DEPARTMENT OF JUSTICE MATERIAL CYBERSECURITY INCIDENT DELAY DETERMINATIONS
December 12, 2023

These departmental guidelines outline the process that companies subject to the reporting requirements in Section 13 or 15(d) of the Securities Exchange Act of 1934 ("registrants"), or U.S. Government agencies in coordination with registrants, may use to request that the Attorney General[1] authorize delays of cyber incident disclosures required by the U.S. Securities and Exchange Commission ("Commission") pursuant to Form 8-K Item 1.05.

When a registrant "experiences a cybersecurity incident that is determined by the registrant to be material," SEC Form 8-K Item 1.05(a) requires the registrant to disclose "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." Instruction 4 to Item 1.05 provides that: "A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident." Item 1.05(c) contains an exception to the general disclosure requirement:

> …if the United States Attorney General determines that disclosure required by paragraph (a) of this Item 1.05 poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, the registrant may delay providing the disclosure required by this Item 1.05 for a time period specified by the Attorney General, up to 30 days following the date when the disclosure required by this Item 1.05 was otherwise required to be provided. Disclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing. In extraordinary circumstances, disclosure 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 and notifies the Commission of such determination in writing. Beyond the final 60-day delay under this paragraph, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order.

This document outlines the approach the Department of Justice ("Department") will take in making the determinations described in Item 1.05(c).

1. Limited circumstances for finding a substantial risk to national security or public safety

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. While cybersecurity incidents themselves frequently threaten public safety and national security, the disclosure to the public that those incidents have occurred poses threats

[1] References to "the Attorney General" throughout this document refer to the Attorney General and authorized designees at the Department of Justice.

less often. In many circumstances, the prompt public disclosure of relevant information about a cybersecurity incident provides an overall benefit for investors, public safety, and national security.

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." Typically, registrants 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. In certain circumstances, however, the disclosure of some or all of the information required by Item 1.05 could pose such a risk. Those circumstances of which a registrant would be aware are expected to be limited to the following categories:

a) 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—for example, exploiting a software vulnerability for which there is no patch or other reasonably available mitigation—and the disclosure required by Item 1.05 could lead to more incidents, thereby posing a substantial risk to national security or public safety.

b) The cybersecurity incident primarily impacts a system operated or maintained by a registrant that contains sensitive U.S. Government information, or information the U.S. Government would consider sensitive, and public disclosure required by Item 1.05 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 pursuant to government contracts.

c) The registrant is conducting remediation efforts for any critical infrastructure or critical system, and any disclosure required by Item 1.05(a) revealing 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.

d) The circumstances described below in Section 3, after a government agency has made the registrant aware of them.

2. Procedure for registrants to follow when Item 1.05(c)'s exception might apply

When a registrant discovers a cybersecurity incident and believes that disclosure may pose a substantial risk to national security or public safety, the registrant should, directly or through another U.S. Government 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)), immediately contact the FBI consistent with reporting instructions the FBI has issued. The registrant should convey in its report 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, citing one or more of the categories described above. The most relevant facts will pertain to the

potential consequences to national security or public safety that would result from a disclosure within the timeframe required by Item 1.05. The Attorney General must invoke the provision permitting a delay in disclosing an incident under the Commission rule within four business days of a determination by the registrant that the registrant has experienced a material cybersecurity incident. As such, it is important that the registrant provide to the FBI, directly or indirectly through another U.S. Government agency, information about a cybersecurity incident likely to meet the requirements for delayed disclosure as soon as possible, even beginning well before the registrant has completed its materiality analysis or its investigation into the incident. The FBI will document the facts of the incident provided by the registrant and findings from related FBI national security and public safety records, equity checks, and appropriate consultations with other U.S. Government agencies including USSS, CISA, or SRMAs. The FBI's referral of a delay request to the Department will include an evaluation of whether the public disclosure required by Form 8-K Item 1.05 within its prescribed timeframe would pose a substantial risk to national security or public safety.

3. Procedure for a U.S. Government agency to follow when Item 1.05(c)'s exception might apply

Whenever 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 potentially required by paragraph (a) of Item 1.05 poses a substantial risk to national security or public safety, that U.S. Government agency should, in consultation with the FBI and other U.S. Government agencies as appropriate, determine whether the U.S. Government should notify and coordinate with the registrant to determine the timing and content of information the registrant plans to disclose, absent an Item 1.05(c) exemption; and whether the registrant would agree to a delayed disclosure should the Attorney General make the necessary determination. If a delay in public disclosure is believed to be warranted by the relevant U.S. Government agency and is agreed to by the registrant, then the U.S. Government agency should immediately contact the Department through the FBI, communicate the relevant facts, explain why a delay is appropriate, and recommend a period for delay. The Department anticipates that the following are the types of scenarios in which, at least initially, a recommending U.S. Government agency, rather than a registrant, is likely to be aware of a substantial risk to national security or public safety:

a) Disclosure to the public of the cybersecurity incident as required by Item 1.05 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. 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 possibility of occurrence.

b) The U.S. Government is prepared to execute, or is aware of, an operation to disrupt ongoing illicit cyber activity that poses a substantial risk to national security or public safety, such as through freezing or seizing information, assets, or infrastructure involved in illicit cyber activity, or by effecting the arrest of an individual or individuals for illicit cyber activity, and public disclosure of the cybersecurity incident as required by Item 1.05 would pose a demonstrable threat or impediment to the success of such an operation.

c) The U.S. Government is aware of or conducting remediation efforts for any critical infrastructure or critical system, and any disclosure required by Item 1.05(a) revealing 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.

4. Procedures following the Department's determination of whether an Item 1.05(c) exception might apply

The Department 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. In making this determination and as referenced in section 2, the Department, through the FBI, will consult with other relevant U.S. Government agencies, such as USSS, CISA, and SRMAs, as appropriate. When the Attorney General determines that disclosure of all or part of the information required by Item 1.05 poses a substantial risk to national security or public safety, the Department will notify the Commission of such determination in writing. That notice will specify a period for the delay, up to 30 days. The Attorney General's determination might pertain to only part of the information that Item 1.05 requires; for example, that disclosure of the timing of the incident would not pose a substantial risk to national security or public safety, but disclosure of the nature or scope of the incident would pose such a risk. The Department will, at or near the same time, also notify the recommending agency and the registrant of the determination, including the scope of information described in Item 1.05 covered by the determination, and the period for the delay.

When the Department determines, in its discretion, that the standard is not met for a disclosure delay, it will inform the recommending agency and the registrant, where applicable. If the recommending agency disagrees with the Department's determination, it should inform the Department immediately and, time permitting, provide additional information or supporting material.

5. Changes in circumstances during a delay period

The recommending agency should inform the registrant of the ongoing need to apprise the recommending agency of any new or changed information relevant or potentially relevant to the national security or public safety risks of public disclosure that arises during the delay period. If, during the period of delay, the recommending agency assesses that public disclosure as required by Item 1.05 would no longer pose a substantial risk to national security or public safety, it will immediately notify the Department through the FBI. If the Department determines that the circumstances no longer meet Item 1.05(c)'s requirements for delaying disclosure, it will notify the recommending U.S. Government agency, the Commission, and the registrant of that determination in writing.

6. Subsequent periods of delay

Item 1.05(c) refers to an initial delay of up to 30 days, a possible "additional" period of up to 30 days, a possible "final additional" period of delay of up to 60 days, and a possible further delay "beyond the final 60-day delay."

"Additional" periods of delay after initial delay

Item 1.05(c) provides that "[d]isclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing."

If, during an initial delay period, the recommending agency, the registrant, or another U.S. Government agency assesses that the substantial risk to national security or public safety from public disclosure will continue to exist beyond the initial delay period, then a request to the FBI for an "additional period" of delay is appropriate. A request for an "additional period" 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 that such risk may last.

When the Attorney General determines that public disclosure continues to pose a substantial risk to national security or public safety and that a specific additional period of delay is justified, the Department will notify the Commission, the recommending agency, and the registrant of the nature and scope of such determination and the duration of the additional delay period in writing.

When the Department determines that the standard is not met for an additional delay in disclosure, it will inform the recommending agency and the registrant, where applicable. If the recommending agency disagrees with the Department's determination, it may inform the Department immediately and, time permitting, provide additional information or supporting material.

"Final additional" periods of delay

Item 1.05(c) provides that "[i]n extraordinary circumstances, disclosure 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 and notifies the Commission of such determination in writing."

If, during an "additional period" of delay, the recommending agency, the registrant, or another U.S. Government agency assesses that there is an extraordinary circumstance in which public disclosure continues to pose a substantial risk to national security beyond the additional delay period, the recommending agency, registrant, or other relevant U.S. Government agency will inform the FBI and the Department as soon as possible. A request for a "final additional period" should include a description of the extraordinary circumstances and continued substantial risk that public disclosure poses to national security. As with the earlier periods of delay, the Department's determination might pertain to only part of the information that Item 1.05(a) requires and might be narrower in scope than the determination for the additional period of delay. If the Attorney General determines that public disclosure continues to pose a substantial risk to national security or public safety (as described in Section 2 above), the Department will notify the Commission, the recommending agency, and the registrant of the nature and scope of such determination and the duration of the final additional delay period in writing.

When the Department determines that the standard is not met for an additional disclosure delay, it will inform the recommending agency and the registrant, where applicable. If the recommending agency

disagrees with the Department's determination, it may inform the Department immediately and, time permitting, provide additional information or supporting material.

Periods "beyond the final 60-day delay"

Item 1.05(c) provides that "[b]eyond the final 60-day delay under this paragraph, if the Attorney General indicates that further delay is necessary, the Commission will consider additional requests for delay and may grant such relief through Commission exemptive order."

If, during a "final additional" period of delay, the recommending agency, the registrant, or another U.S. Government agency assesses that public disclosure continues to pose a substantial risk to national security beyond the final additional period of delay, the recommending agency, registrant, or other relevant U.S. Government agency will so inform the FBI and the Department. If the Attorney General determines that public disclosure continues to pose a substantial risk to national security, the Department will so indicate in writing to the Commission, which will consider the merits of issuing an exemptive order allowing additional delay. If any additional delay is allowed, the Department will notify the recommending agency and the registrant of the nature and scope of such determination and the duration of the additional delay period in writing.

When the Department determines that the standard is not met for an additional disclosure delay, it will inform the recommending agency and the registrant, where applicable. If the recommending agency disagrees with the Department's determination, it may inform the Department immediately and, time permitting, provide additional information or supporting material.

7. This document's limited scope

These guidelines do not address processes or procedures for interagency sharing of registrant-related information. While the Department anticipates considerable coordination and consultation with other agencies, this document does not purport to describe that work.

These guidelines do not attempt to describe every situation in which the law might require a cybersecurity disclosure, or when cybersecurity disclosures are advisable even if not required. Aside from the Commission's public disclosure requirements contained in Item 1.05, additional or concurrent reporting to the Commission pursuant to other statutory or regulator provisions or other government agencies (such as to CISA, SRMAs, or regulators) may be legally required or advisable.

This document provides no legal advice about the meaning of Item 1.05, or about the nature or extent of the Commission's reporting requirements.

Future rulemaking pursuant to the Cyber Incident Reporting Act for Critical Infrastructure (CIRCIA) and the Cyber Incident Reporting Council's directive to harmonize mandatory cyber incident reporting under CIRCIA (see 6 U.S.C. §§ 681f and 681g) may affect the contents of these guidelines. The Department will reassess these guidelines after CIRCIA rulemaking is complete, with consideration of any relevant recommendations from the Council on harmonization and streamlined reporting processes.

These guidelines have no regulatory effect, confer no rights or remedies, and do not have the force of law. *See United States v. Caceres,* 440 U.S. 741 (1979).