FEDERAL BUREAU OF INVESTIGATION

POLICY NOTICE

Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Policy Notice 1297N

General Information

Proponent	Cyber Division (CyD)
Publication Date	2023-12-06
Last Updated	N/A
Supersession	N/A

1. Authorities

- Volume 88 Federal Register (Fed. Reg.), No. 51896, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Securities and Exchange Commission (SEC), 4 August 2023.
- Department of Justice (DOJ) Public Guidance Memo

2. Purpose

2.1. This policy notice (PN) 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 PN 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 (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 SEC's 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. 88 Fed. Reg. 51896 permits DOJ to notify these companies that they may delay public filing if the Attorney General (AG) (or designee) determines that a public filing would pose a significant threat to public safety or national security. The rule permits the AG to determine a delay of public SEC filing for 30 business days, with an option to delay for an additional 30 business days. In extraordinary circumstances, the AG can delay for an additional 60 business days due to substantial national security (but not public safety) risks. Delays cannot exceed a total of 120 business days without an exemptive order from the SEC. The DOJ Public Guidance 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.

2.4. This PN will be superseded by a forthcoming policy directive (PD).

3. Scope

This PN applies to all FBI personnel.

4. Exemptions

There are no exemptions to this PN.

5. Policy Statement

5.1. This PN 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 PN 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 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 PN complements and does not supersede other cyber incident response, victim notification, or coordination requirements found in the *Cyber Division Policy Guide* (1181PG) [links to a SECRET//NOFORN document], hereafter referred to as *CyD PG*.

6. Roles and Responsibilities

6.1. All FBI personnel who are in direct receipt of a request from a cyber incident victim for a referral of their incident to DOJ for a delay of SEC public filing requirements must direct victims to make these delay requests to CyWatch, CyD.

6.2. CyWatch must:

6.2.1. Within two hours of receipt of a request from a cyber incident victim for a referral of their incident to DOJ for a delay of SEC public filing requirements:

6.2.1.1. Verify the request is being made by a publicly traded company with a material cyber incident.

6.2.1.2. Verify the request is being made concurrently with the materiality determination.

6.2.1.3. Upon verification of the criteria asked in subsections 6.2.1.1.–6.2.1.2. of this PN, conduct initial record checks of FBI systems for information specifically related to the incident. If the victim is not a publicly traded company or if the victim does not make this request to CyWatch concurrently with the materiality determination, 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 maintained in Sentinel by CyWatch.

6.2.1.4. Draft input into Questions 1–6 of a new FD-1219, based on the information provided in the victim's request and initial record checks, per subsection 6.2.1.3. of this PN.

6.2.1.5. Initiate and assign a Guardian to the victim's local field office (FO) that (1) conveys the incoming request from a cyber incident victim, (2) documents the results of record checks accomplished per subsection 6.2.1.3. of this PN, (3) attaches the draft FD-1219 initiated per subsection 6.2.1.4. of this PN, and (4) instructs the FO to complete roles and responsibilities assigned in subsection 6.3. of this PN within 24 hours.

6.2.1.6. Concurrent with the notification to the victim's local FO initiated in subsection 6.2.1.5. of this PN, notify appropriate operational desk program managers (PM) of the incoming request from a cyber incident victim. This notification must include a copy of the draft FD-1219 initiated per subsection 6.2.1.4. of this PN. This notification must task these PMs to commence completing the roles and responsibilities assigned in subsection 6.7. of this PN within 28 hours.

6.2.1.7. Concurrent with the notifications made per subsections 6.2.1.5. and 6.2.1.6. of this PN, 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.

6.2.1.7.1. This notification must include the incident information provided through the victim's request and information documented per subsections 6.2.1.4. of this PN. The notification must task these OGAs to (1) conduct equity checks to help determine if public filing of the incident would pose a significant risk to national security or public safety, (2) return results of these equity checks to CyWatch within 12 hours, and (3) 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 22 April 2020.

6.2.1.8. Notify the section chief (SC) of the Cyber Operations Support Section (COSS), CyD with a confirmation that CyD intends to process the request.

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

6.2.2. Within two hours of receipt of responses from the victim's local FO, per the concurrent tasks assigned in subsections 6.2.1.5.–6.2.1.7. of this PN, appropriate operational desk PMs and appropriate OGAs:

6.2.2.1. Complete the remainder of FD-1219, Section 2. This action must include (1) ensuring that documentation of record checks were performed by operational desk PMs for Question 6 of the FD-1219, per subsections 6.2.1.6. and 6.7. of this PN; (2) completing Question 7 of the FD-1219, based on responses provided by appropriate OGAs, per subsection 6.2.1.7. of this PN; and (3) providing a summary of the findings of risk for public disclosure to national security or public safety in response to Questions 8 and 9 of the FD-1219.

6.2.2.2. Request and gain, if applicable, verbal or written approval of the final FD-1219 from the COSS SC (or other approver) per subsections 6.4.–6.6. of this PN.

6.2.2.3. Send a copy of the approved form to the designated DOJ email inbox. This email must include (1) confirmation that CyD is making the referral following internal records checks and OGA equity checks, (2) a copy of the FD-1219 approved per subsections 6.4.–6.6. of this PN, and (3) a request for confirmation from DOJ of its delay determination.

6.2.3. Within 10 business days of receipt of approval of the final FD-1219, per subsection 6.2.2.2. of this PN, file the completed FD-1219 and documentation of this approval in an FD-1057, "Electronic Communication" (EC), in the same administrative case file referenced in subsection 6.2.1.3. of this PN. This EC should be copied to FO investigative and administrative case files and include relevant victim identity tags, as appropriate.

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

6.2.4.1. Contact the victim, 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 to CyWatch. CyWatch should copy the victim's local FO, relevant operational desk PMs, and the COSS SC or make them aware of this contact, as appropriate.

6.2.4.2. Document DOJ's delay determination in an EC in the same administrative case file referenced in subsection 6.2.1.3. of this PN. The EC should be copied to FO investigative and administrative case files and include relevant victim identity tags, as appropriate.

6.2.5. 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.

6.2.6. 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.

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

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

6.3.1. Must establish and execute a process by which their subordinate personnel action Guardians assigned to their FOs, per subsection 6.2.1.5. of this PN. The established process must, at minimum, execute the following actions within 24 hours:

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

6.3.1.2. Review and edit the drafted FD-1219, Section 1—which is attached to the Guardian—based on information learned during victim engagement, when applicable.

6.3.1.3. Respond to the Guardian with (1) an attached, completed FD-1219, Section 1; (2) a list of the FO's investigative and administrative case files that the FO would like CyD to copy in the future Sentinel EC that will accompany the completed Guardian; and (3) as appropriate, a recommendation of other FOs with whom CyD should consult as it determines potential related national security or public safety equities.

6.3.2. Should ensure that their FOs provide timely input, as appropriate, if operational desk PMs notify the FO of a pending request and related equities in the FO's investigative records, per subsection 6.7.2. of this PN.

6.4. The SC, COSS must approve or deny FD-1219s within CyWatch's two-hour deadline, per subsection 6.2.2.2. of this PN. The SC, COSS must not delegate this task or reassign it to another SC.

6.5. 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 6.2.2.2. of this PN.

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

6.6.1. 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 6.2.2.2. of this PN.

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

6.7. Within 28 hours of receipt of notification from CyWatch, per subsection 6.2.1.6. of this PN, CyD operational PM(s) must:

6.7.1. Review the draft FD-1219.

6.7.2. Conduct additional record checks in FBI systems and information holdings of their operational desk, as appropriate, and amend Question 6 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 EDGAR database. 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 6, as appropriate.

7. References

- *CyD PG* (1181PG) [links to a SECRET//NOFORN document]
- DOJ's Public Guidance Memo
- FD-1219, "Federal Bureau of Investigation 8-K Cyber Delay Referral Form"
- *Framework for Improved Cyber Information Sharing and Interagency Coordination for Critical Infrastructure Engagements Regarding Cyber Threats and Incidents*, also known as the "FSLC Framework," approved by the National Security Council Cyber Policy Coordination Committee on 22 April 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
CyD	Cyber Division
DAD	deputy assistant director
DOJ	Department of Justice
EC	electronic communication
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
PN	policy notice
POC	point of contact
SC	section chief
SEC	Securities and Exchange Commission
TFM	task force member
TFO	task force officer
TFP	task force participant
USG	United States government

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