

Strengthening Your Incident Response Plans Ahead of Cyber Incident Reporting for Critical Infrastructure Act

Mar 31, 2022

Categories:

Publications

Authors:

Emma H. Mulvaney
William T. Repasky

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (the "Act"), a part of the larger Consolidated Appropriations Act, was signed into law by President Joe Biden on March 15. This Act continues to demonstrate the White House's concern for potential cyberattacks, no doubt heightened as tensions with Russia escalate. [1]

While the Act touches upon a number of important matters, what may be of greatest consequence are its new reporting/disclosure obligations.

Primary Components of the Act

- The Cybersecurity and Infrastructure Security Agency (the "Agency") is to act in a clearinghouse role for the new reports now due from "covered entities" under the Act, in addition to other tasks the Act assigns to Agency.
- Entities in a critical infrastructure sector that experience a substantial cyber incident shall report to Agency within 72 hours.
- Entities in a critical infrastructure sector that make a ransom payment as the result of a ransomware attack shall report the payment to the Agency within 24 hours.
- Provide supplemental disclosures after substantial cyber incidents, as necessary.
- Record retention obligations are imposed.

Why It Matters to You

To be able to comply with the tight reporting requirements under the Act, every covered entity should revisit its incident response

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

plan, and in particular the plan's communication matrix. Although the functional requirements of the Act are subject to additional rulemaking, companies should immediately consider:

- Are they a covered entity subject to the Act?
- Which stakeholders need to be engaged in this process of revision and future compliance?
- How best to modify your communication matrix in light of the Act?
- How must your response plan be modified to meet the expedited reporting?

There are a total of 16 critical infrastructure sectors affected by the Act, including: Energy, Financial Services, Government Facilities, Healthcare and Public Health, Information Technology, Transportation Systems, and more.[2]

Preparing for your company for a cybersecurity incident is more important than ever. [3] Navigating the Act's new requirements, and compliance with other existing cyber security and reporting laws and regulations can be daunting, with the risk that mistakes can result in brand damage and adverse legal consequences.

For more information, contact Bill Repasky, Emma Mulvaney, or any attorney with Frost Brown Todd's Financial Services, Energy, Health Care industry teams, or Government Services practice group with any questions you may have.

---

[1] *See e.g.,* The White House, "FACT SHEET: Act Now to Protect Against Potential Cyberattacks," March 21, 2022; The White House's memorandum "What We Urge You To Do Protect Against the Threat of Ransomware," June 2, 2021.

[2]The White House, "Presidential Policy Directive — Critical Infrastructure Security and Resilience," February 12, 2013. Further, the implementing regulations, while expected on an expedited basis, possibly will impact the scope of covered entities beyond the original definition stated in § 2240 of the Homeland Security Act of 2002.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons