wiley

NEWSLETTER

CISA Signals Cyber Incident Reporting Requirements

May 2022

Privacy In Focus®

In March 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requiring critical infrastructure to report significant cyber incidents and ransomware payments to the Cybersecurity & Infrastructure Security Agency (CISA) within tight time frames under rules to be developed. CISA has now signaled what its reporting priorities are. Here's what critical infrastructure entities should know:

What Triggers a Reporting Obligation

CISA's reporting obligations focus on the following:

1. **Significant Cyber Incident:** When there is a reasonable belief that a significant cyber incident has occurred, the covered incident must be reported to CISA within **72 hours**.
2. **Ransomware Payment:** When a covered entity has made a ransomware payment, CISA must be notified within **24 hours of ransom payment.**

Where CISA Is with Promulgating Rules

Under CIRCIA, CISA must issue a notice of proposed rulemaking (NPRM) within 24 months and then issue a final rule within 18 months after the NPRM is issued. The reporting requirement does not go into effect until the rule is finalized, but CISA strongly encourages voluntary sharing of cyber event information.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Of Counsel
202.719.4114
jfbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Privacy, Cyber & Data Governance

While those rules are being developed, CISA recently offered a preview of its incident reporting priorities. On April 7, 2022, CISA provided stakeholders with guidance about sharing cyber event information providing specific information about what to share, who should share, and how to share information about unusual cyber incidents or activities. In doing so, CISA emphasized that cybersecurity information sharing is essential to our collective defense and strengthening cybersecurity for the nation.

What Types of Activity to Share

CISA wants critical infrastructure entities to report the following types of activities to CISA:

1. Unauthorized system access
2. Denial of Service (DOS) attacks that last more than 12 hours
3. Malicious code found on systems, including any variants, if known
4. Targeted and repeated scans against services on systems
5. Repeated attempts to gain unauthorized access to a system
6. Email or mobile messages associated with phishing attempts or successes
7. Ransomware attacks against critical infrastructure, including the variant and ransom details

Top 10 Key Elements to Share

CISA has prioritized the following 10 key elements for sharing:

1. Incident date and time
2. Incident location
3. Type of observed activity
4. Detailed narrative of the event
5. Number of people or systems affected
6. Company/Organization name
7. Point of Contact details
8. Severity of event
9. Critical Infrastructure Sector, if known
10. Anyone else the victim informed

Who Should Share

Critical infrastructure owners and operators now face statutory mandates to report significant cyber incidents or ransomware payments, which obligations will become effective when CISA finalizes its new rules.

Entities in the 16 critical infrastructure sectors currently include: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care/public health, information technology, nuclear reactors/materials/waste, transportation, and water/wastewater systems.

The subsequent rulemaking will further define whether companies in those sectors are "covered entities" who must report, based on the impact of a compromise or disruption and the likelihood that the company could be targeted.

How to Share

CISA has three (3) established mechanisms for sharing cyber event information:

- CISA Incident Reporting System: Critical infrastructure partners can complete an incident report form, which contains a variety of prompts and a convenient way to electronically report.
- Reports@cisa.gov: Critical infrastructure entities that have never used the CISA Incident Report System, or that want to expeditiously submit a report, can send an email to Reports@cisa.gov providing as much information about the cyber event as they can.
- Phishing-report@us-cert.gov: Entities can also share phishing information regarding phishing emails, mobile messages, and website locations by sending an email to phishing-report@us-cert.gov.

Upon receipt, CISA will triage the reports and may share anonymized information about the reported activity with others to help them manage their risks. CISA frequently uses reported information to provide assistance to the victim or to warn other organizations about particular attacks. As these reporting rules are being developed, CISA continues to encourage stakeholders to voluntarily share information about cyber-related events that could help mitigate current or emerging cybersecurity threats to critical infrastructure.

What's Next

While CIRCIA provides CISA with two years to develop proposed rules, Wiley anticipates that CISA may attempt to issue an NRPM in advance of that date given the increased magnitude of cybersecurity threats and ransomware attacks.

Once those proposed rules are issued, critical infrastructure entities and related trade associations will have an important opportunity to comment on how the prospective obligations will impact their operations. Critical infrastructure owners and operators should consider making comments on the NRPM to help define which companies need to report what types of incidents.

Whom to Contact

Wiley's Cyber and Privacy Investigations, Incidents & Enforcement Team has been advising clients for over a decade on cybersecurity incident response and risk management. Wiley helps organizations comply with recent government reporting requirements, plan for compliance with the Cyber Incident Reporting for Critical

Infrastructure Act of 2022 and proposed SEC rules, and obtain protections under the program for Protected Critical Infrastructure Information and CISA 2015. We urge clients to proactively build relationships with the Federal Bureau of Investigation (FBI) and DHS as we enter a new phase of public-private collaboration, which includes disclosure obligations and penalties for cybersecurity deficiencies, and we can help them do so.

Please contact Megan L. Brown, Jacqueline F. "Lyn" Brown, Jon W. Burd, Duane C. Pozza, Antonio J. Reynolds, Kathleen E. Scott, Joan Stewart, or Joshua K. Waldman with questions or for advice.