Hogan Lovells

SEC Update

January 9, 2024

This is a commercial communication from Hogan Lovells. See note below.

Agencies issue guidance on delayed SEC reporting of material cybersecurity incidents

Since December 18, 2023 public companies other than smaller reporting companies are required to report a cybersecurity incident under Item 1.05 of Form 8-K within four business days after the company determines the incident is material.

Item 1.05(c) of Form 8-K permits a company to delay disclosing a material cybersecurity incident for a limited period of time if the U.S. Attorney General determines that the disclosure required by Item 1.05(a) poses a substantial risk to national security or public safety. The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) recently issued guidance describing the process for making that determination. The process requires the company experiencing the incident or a U.S. government agency in some circumstances to submit to the FBI a written request for delayed disclosure.

In addition, the SEC's Division of Corporation Finance has issued compliance and disclosure interpretations (C&DIs) under Form 8-K clarifying the application of the Item 1.05 filing deadline when delayed disclosure may be available.

The DOJ guidelines with respect to Item 1.05(c) determinations can be viewed here, while the FBI's guidance and its related policy statement can be viewed here and here. The new C&DIs can be seen here.

Delayed disclosure authorized by Item 1.05(c)

Item 1.05(c) permits a company to delay disclosure of a material cybersecurity incident beyond the filing deadline of four business days after the company's materiality determination if the U.S. Attorney General determines that the Item 1.05(a) disclosure "poses a substantial risk to national security or public safety" and notifies the SEC in writing of its determination.

The new guidance emphasizes that, as specified in Item 1.05(c), a delay is permitted only if the risk to national security or public safety is posed by public disclosure of the incident, rather than by the incident itself.

Item 1.05(c) authorizes delayed disclosure periods that, taken together, provide for a delay of up to 60 days if the Attorney General determines that the required disclosure poses a substantial risk related solely to public safety, and up to 120 days if it determines that the disclosure poses a substantial risk to national security.

Item 1.05(c) states that:

- the Attorney General may initially approve a delayed disclosure period of up to 30 days based on the required determination of a substantial risk to national security or public safety;
- if the Attorney General determines that disclosure of the incident continues to pose such a risk, disclosure may be delayed for an additional period of up to 30 days; and
- in "extraordinary circumstances," disclosure of the incident may be delayed for a "final additional period of up to 60 days" if the Attorney General determines that disclosure continues to pose a substantial risk to national security.

Item 1.05(c) provides that the Attorney General will specify the length of the delayed disclosure period in the determination notice it delivers to the SEC.

Item 1.05(c) further states that, if the Attorney General determines that a disclosure delay beyond the final 60-day delay period is necessary, the SEC will consider additional requests for delay and may grant additional relief from the disclosure deadline by an exemptive order. In its 2023 adopting release for the new cybersecurity disclosure rules, the SEC noted that exercise of its exemptive authority would have to

meet the standards of Exchange Act Section 36, which requires the SEC to determine that the exemption is necessary or appropriate in the public interest, and is consistent with the protection of investors.

Summary of guidance relating to Item 1.05(c)

SEC staff guidance on delayed disclosure

On December 12 and 14, 2023, the SEC staff published C&DIs under Form 8-K providing guidance on the operation of Item 1.05(c) in relation to the DOJ's guidelines for making delay determinations.

The SEC staff underscores that a *request* for a disclosure delay is not sufficient to relieve a company of its obligation to report a material cybersecurity incident within four business days after it has determined that the incident is material. Delayed disclosure is authorized only if the requirements of Item 1.05(c) – consisting of the Attorney General's risk determination and notice to the SEC – are satisfied before the company's report otherwise would be due. (C&DI 104B.01) As a result, the company would be required to file its report within four business days after its materiality determination if, by that time, the DOJ has declined to determine that disclosure of the incident poses a substantial risk to national security or public safety, or has not responded to the company's request for a delay.

The SEC staff confirms that the company must file its Form 8-K within four business days after the expiration of any delay period designated by the Attorney General. In its example applying this guidance, the staff considers a situation where, following the Attorney General's authorization of a delay period, the company requests that the Attorney General determine that the Item 1.05(a) disclosure should be delayed for an additional period. In this situation, the company must file its report within four business days after expiration of the current delay period if, before the expiration, the Attorney General declines to determine that the period should be extended or has not responded to the company's extension request. (C&DI 104B.02)

The SEC staff clarifies that if during the pendency of a delay period the Attorney General determines that the material cybersecurity incident no longer poses a substantial risk to national security or public safety, and notifies the SEC and the company of the new determination, the company will be required to file its Form 8-K within four business days after the Attorney General's notification. (C&DI 104B.03)

Consistent with the SEC's discussion in the rule release of company determinations of the materiality of cybersecurity incidents, the SEC staff affirms that a company's consultation with the DOJ regarding the availability of delayed disclosure would not necessarily result in the determination that the incident is material and therefore reportable under Item 1.05. The staff underlines that "the determination of whether an incident is material is based on all relevant facts and circumstances surrounding the incident, including both quantitative and qualitative factors, and should focus on the traditional notion of materiality as articulated by the Supreme Court." (C&DI 104B.04)

DOJ guidance regarding limited circumstances warranting delayed disclosure

On December 12, 2023, the DOJ, which operates under the direction of the Attorney General, issued "departmental guidelines" titled "Department of Justice Material Cybersecurity Incident Delay Determinations," in which the DOJ outlines the approach it will take in making determinations described in Item 1.05(c). The DOJ states in this document that it "has sole discretionary authority to determine whether and how long a substantial risk to national security or public safety exists such that a delay in disclosure is necessary consistent with Item 1.05." The guidelines describe the circumstances in which the Attorney General may determine that disclosure of a material cybersecurity incident poses such a risk.

Under Item 1.05(a), a company that experiences a material cybersecurity incident is required 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." The DOJ cautions that the basis for delaying disclosure of this information will be limited, since the agency's "primary inquiry" is whether 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."

The DOJ expresses the view that "typically" companies will be able to make the required disclosure "at a level of generality that does not pose a substantial risk to national security or public safety." Whether the DOJ's assessment applies to disclosure

of any particular cybersecurity incident will turn on the circumstances and effects of the incident and the company's judgment regarding the information it must provide to satisfy federal securities laws and SEC rules requiring complete and accurate disclosure.

The DOJ acknowledges that in certain circumstances disclosure of some or all of the information required by Item 1.05(a) could pose a risk that warrants delayed disclosure. The DOJ indicates that the circumstances in which disclosure could pose a substantial risk to national security or public safety "are expected to be limited to" disclosure involving the following categories of incidents:

- incidents reasonably suspected to involve techniques for which there is not yet well-known mitigation, where disclosure could lead to more incidents;
- incidents primarily affecting a system containing sensitive U.S. government information (or information the U.S. government would consider sensitive), such as information regarding national defense or research and development performed under government contracts, where disclosure could make the system or information vulnerable to further exploitation;
- incidents occurring while the company is conducting remediation efforts for any critical infrastructure or critical system, where disclosure revealing that the company is aware of the incident would undermine those efforts; and
- incidents which a U.S. government agency believes pose a substantial risk to national security or public safety, and the disclosure of which the agency recommends to the DOJ be delayed, where:
  - disclosure would risk revealing a confidential source, information relating to U.S. national security, or sensitive information relating to law enforcement;
  - disclosure would pose a "demonstrable threat or impediment to the success of" an operation to disrupt ongoing illicit cyber activity which the U.S. government is prepared to execute or of which it is aware; or
  - disclosure that the company is aware of the incident would undermine remediation efforts for any critical infrastructure or critical system being conducted by the U.S. government or of which the U.S. government is aware.

DOJ and FBI guidance regarding delayed disclosure process

The process for requesting delayed disclosure permitted by Item 1.05(c) is described in the DOJ guidelines and guidance issued in December by the FBI, including a document called "Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Policy Notice." The FBI, which operates as the principal investigative arm of the DOJ, is responsible for shepherding companies through the request process and, in this role, receiving and documenting disclosure delay requests and providing other administrative support to facilitate the Attorney General's delay determinations.

Party submitting delay requests. The agency guidance specifies that the request for delayed disclosure of a material cybersecurity incident typically must be submitted by the company that experienced the incident.

The DOJ guidelines, however, also provide that a U.S. government agency may recommend delayed disclosure to the DOJ through the FBI if it believes disclosure poses a substantial risk to national security or public safety, so long as the company concurs with the recommendation and agrees to delay its disclosure in accordance with the Attorney General's determination. The DOJ expects that the delay request process is most likely to be initiated by an agency in circumstances – falling within the last incident category listed above – in which, at least initially, the agency rather than the company is likely to be aware of the risk. The guidelines direct the U.S. government agency with knowledge of the incident to consult with the FBI and other appropriate U.S. government agencies to determine whether the U.S. government should notify and coordinate with the company regarding the company's disclosure plans and willingness to defer disclosure in reliance on Item 1.05(c).

Timing of delay requests. In its guidance, the FBI highlights that the company must submit its delay request "immediately" upon determining that the cybersecurity incident is material and include in the request the date and time when it made its materiality determination. The guidance warns companies that failure to report the incident "immediately upon determination will cause your delay-referral request to be denied."

The FBI encourages companies to contact the FBI or another sector risk management agency "soon" after the company believes that disclosure of a

"newly-discovered" cybersecurity incident may pose a substantial risk to national security or public safety. The FBI explains that this early outreach will allow it to become familiar with the circumstances of the incident before the company makes its materiality determination.

The DOJ guidelines state that a request for an additional period of delay should be made at least five business days before the end of the initial period of delay and include a description of the continued substantial risk that disclosure poses to national security or public safety and an estimate of the duration of the risk.

Submission of delay requests. The FBI's guidance directs companies requesting a delay to contact the FBI directly by e-mail at cyber_sec_disclosure_delay_referrals@fbi.gov, or through the U.S. Secret Service, the Cybersecurity and Infrastructure Security Agency, the Department of Defense, or another sector risk management agency. Companies may use the same FBI e-mail address to request an extension of a previously granted delay period.

Government officials previously had informally indicated that the government was considering establishing a web form for submission of delay requests, but no such form has yet been made available.

Content of delay requests. The FBI's guidance specifies that the delay request must contain all of the following information:

- the company's name;
- when the cybersecurity incident occurred;
- when the company made its materiality determination;
- whether and how the company is in contact with the FBI or another U.S. government agency regarding the incident;
- detailed information about the incident (including the type of incident, known or suspected intrusion vectors (including any identified vulnerabilities), affected infrastructure or data, and any known operational impact);
- confirmed or suspected attribution of the responsible cyber actors;
- current status of remediation or mitigation efforts;
- incident location (including street address, city, and state);
- company contact information; and
- information about submission and disposition of any prior delay request.

The DOJ guidelines separately state that any delay request should convey "a concise description of the facts forming the basis of the registrant's belief that disclosure required under Item 1.05 may pose a substantial risk to national security or public safety" and cite one of the categories of incidents summarized above for which the DOJ believes that delayed disclosure could be warranted. According to this guidance, the "most relevant" facts for the Attorney General's determination will be those pertaining to the potential consequences for national security or public safety if the incident were reported within four business days after the company's materiality determination.

Processing of delay requests. The DOJ and FBI guidance contains a series of timing milestones for agency action to ensure that, as formulated by the DOJ guidelines, the Attorney General will "invoke the provision permitting a delay in disclosing an incident" under Item 1.05 "within four business days of a determination by the registrant that the registrant has experienced a material cybersecurity incident."

Following its receipt of a delay request, before it refers the request to the DOJ, the FBI will coordinate checks of national security and public safety equities and document facts relating to the incident based on the submission, findings from FBI national security and public safety records, and consultations with other U.S. government agencies. In its referral of the delay request to the DOJ, the FBI will include an evaluation of whether public disclosure about the incident within the required period would pose a substantial risk to national security or public safety.

Attorney General's determination. After considering the FBI's referral, the Attorney General will determine whether and for how long a disclosure delay is warranted and then notify both the SEC and the requesting company (as well as any recommending government agency) of its determination. The DOJ guidelines stress that the Attorney General's approval of a delay might pertain only to some portions of the required Item 1.05(a) disclosure (such as the nature or scope of the incident) and not others (such as the timing of the incident).

Omission of classified information

In its cybersecurity disclosure rule release, the SEC indicated that the process for delayed disclosure of a material cybersecurity incident under Item 1.05(c) does not limit, and is separate from, the provisions of Exchange Act Rule 0-6 authorizing the omission of information from a filed report that has been classified by a U.S. government department or agency "for protection in the interests of national defense or foreign policy."

The SEC noted that where information a company is otherwise required to disclose under Item 1.05 is classified, the company may omit the information in compliance with Rule 0-6. That rule provides that any omission of classified information in reliance on the rule should be accompanied by the filing of a statement by the appropriate U.S. government agency indicating that the omitted information is classified, or that the classification of the information is awaiting determination.

Looking ahead

The DOJ and FBI guidance make clear that the grant of delayed disclosure permitted by Item 1.05(c) for national security or public safety reasons will be limited to narrow circumstances evaluated in a rigorous process with strict timing requirements.

As a result, as recommended by the FBI, companies should consider establishing a relationship with the cyber squad at their local FBI field office. If a cybersecurity incident appears to pose a substantial risk to national security or public safety and the company may wish to seek delayed disclosure, it should be prepared to move quickly to inform the FBI or another appropriate U.S. government agency of the occurrence of the incident and of its intention to seek a disclosure delay if warranted. Company personnel responsible for making materiality determinations for SEC disclosure should be aware of the process for requesting delayed disclosure and of the importance of submitting a delay request immediately upon determining that the incident is reportable under Item 1.05.

Because the Attorney General's determination will be subject to the uncertainties that affect any evaluation of national security and public safety matters, it will be prudent to stand ready to file the Item 1.05 report without the benefit of a delay if the Attorney General has declined to make the requested determination or has not responded to the delay request.

Contributors

Alan L. Dye (co-editor)
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5737
alan.dye@hoganlovells.com

Richard Parrino (co-editor)
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5530
richard.parrino@hoganlovells.com

John B. Beckman
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5464
john.beckman@hoganlovells.com

Kevin K. Greenslade
Partner, Northern Virginia
Securities & Public Company Advisory
T +1 703 610 6189
kevin.greenslade@hoganlovells.com

Ann C. Kim
Partner, Los Angeles
Investigations, White Collar and Fraud
T +1 310 785 4711
ann.kim@hoganlovells.com

Paul Otto
Partner, Washington, D.C.
Privacy and Cybersecurity
T +1 202 637 5887
paul.otto@hoganlovells.com

Peter M. Marta
Partner, New York
Privacy and Cybersecurity
T +1 212 918 3528
peter.marta@hoganlovells.com

Allison Holt Ryan
Partner, Washington, D.C.
Litigation
T +1 202 637 5872
allison.holt-ryan@hoganlovells.com

Nathan Salminen
Partner, Washington, D.C.
Privacy and Cybersecurity
T +1 202 637 5413
nathan.salminen@hoganlovells.com

J. Nicholas Hoover
Counsel, Baltimore
Securities & Public Company Advisory
T +1 410 659 2790
nick.hoover@hoganlovells.com

Additional contacts

Steven J. Abrams
Partner, Philadelphia
T +1 267 675 4671
steve.abrams@hoganlovells.com

Richard Aftanas
Partner, New York
T +1 212 918 3267
richard.aftanas@hoganlovells.com

Tifarah Roberts Allen
Partner, Washington, D.C.
T +1 202 637 5427
tifarah.allen@hoganlovells.com

Jessica A. Bisignano
Partner, Philadelphia
T +1 267 675 4643
jessica.bisignano@hoganlovells.com

David W. Bonser
Partner, Washington, D.C.
T +1 202 637 5868
david.bonser@hoganlovells.com

Glenn C. Campbell
Partner, Baltimore, Washington, D.C.
T +1 410 659 2709 (Baltimore)
T +1 202 637 5622 (Washington, D.C.)
glenn.campbell@hoganlovells.com

David Crandall
Partner, Denver
T +1 303 454 2449
david.crandall@hoganlovells.com

John P. Duke
Partner, Philadelphia, New York
T +1 267 675 4616 (Philadelphia)
T +1 212 918 5616 (New York)
john.duke@hoganlovells.com

Allen Hicks
Partner, Washington, D.C.
T +1 202 637 6420
allen.hicks@hoganlovells.com

Paul Hilton
Senior Counsel, Denver, New York
T +1 303 454 2414 (Denver)
T +1 212 918 3514 (New York)
paul.hilton@hoganlovells.com

Eve N. Howard
Senior Counsel, Washington, D.C.
T +1 202 637 5627
eve.howard@hoganlovells.com

William I. Intner
Partner, Baltimore
T +1 410 659 2778
william.intner@hoganlovells.com

Bob Juelke
Partner, Philadelphia
T +1 267 675 4615
bob.juelke@hoganlovells.com

Paul D. Manca
Partner, Washington, D.C.
T +1 202 637 5821
paul.manca@hoganlovells.com

Michael E. McTiernan
Partner, Washington, D.C.
T +1 202 637 5684
michael.mctiernan@hoganlovells.com

Stephen M. Nicolai
Partner, Philadelphia
T +1 267 675 4642
stephen.nicolai@hoganlovells.com

Brian C. O'Fahey
Partner, Washington, D.C.
T +1 202 637 6541
brian.ofahey@hoganlovells.com

Leslie (Les) B. Reese, III
Partner, Washington, D.C.
T +1 202 637 5542
leslie.reese@hoganlovells.com

Richard Schaberg
Partner, Washington, D.C., New York
T +1 202 637 5671 (Washington, D.C.)
T +1 212 918 3000 (New York)
richard.schaberg@hoganlovells.com

Michael J. Silver
Partner, New York, Baltimore
T +1 212 918 8235 (New York)
T +1 410 659 2741 (Baltimore)
michael.silver@hoganlovells.com

Andrew S. Zahn
Partner, Washington, D.C.
T +1 202 637 3658
andrew.zahn@hoganlovells.com

Elizabeth (Liz) L. Banks
Counsel, Washington, D.C.
T +1 202 637 2523
elizabeth.banks@hoganlovells.com

Val Delp
Counsel, Philadelphia
T +1 267 675 4649
val.delp@hoganlovells.com

Weston J. Gaines
Counsel, Washington, D.C.
T +1 202 637 5846
weston.gaines@hoganlovells.com

Meredith A. Hines
Counsel, New York
T +1 212 918 3729
meredith.hines@hoganlovells.com

Catalina Santos Parkinson
Counsel, Washington, D.C.
T +1 202 637 5767
catalina.parkinson@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Berlin**
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta *
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
**Legal Services Center

www.hoganlovells.com