April 29, 2022

WHAT YOU NEED TO KNOW ABOUT

Cyber Incident Reporting Rules

PRO POINTS

- **Facing a growing spate of cyberattacks, lawmakers** passed a cyber incident reporting mandate as part of a government spending bill in March.
- **DHS' Cybersecurity and Infrastructure Security Agency** must now craft specific rules for the program, including what critical infrastructure companies are covered and what information they must provide about incidents.
- **Critical infrastructure firms are likely to push for** rules that are flexible and minimize the disruption to companies' incident response procedures.

HOW WE GOT HERE

2020 and 2021 were banner years for cyberattacks. Russian government operatives breached SolarWinds, an IT software vendor, tampered with its software and hacked many of its clients, including nine federal agencies. Cyber criminals infected the meat supplier JBS, the insurer CNA and the IT vendor Kaseya with ransomware, crippling their operations. And in May 2021, a Russian ransomware gang breached the Colonial Pipeline Co., prompting the firm to temporarily shut down its pipeline and causing fuel shortages across the East Coast.

These hacks were just the tip of the iceberg. Businesses, including those operating critical infrastructure, experience cyberattacks every day. But the federal government only learns about a small fraction of these incidents, hampering its ability to understand the threat landscape and provide the necessary defensive services. In February, Bryan Vorndran, the head of the FBI's Cyber Division, estimated that the government only hears about a roughly a quarter of U.S. cyberattacks.

The cascade of hacks, and the associated warnings from senior cyber officials, spurred House and Senate lawmakers to craft bills requiring critical infrastructure firms to promptly report hacks to the government. The legislation went through many changes as various panels haggled over the details, but by the end of 2021, it was effectively finalized. After a few more months of procedural wrangling, Congress passed the incident reporting mandate as part of the fiscal 2022 spending bill (H.R. 2471).

WHAT'S NEXT

The legislation gives CISA 24 months to publish interim regulations laying out how the incident reporting program will work. After that, the agency will have 18 months to tweak the regulations and publish a final rule.

Lawmakers instructed CISA to consult with companies likely to be covered by the program as the agency crafts the rules. It must also consult with firms that handle ransomware negotiations and ransom payments on behalf of victims, since the bill contains a separate provision requiring companies to report paying ransoms. The bill also requires outreach to cybersecurity service providers and to insurers that provide cyber insurance plans.

As Congress debated the incident reporting bill, industry trade associations representing companies in key sectors, such as energy, water and health care, advocated for a flexible approach that took into account companies' limited resources and their urgent need to contain the damage from hacks as soon as possible. In a white paper published last summer, for example, a trade group representing the IT sector argued for giving companies 72 hours, rather than 24 hours, to report breaches.

Congress gave CISA a blueprint for what its incident reporting regulations must contain, but lawmakers left the specifics up to the agency. As CISA fills in the blanks in the coming months, industry lobbyists will be pushing for the least onerous outcomes possible.

Here are a few questions that the industry hopes CISA will answer to its benefit:

- **What range of companies** must report incidents? The law says that this must be based in part on the consequences of a breach to "national security, economic security, or public health and safety." How will CISA evaluate those potential consequences?

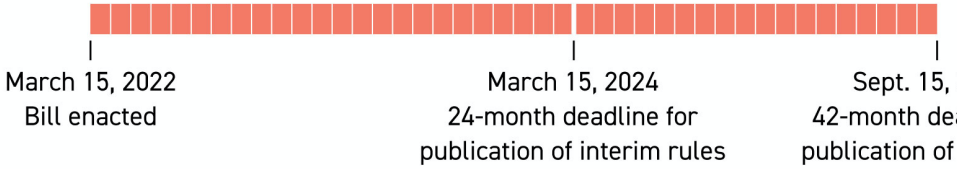
- **What constitutes an incident** that needs to be reported? The law dictated minimum factors, including a "serious impact" on infrastructure operations. How narrowly will CISA draw the final definition?

- **How much information** must companies report initially? The goal of the law is for companies to identify, to the extent possible, all affected systems and the extent of the damage.

Lobbyists will also be barraging CISA with advice and pleas as it works with other agencies to reduce redundancy in existing incident reporting rules, which cover sectors such as energy and financial services.

Timeline for crafting the cyber incident reporting rules

The cyber incident reporting legislation lays out the timeframe for CISA to publish interim regulations and then to publish a final rule.



Consultation with industry groups

Lawmakers instructed CISA to consult with companies likely to be covered by the program as the agency crafts the rules. The program is likely to affect many companies from the 16 critical infrastructure sectors that DHS has defined.

*Sept. 15, 2025, is the latest that the final rules could be published. CISA has 18 months to do so after publishing the interim rules.
Source: POLITICO staff reports

POWER PLAYERS

- **CISA Director Jen Easterly:** The National Security Agency veteran also has private sector experience from her time leading cyber and resilience efforts at Morgan Stanley. Her voice will carry enormous weight in resolving disputes about how flexible and lenient to make the new rules.

- **National Cyber Director Chris Inglis:** As the White House's point person on U.S. cyber resilience, Inglis will be both a key conduit for private sector hopes and frustrations and a source of strategic vision and guidance for the work of Easterly's agency.

- **Rep. Bennie Thompson:** The Mississippi Democrat, who chairs the House committee overseeing CISA, will likely speak frequently with the Biden administration to discuss CISA's decisions about the rules.

- **Rep. John Katko:** As the ranking member on CISA's House oversight panel, Katko (R-N.Y.) has been a consistent champion of the agency. But he's also warned against overly burdensome regulations, and he might object to some of the agency's choices.

- **Sen. Gary Peters:** Peters (D-Mich.) chairs the Senate committee overseeing CISA and helped spearhead the incident reporting mandate. His advice and counsel could influence how the agency resolves complicated rulemaking decisions.

- **Sen. Rob Portman:** Like his House counterpart Katko, Portman (Ohio), as the top Republican on the Senate committee with jurisdiction over CISA, has celebrated the agency's growth while encouraging it to prioritize friendly relations with the private sector.