POLSINELLI. What a law firm should be.™

Critical Infrastructure Cybersecurity – Evolving Incident Response Obligations, Integral to Effective Risk Management

Just over a year ago, the White House issued its long-awaited **National Cybersecurity Strategy**,[1] with an emphasis on defending **Critical Infrastructure**,[2] **promoting public and private collaboration**,[3] and safeguarding the *availability* of sixteen sectors whose assets, systems, and networks are deemed critical to national security, and public health or safety.

For the cybersecurity threat landscape, a year can seem like an eternity. In January, this was hammered home when appearing before a House subcommittee, the FBI Director warned that China was ramping up an extensive hacking operation designed to take down the United States' power gird, oil pipelines, and water systems:[4]

Low blows against civilians are part of China's plan. China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike.

Russia has been ramping up too. A 44-page report published this week by cybersecurity firm Mandiant,[5] describes how a group calling itself CyberArmyofRussia_Reborn hacked into "multiple local U.S. water infrastructure systems." Two of these systems are in Texas, as was confirmed in early February.[6]

As if on cue, in mid-February the Cybersecurity and Infrastructure Security Agency released three priorities for public and private partners: (1) defending against advanced persistent threat (APT) operations, (2) raising the cybersecurity baseline, and (3) anticipating emerging technology and risks.[7] According to CISA, these priorities will enable alignment.

On March 27, 2024, CISA released a notice of proposed rulemaking for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which will implicate all of the above priorities, especially the second. The final rule is expected by 2025 with reporting requirements beginning in 2026. Interested parties have until June 3, 2024, to submit comments.

I. CIRCIA -- Who and What is Covered

At its core, CIRCIA requires critical infrastructure entities to report substantial cybersecurity incidents to CISA within 72 hours and ransomware payments within 24 hours, and applies to the 16 critical infrastructure sectors entities enumerated in Presidential Policy Directive 21 (PPD 21)[8] and graphically depicted here:

CISA estimates that there will be 316,244 entities potentially affected by the proposed rule.

Substantial Cyber Incidents

Under CIRCIA, a substantial cybersecurity incident is defined as an incident that leads to any of the following:

1. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
2. A serious impact on safety and resiliency of operational systems and processes;
3. A disruption of ability to engage in business or industrial operations, or deliver goods or services; or
4. Unauthorized access caused by a: (1) compromise of a cloud service provider, managed service provider, or other third-party data hosting provider, or (2) supply chain compromise.

The proposed rule lists 10 examples of incidents that would likely qualify as substantial cyber incidents. For example, a distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period, or a ransomware attack that locks a covered entity out of its industrial control system.

Reporting Requirements for CIRCIA

Covered entities **must report substantial cyber incidents** within 72 hours after they "reasonably believe" that a reportable incident has occurred, similar to the recent NCUA 72 hour reporting rule for some financial institutions.[9] While a covered entity is not required to determine the cause of an incident, it may be necessary to grant any additional time.

When CIRCIA was passed in 2022, CISA identified "10 Key Elements to Share" as part of the reporting requirement.[10] That has been expanded through the rulemaking process to require more

granular information such as a description of the covered entity's security defenses, any indicators of compromise, and a description, copy or sample of any malicious software.

Notice of a ransom payment having been made must be submitted within 24 hours even if the ransomware attack that resulted in a ransom payment is not a substantial incident. Ransom payment reports must generally also include the same or similar granular information provided for a substantial incident cyber incident and also identify incident response efforts.

The proposed rule also requires covered entities to file Supplemental Reports if new or different information becomes available after filing the initial report or if a ransom payment is made, and to reduce the number of required notices, CISA can enter into "CIRCIA Agreements" with other Federal agencies to establish information sharing mechanisms.

Liability Protection and Enforcement

CIRCIA reports are exempt from disclosure under the Freedom of Information Act, and "may not be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof."

Also, CISA will have the ability to request or subpoena information if they believe an organization did not report a covered cyber incident or ransomware payment. Further, CISA may pursue criminal penalties under 18 U.S.C. 1001 against any person who knowingly and willfully makes materially false or fraudulent statements in connection with a CIRCIA Report.

II. NIST Releases New Incident Response Recommendations

Even though CIRCIA will not be enforced until 2026, it arguably mandates standards that many covered entities should already have: (1) a Cybersecurity Incident Response Plan, (2) a Cybersecurity Risk Assessment, and (3) a Written Information Security Program. For CIRCIA-readiness, each of these should be reviewed and updated.

Coincidentally, on April 2, 2024, the National Institute of Standards and Technology (NIST) released for public comment its *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*.[11] These recommendations are significant given NIST's recognition by various federal regulations and even some state cybersecurity laws.

The recommendations are in draft form and will incorporate NIST's landmark release of version 2.0 of its Cybersecurity Framework in February, and is essentially a makeover of the Computer Security Incident Handling Guide released in 2012. These two statements stand out:

- Lessons learned from incident response activities and root cause analysis help improve cybersecurity risk management and governance efforts, and
- Incident response has evolved to become a critical part of cybersecurity risk management, as well as how the concept of the incident response life cycle has changed to reflect that.

With CIRCIA and the other cybersecurity regulations that have emerged, and the surging wave of 'adversarial AI' cyberattacks, incident readiness will become an intense area of focus for legal and compliance obligations. Improving governance is expected, but achieving technical perfection is not. A month ago, even CISA announced it had been successfully hacked.[12]

---

[1] https://www.polsinelli.com/kurt-r-erskine/publications/its-here-the-new-national-cybersecurity-strategy

[2] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] https://www.jdsupra.com/legalnews/leveraging-public-private-collaboration-2851378/

[4] https://www.nytimes.com/2024/01/31/us/politics/fbi-director-china-wray-.html#:~:text=Christopher%20A.%20Wray%2C%20director%20of,of%20a%20conflict%20over%20Taiwan.

[5] https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

[6] https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/?

[7]https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2024-jcdc-priorities

[8] *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*, The White House: Office of the Press Secretary, **https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil**.

[9] https://www.polsinelli.com/alexander-d-boyd/publications/how-credit-unions-can-prepare-for-3-day-cyber-report-rule

[10] https://www.cisa.gov/sites/default/files/2022-11/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf

[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[12] https://www.cybersecuritydive.com/news/cisa-attacked-ivanti-cve-exploits/709893/