FEDERAL BUREAU OF INVESTIGATION
POLICY DIRECTIVE

Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Policy Directive 1355D

General Information

Proponent	Cyber Division (CyD)
Publication Date	2025-02-28
Last Updated	N/A
Supersession	*Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Policy Notice* (1297N)

1. Authorities

- Volume 88 Federal Register (Fed. Reg.), No. 51896, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Securities and Exchange Commission (SEC) (2023)
- *Department of Justice (DOJ) Material Cybersecurity Incident Delay Determinations* <https://www.justice.gov/archives/opa/media/1328226/dl?inline> (2023)
- Securities Exchange Act of 1934

2. Purpose

2.1. This policy directive (PD) implements the *DOJ Material Cybersecurity Incident Delay Determinations* guidelines and establishes procedures by which Federal Bureau of Investigation (FBI) personnel will document cybersecurity incident public disclosure delay requests, related incident details, and United States government (USG) national security or public safety checks in an FD-1219, "Federal Bureau of Investigation 8-K Cyber Delay Referral Form." This PD also establishes the roles, responsibilities, and procedures by which FBI personnel will send these forms to DOJ to facilitate delay determinations.

2.2. Per the SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule (88 Fed. Reg. 51896), publicly traded companies are required to determine whether each cybersecurity incident that they experience is a material cybersecurity incident pursuant to the rule. This determination is the responsibility of publicly traded companies subject to the rule and the Securities Exchange Act. Once a company makes a materiality determination, the company has four business days to publicly disclose the incident by filing an SEC Form 8-K in the SEC's EDGAR database.

2.3. The SEC rule permits DOJ to notify these companies that they may delay public filing if the Attorney General (AG) (or designee) determines that disclosure through a public filing poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing. Initially, disclosure may be delayed for a timeframe specified by the AG but must only last up to 30 calendar days following the date when the SEC disclosure was otherwise required to be provided (i.e., four business days from determining

materiality). If the AG determines that disclosure continues to pose a substantial risk to national security or public safety, the disclosure delay may be extended for an additional period of up to 30 calendar days, and DOJ will notify the SEC of such determination in writing. In extraordinary circumstances, if the AG determines that disclosure continues to pose a substantial risk to national security and notifies the SEC of such determination in writing, disclosure may be delayed for a final additional period of up to 60 calendar days. The *DOJ Material Cybersecurity Incident Delay Determinations* memo explains how DOJ and the AG will make these determinations and notify the requesting victim, the SEC, and the referring agency (including the FBI) of determinations. Through this memo, the FBI is responsible for intaking all such requests (either from a victim directly, the Cybersecurity and Infrastructure Security Agency [CISA], or other government agencies [OGA]) on behalf of DOJ; coordinating checks of USG national security and public safety equities; and reporting the outcome of these checks to DOJ.

3. Scope

This PD applies to all FBI personnel.

4. Exemptions

There are no exemptions to this PD.

5. Policy Statement

5.1. This PD applies to all requests from cyber incident victims for a referral of their incident to DOJ for a delay of SEC public filing requirements, regardless of whether:

5.1.1. The request is the FBI's first notice of the incident or the request is made after the FBI is already aware of the incident.

5.1.2. The victim is requesting a delay determination for the first time or an extension of an existing delay determination.

5.2. This PD establishes roles, responsibilities, and procedures of FBI personnel for:

5.2.1. The intake of delay referral requests from cyber incident victims directly or via CISA or OGAs.

5.2.2. Coordinating checks of USG national security and public safety equities for each delay referral request.

5.2.3. Documenting these requests and checks in an FD-1219.

5.2.4. Submitting approved and completed FD-1219 forms to DOJ.

5.2.5. Conducting follow-up victim engagement, as appropriate.

5.2.6. Coordinating and documenting requests for additional delay referrals.

5.3. This PD complements and does not supersede other cyber incident response, victim notification, or coordination requirements found in the *Cyber Division Policy Guide* (1181PG) [Redacted].

6. Roles and Responsibilities

6.1. All FBI personnel who are in receipt of a request from a cyber incident victim, either directly or via CISA or OGAs, for a referral of their incident to DOJ for a delay of SEC public

filing requirements must as soon as possible direct victims to make these delay requests by filling out the online "SEC Reporting Requirements Delay Request Form" <https://sec8k.ic3.gov>.

6.2. The time requirements of the following subsections of this policy must be actioned for all initial requests for a disclosure delay. If a victim is granted a disclosure delay by DOJ and submits a request for an extension at least five business days prior to the expiration of the granted delay, then CyWatch may adjust the timeliness requirements of the following subsections as appropriate per its judgement.

6.3. CyWatch must:

6.3.1. Within two hours of receipt of a request submitted through the online form, conduct the following actions (although, if the online form is submitted during a non-business day, these designated time requirements commence at the next opening of business hours):

6.3.1.1. Verify the request has been made by a publicly traded company.

6.3.1.2. Verify the request has been made immediately upon the company's determination to disclose details of a cyber incident via an SEC Form 8-K.

6.3.1.3. Upon verification of the criteria asked in the above subsections 6.3.1.1. and 6.3.1.2. of this PD, conduct initial record checks of FBI databases for information specifically related to the incident, including but not limited to a past or present investigation or [Redacted] on the request's referenced cyber incident and the attributed threat activity or actors responsible for the incident, if known. If the victim is not a publicly traded company, or if the victim does not make this request to CyWatch immediately upon the company's determination to disclose details of a cyber incident via an SEC Form 8-K, CyWatch should not process the request. If CyWatch determines not to process a request based on these criteria, it must document this determination in an administrative case file maintained [Redacted] by CyWatch.

6.3.1.4. Populate questions one through six of a new draft FD-1219 based on the information provided in the victim's request and initial record checks, per the above subsection 6.3.1.3. of this PD. If responses to the online delay request form satisfy any or all of questions one through six of the FD-1219, CyWatch should not alter the provided information but may add to it, as appropriate (e.g., using information found during record checks). CyWatch must designate in the FD-1219 which text was provided by the victim and which was new text added by CyWatch.

6.3.1.5. If a field office (FO) has an open investigation on the request's referenced cyber incident, send a [Redacted] email to the corresponding appropriate FO cyber squad(s) for the investigation. If no FO has an open investigation on the request's referenced cyber incident, send a [Redacted] email to the corresponding appropriate FO cyber squad(s) of the victim's local FO. These emails should include, at minimum:

6.3.1.5.1. A subject line stating, "SEC Disclosure Delay Referral: Request by [Insert Victim Identity]."

6.3.1.5.2. The draft FD-1219, initiated per the above subsection 6.3.1.4. of this PD [Redacted].

6.3.1.5.3. A summary of the incoming request from the cyber incident victim, including where the incident occurred.

6.3.1.5.4. The following statement: "The FO in receipt of this email must complete the roles and responsibilities assigned in subsection 6.4. of the *Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Policy Directive* (1355D) within 24 hours of receipt."

6.3.1.5.5. A copy to the appropriate CyD operational desk program managers (PMs) and Cyber Threat Team (CTT), if applicable; the section chief (SC) of the Cyber Operations Support Section (COSS).

6.3.1.6. Following the FO's return of the draft FD-1219 to CyWatch, CyWatch must share this returned copy of the FD-1219 with the appropriate CyD operational desk PMs. This notification must task these PMs to commence completing the roles and responsibilities assigned in subsection 6.8. of this PD within 28 hours of the receipt of the draft FD-1219.

6.3.1.7. Concurrent with the notifications made per subsection 6.3.1.5. and the above 6.3.1.6. of this PD, notify the appropriate OGAs (as determined by CyWatch's list) with national security and public safety equities of the incoming request from a cyber incident victim.

6.3.1.7.1. This notification must include the incident information provided through the victim's request and information documented per subsection 6.3.1.4. of this PD. The notification must task these OGAs to conduct equity checks to help determine if public filing of the incident would pose a substantial risk to national security or public safety; return results of these equity checks to CyWatch within 24 hours; and handle enclosed victim information in accordance with the *Framework for Improved Cyber Information Sharing and Interagency Coordination for Critical Infrastructure Engagements Regarding Cyber Threats and Incidents*, also known as the Federal Senior Leadership Council (FSLC) Framework, approved by the National Security Council Cyber Policy Coordination Committee on April 22, 2020.

6.3.1.8. Notify DOJ of the request with a confirmation that CyD intends to process the request.

6.3.2. Maintain a list of OGAs eligible to submit online delay request forms on behalf of cyber incident victims.

6.3.3. Within two hours of receipt of responses from the relevant FO, CyD operational desk PMs, and OGAs, per the concurrent tasks assigned in subsection 6.3.1.5. through the above subsection 6.3.1.7. of this PD, must:

6.3.3.1. Complete the remainder of FD-1219, Section Two. This action must include ensuring that documentation of record checks was performed by CyD operational desk PMs for question six of the FD-1219, per the above subsection 6.3.1.6. and subsection 6.8. of this PD; completing question seven of the FD-1219, based on responses provided by appropriate OGAs, per the above subsection 6.3.1.7. of this PD; and providing a summary of the findings of risk for public disclosure to national security or public safety in response to questions eight and nine of the FD-1219.

6.3.3.2. Request and gain, if applicable, verbal or written approval of the final FD-1219 from the COSS SC (delegable to the DAD or AD) per subsection 6.5. to subsection 6.7.2. of this PD. An acting official may not approve the FD-1219.

6.3.3.3. Send a copy of the approved form to the designated DOJ email inboxes. This email must include confirmation that CyD is making the referral following internal records checks and OGA equity checks; a copy of the FD-1219, approved per subsection 6.5. through subsection 6.7. of this PD; and a request for confirmation from DOJ of its delay determination.

6.3.4. Within 10 business days of receipt of approval of the final FD-1219, per subsection 6.3.3.2. of this PD, upload the email chain containing SC approval of the completed FD-1219 to the appropriate [Redacted] file maintained by CyWatch.

6.3.5. Upon receipt of DOJ's delay determination (which DOJ will make concurrently to the victim and the SEC):

6.3.5.1. Contact the victim via formal written communication, as appropriate, to confirm that the FBI is aware of DOJ's determination. If DOJ approves the delay request, CyWatch's contact with the victim should include an invitation for the victim to submit any requests for delay extensions no later than five business days before the expiration of the granted delay. CyWatch should advise the victim to submit this renewal request through the online form referred to in subsection 6.1. of this PD. CyWatch must make the relevant FO(s), relevant CyD operational desk PMs, and the COSS SC aware of this contact, as appropriate. This will enable additional relevant FO engagement with the victim.

6.3.5.2. Document DOJ's delay determination [Redacted].

6.3.6. Manage related communications with DOJ following the referral of an FD-1219 to DOJ. These communications may include, but not be limited to, follow-up questions related to the contents of the FD-1219 and the process by which FBI arrived at the facts and findings documented therein.

6.3.7. Manage communication mechanisms (e.g., email inboxes or telephone lines) for the victim request intake and referral process and monitor them on a 24/7 basis.

6.3.8. Develop, update, and provide appropriate training materials and communications to stakeholders of the processes outlined in this PD, in coordination with CyD's Cyber Education and Training Unit (CETU), Executive Staff Unit (ESU), the Cyber Policy Team, and the Office of the General Counsel (OGC), as appropriate.

6.4. FO heads (delegable to assistant special agents in charge [ASAC]):

6.4.1. Must establish and execute a process by which their subordinate personnel respond to CyWatch emails sent to FOs, per subsection 6.3.1.5. of this PD. The established process must, at minimum, execute the following actions within 24 hours:

6.4.1.1. Intake the request and engage with the victim, as appropriate.

6.4.1.2. Review and edit the drafted FD-1219, Section One based on information learned during victim engagement, when applicable.

6.4.1.3. Respond to CyWatch's email per subsection 6.3.1.5. of this PD with an attached, completed FD-1219, Section One; [Redacted]; and as appropriate, a recommendation of other FOs with whom CyD should consult as it determines potential related national security or public safety equities.

6.4.2. Should ensure that their FOs provide timely input, as appropriate, if CyD operational desk PMs notify the FO of a pending request and related equities in the FO's investigative records, per subsection 6.8.2. of this PD.

6.5. The COSS SC must approve or deny FD-1219s, per subsection 6.3.3.2. of this PD, within CyWatch's two-hour deadline. The COSS SC must not delegate this task or reassign it to another SC.

6.6. The deputy assistant director (DAD) of CyD's Cyber Operations Branch (COB), in the absence of the COSS SC, must approve or deny FD-1219s within CyWatch's two-hour deadline, per subsection 6.3.3.2. of this PD.

6.7. The assistant director (AD) of CyD must:

6.7.1. In the absence of both the COSS SC and the COB DAD, approve or deny FD-1219s within CyWatch's 2-hour deadline, per subsection 6.3.3.2. of this PD.

6.7.2. Designate an approver of FD-1219s in the joint absence of the COSS SC; DAD, COB; and AD, CyD.

6.8. CyD operational desk PM(s) must, within 28 hours of receipt of the draft FD-1219 from CyWatch, per subsection 6.3.1.6. of this PD:

6.8.1. Review the incident information provided.

6.8.2. Conduct additional record checks in FBI systems and information holdings of their operational desk, as appropriate, and amend question six of the draft FD-1219 to reflect additional findings of specific and credible national security or public safety concerns with the victim's public filing of the cyber incident in the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database.

6.8.2.1. If a related national security or public safety equity in the investigative records of an FO is identified, the operational desk PM(s) must notify the appropriate FO points of contact (POC). The operational desk PM(s) must incorporate related FO feedback into the amendments of question six, as appropriate.

6.8.2.2. If the incident has been attributed to a specific threat actor, the operational desk PM(s) also must notify the appropriate Cyber Threat Team FO POCs. The operational desk PM(s) must incorporate related FO feedback resulting from this notification into the amendments of question six, as appropriate.

7. References

- *Cyber Division Policy Guide* (1181PG) [Redacted]
- DOJ Material Cybersecurity Incident Delay Determinations (2023) <https://www.justice.gov/opa/media/1328226/dl?inline>
- FD-1219, "Federal Bureau of Investigation 8-K Cyber Delay Referral Form"
- National Security Council Cyber Policy Coordination Committee, *Framework for Improved Cyber Information Sharing and Interagency Coordination for Critical Infrastructure Engagements Regarding Cyber Threats and Incidents* (2020)
- SEC's *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (88 Fed. Reg. 51896) <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

8. Definitions and Acronyms

8.1. Definitions

8.1.1. Federal Bureau of Investigation personnel: FBI employees, task force officers (TFO), task force members (TFM), task force participants (TFP), detailees, and contractors

8.2. Acronyms

AD	assistant director
AG	Attorney General
ASAC	assistant special agent in charge
CETU	Cyber Education and Training Unit
CISA	Cybersecurity and Infrastructure Security Agency

COB	Cyber Operations Branch
COSS	Cyber Operations Support Section
CTT	Cyber Threat Team
CyD	Cyber Division
DAD	deputy assistant director
DOJ	Department of Justice
EC	electronic communication
EDGAR	Electronic Data Gathering, Analysis, and Retrieval
ESU	Executive Staff Unit
FBI	Federal Bureau of Investigation
Fed. Reg.	Federal Register
FO	field office
FSLC	Federal Senior Leadership Council
OGA	other government agency
OGC	Office of the General Counsel
PD	policy directive
PM	program manager
POC	point of contact
SC	section chief
SEC	Securities and Exchange Commission
TFM	task force member
TFO	task force officer
TFP	task force participant
[Redacted]	[Redacted]
USG	United States government

Approvals	
Sponsoring Executive Approval	
Name	**Title**
Bryan A. Vorndran	Assistant Director Cyber Division
Final Approval	
Name	**Title**
Bryan A. Vorndran	Acting Executive Assistant Director Criminal, Cyber, Response and Services Branch