the US Securities and Exchange Commission (SEC) regarding disclosure of material cybersecurity incidents under Item 1.05 of Form 8-K went into effect, requiring companies[2] to report a cybersecurity incident within four business days of determining the incident is material. The new rules include a limited exception providing that reporting companies may delay the filing of such a Form 8-K if the US Attorney General (AG) determines immediate disclosure would pose a substantial risk to national security or public safety.

DOJ GUIDELINES ON DELAY DETERMINATIONS

On 12 December 2023, the Department of Justice (DOJ) issued guidelines for companies to follow in requesting that the AG authorize delays of cybersecurity incident disclosures required by the SEC pursuant to Item 1.05 of Form 8-K. Pursuant to the DOJ's guidelines, the primary inquiry is whether the public disclosure of a cybersecurity incident (not the incident itself) threatens public safety or national security. These guidelines also offered examples of when a delay in reporting may be warranted, such as:

- The cybersecurity incident occurred because the illicit cyber activities were reasonably suspected to have involved a technique for which there is not yet well-known mitigation;
- The cybersecurity incident primarily impacts a system operated or maintained by a company that contains sensitive US government information, or information the US government would consider sensitive, and disclosure would make that information or system vulnerable to further exploitation by illicit cyber activity;
- The company is conducting remediation efforts for a critical infrastructure or critical system, and disclosure revealing that the company is aware of the incident would undermine those remediation efforts; or
- A US government agency believes the available facts show that disclosure poses a substantial risk to national security or public safety and has made the company aware of them.

When a company believes that disclosure of a cybersecurity incident may pose a substantial risk to national security or public safety, it should immediately contact the Federal Bureau of Investigation (FBI), which will initiate a complex process within the DOJ to assess the national security risks. The AG must make a determination, based on the company's request and the FBI's assessment, as to whether or not to permit a disclosure delay

©2005-2026 K&L Gates LLP. All Rights Reserved.

within four business days of a company's determination that a cybersecurity incident is material. It will therefore be important to communicate with the FBI early and often in the event of a cybersecurity incident, potentially even before a company makes a materiality determination.

The DOJ exception will likely apply to very few cybersecurity incidents, and the DOJ guidelines note that, typically, companies will be able to publicly disclose this material information at a level of generality that does not pose a substantial risk to national security or public safety.

FBI GUIDANCE ON PROCEDURES FOR DELAY REQUESTS

The FBI, in coordination with the DOJ, recently announced that companies requesting disclosure delays should contact the FBI directly or through the US Secret Service, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Defense, or another sector risk management agency. The FBI's guidance outlines the detailed information a company must provide regarding the cybersecurity incident, which includes the type of cybersecurity incident, the timing of both the incident and the company's materiality determination, and other specific information concerning the incident, the company and the company's prior communications with US government agencies related to the incident.

If the AG determines that disclosure would pose a substantial risk to national security or public safety, the DOJ is to notify the SEC of such determination in writing.

SEC COMPLIANCE AND DISCLOSURE INTERPRETATIONS ON MATERIAL CYBERSECURITY INCIDENTS

On 12 December and 14 December 2023, the SEC issued four Compliance and Disclosure Interpretations regarding disclosure delays that provide as follows:

AG does not respond or declines to respond to delay request for initial delay period–Form 8-K due within four business days of materiality determination

If a company requests a disclosure delay from the AG and the AG does not respond or declines to respond before the Form 8-K filing deadline, the company is still required to file the Form 8-K within four business days of determining that the incident is material. A company may only delay the disclosure if the AG notifies the SEC in writing before the Form 8-K otherwise would be due of its determination that a delay is justified.

AG does not respond or declines to respond to delay request for additional delay period–Form 8-K due within four business days of expiration of current delay period

If the AG grants an initial disclosure delay and notifies the SEC accordingly and the company requests an additional delay period, but the AG does not respond or declines to respond before the expiration of the current delay period, the company is required to file the Form 8-K within four business days of the expiration of the current delay period.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Incident no longer poses a substantial risk to national security or public safety–Form 8-K due within four business days of such notification from the AG

If, after granting a disclosure delay, the AG determines that disclosure of the incident no longer poses a substantial risk to national security or public safety, the company is required to file the Form 8-K within four business days of the AG's notification to the company and the SEC that the disclosure of the incident no longer poses a substantial risk to national security or public safety.

Consultation does not necessarily equate to materiality

The fact that a company consults with the DOJ, including the FBI, CISA, or any other law enforcement or national security agency, regarding the availability of a disclosure delay does not necessarily mean that the company must deem the incident to be material. A materiality determination should be based on the traditional materiality standards and should take into account all relevant facts and circumstances surrounding the incident. This guidance was emphasized in the 14 December 2023 statement of Erik Gerding, director of the SEC's Division of Corporation Finance.

NEXT STEPS AND RECOMMENDATIONS

Companies should establish a relationship with the cyber division of their local FBI field offices as soon as practicable, as they will be the primary points of contact in the event of a cybersecurity incident. Timely engagement will be crucial if the need to communicate with the FBI arises. The contact information of the FBI's field offices can be found here. In the case of a cybersecurity incident, companies should engage experienced outside cyber counsel to advise in the assessment and notification process, including the preparation of the delay request. Experienced cyber experts can help companies avoid unnecessary disclosures, minimize delays inherent in the agency review and disclosure delay approval process, and protect client confidentiality and privilege.

We also recommend that companies subject to the SEC rules review and revise their incident response protocols to incorporate processes to ensure rapid incident assessments and materiality determinations. Additionally, we recommend that companies undertake tabletop exercises specifically tailored to test their incident response plans in circumstances where SEC disclosure obligations may be implicated. Our cybersecurity team has extensive experience with incident response and strong contacts within the FBI and thus can provide valuable assistance in cybersecurity incident preparation, response, and mitigation.

FOOTNOTES

[1] We previously analyzed the SEC's new cybersecurity incident reporting rules in the following client alert and webinar available on the K&L Gates Hub: SEC Adopts Final Rules for Cybersecurity Disclosures and SEC's Final Public Company Cybersecurity Disclosure Rules.

[2] Smaller reporting companies are not subject to the new Form 8-K disclosure requirements until 15 June 2024.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



PATRICK J. ROGERS
PARTNER

CHARLOTTE
+1.704.331.5712
PATRICK.ROGERS@KLGATES.COM



DAVID A. BARTZ
PARTNER

NASHVILLE, DALLAS, HOUSTON
+1.615.780.6743
DAVID.BARTZ@KLGATES.COM



GUILLERMO S. CHRISTENSEN
PARTNER

WASHINGTON, DC
+1.202.778.9095
GUILLERMO.CHRISTENSEN@KLGATES.COM



HILLARY PELLERIN O'ROURKE
PARTNER

BOSTON
+1.617.951.9104
HILLARY.OROURKE@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.