Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 55fcce2d | Dec 18, 2023, 12:47 PM

This week, *Hacking Healthcare*™ begins with a look at recently published Department of Justice (DOJ) guidance and a Federal Bureau of Investigation (FBI) policy notice that helps outline how the DOJ will intake, assess, and grant a delay to the public disclosure of material cybersecurity incidents as required by the new Securities and Exchange Commission (SEC) rule *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*.[i] We assess what is being required, the process itself, and how it is likely to impact healthcare entities.

Welcome back to *Hacking Healthcare*™.

DOJ and FBI Issue Policy Guidance on SEC Cyber Incident Disclosure

The new SEC cybersecurity incident reporting regulations, which are set to go into effect shortly for many publicly traded companies, riled many for its tight reporting timelines that required even ongoing incidents to be publicly disclosed. However, a provision was included that allowed victims to request an extension from public reporting. A recent DOJ guidance document and a policy update from the FBI is shedding some light on this process. Let's breakdown the new information to assess how it may affect healthcare entities.

Context

For those needing a slight refresher on what we are talking about, the SEC's final rule on cybersecurity risk management, strategy, governance, and incident disclosure includes revisions to the cyber incident disclosure responsibilities of publicly traded companies. Included is the requirement that cybersecurity incidents must be publicly disclosed through the SEC's Form 8-K within four days of determining that the incident was material.

However, the final rule also includes a provision that allows for publicly-traded companies to request a delay of public reporting. The SEC ultimately settled on language that allows for the Attorney General (AG), or the AG's designee, to grant a delay of up to 60 days if they "[determine] that the disclosure poses a substantial risk to national security or public safety."[ii] National security concerns may allow for an additional 60 days, but any further delay would require SEC sign off.

Despite the SEC's willingness to include a delay mechanism and the fact that they acknowledge that a delay may "reduce the costs of premature disclosure such as alerting malicious actors targeting critical infrastructure that their activities have been discovered," the new Policy Note and guidance documents cast doubt on how likely a delay will be granted.[iii]

FBI Policy Notice

The new FBI policy notice, *Cyber Victim Requests to Delay Securities and Exchange Commission Public Disclosure Police Notice 1297N*, was published earlier this month alongside some additional guidance on what a delay referral should include.[iv], [v] The notice outlines the procedures that are to take place between an SEC registrant asking for a delay and that delay either being granted or rejected.

To summarize the process:

- The FBI is responsible for intaking and documenting delay referrals, and for coordinating with relevant government entities on potential national security or public safety equities.
- The timelines for intake and evaluation of a delay referral appear to be under 48-hours.
- Delay referrals must come directly from an SEC registrant or through a handful of other government entities (US Secret Service (USSS), the Cybersecurity and Infrastructure Security Agency (CISA), or another sector risk management agency (SRMAs)).
- The FBI will have a dedicated email for delay referrals.
- Delay referrals must be submitted "concurrently" with the materiality determination.
- FBI will make a referral to DOJ who will issue a delay determination – the determination will be communicated concurrently to the SEC registrant requesting a delay and the SEC.

Beyond some basic information, the delay referral is to include the following elements:

- A detailed description of the cybersecurity incident that includes:
    a. Type of incident
    b. Known or suspected intrusion vectors and identified vulnerabilities
    c. What infrastructure or data was affected and how
    d. The known operational impact
- Confirmed or suspected attribution of the attack
- Status of remediation/mitigation
- Geographic location of the incident
- And points of contact for the FBI

DOJ Guidance

Alongside the FBI's Policy note, the DOJ released their own guidance to explain the approach that "the [DOJ] will take in making delay referral determinations…"[vi] A few key points from this document include: [vii]

- The DOJ's focus is to assess "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." DOJ cites that public disclosure of cybersecurity incidents often poses less of a threat.
- The DOJ highlights that "prompt public disclosure" often "provides an overall benefit for investors, public safety, and national security."
- DOJ believes that in general, the SEC's reporting requirements allow enough flexibility to avoid providing the kinds of details that could pose a national security or public safety risk.
- DOJ does outline a few cases where required disclosure could pose a substantial risk to public safety or national security that may meet the threshold for delay. This includes:
    a. When an incident is reasonably suspected of involving "a technique for which there is not yet well-known mitigation,…and disclosure could lead to more incidents."
    b. When disclosure may undermine remediation efforts for any critical infrastructure or critical system.
- The DOJ also adds that delay referrals sent to the FBI should include a concise description of why disclosure would pose a substantial risk to public safety or national security.

There are additional details and provisions that may interest members, and we would encourage a full review of the DOJ text.
Let's breakdown what to make of all of this.

Action & Analysis
Available with Health-ISAC Membership*

Health-ISAC Member Considerations
Available with Health-ISAC Membership*

Congress
Tuesday, December 19
No relevant hearings

Wednesday, December 20
No relevant meetings

Thursday, December 21
No relevant meetings

[i] https://www.sec.gov/files/rules/final/2023/33-11216.pdf
[ii] https://www.sec.gov/files/rules/final/2023/33-11216.pdf
[iii] https://www.sec.gov/files/rules/final/2023/33-11216.pdf

[iv] https://www.fbi.gov/file-repository/fbi-policy-notice-120623.pdf/view
[v] https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements-request-a-delay
[vi] https://www.justice.gov/media/1328226/dl?inline
[vii] https://www.justice.gov/media/1328226/dl?inline
[viii] https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements-fbi-policy-notice-summary

Report Source(s)

Health-ISAC

Reference | References

FBI
US Department of Justice
Health-ISAC Webinar Playback
FBI
sec
FBI

Tags

Regulatory, Incident Reporting, Hacking Healthcare, SEC, DOJ, Securities And Exchange Commission, FBI, cybersecurity

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat

Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org