BCLP. Client Intelligent

Insights

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT – WHAT COMPANIES NEED TO KNOW NOW

Jul 05, 2022

The Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA" or "the Act") is a new federal law, adopted in March 2022, which requires critical infrastructure entities to report certain cybersecurity incidents and ransom payments to the Cybersecurity and Infrastructure Security Agency ("CISA") within a matter of hours. Although CIRCIA garnered significant fanfare at the time it was signed into law, many details remain to be hashed out by implementing regulations, which could take years to finalize.[1] Covered entities, however, should take no comfort in this delay. CIRCIA provides remarkably detailed guidance concerning the scope of these regulations, putting covered entities on clear notice of their future obligations and the consequences of failing to comply. In this Alert, we outline what critical infrastructure entities need to know about these new reporting rules – now and in the future.

What Are the New Reporting Obligations?

CIRCIA establishes two new reporting obligations. First, CIRCIA requires covered entities that experience a "covered cyber incident" to report the incident to CISA within 72 hours after the entity "reasonably believes" that the incident has occurred.[2] Second, CIRCIA requires covered entities to report all ransom payments made as a result of ransomware attacks within 24 hours after any such payment, regardless of whether the ransomware attack is a covered cyber incident.[3]

If the "ransomware attack" also qualifies as a "covered cyber incident" and the ransom payment is made within the 72 hour period, the covered entity need only provide one report, even if the report is made more than 24 hours after the ransom was paid.[4]

Who Is Required to Report?

CIRCIA's new reporting requirements will apply to entities that operate in a "critical infrastructure sector" if they also satisfy the definition of "covered entity" – a definition left to the rule-making process.[5] These "critical infrastructure sectors" were identified in a 2013 Presidential Policy

Directive and include a broad swathe of private and public industry conducting business in the following areas:

Critical Infrastructure Sectors			
Chemical	Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services	Energy
Financial Services	Food & Agriculture	Government Facilities	Healthcare & Public Health
Information Tech	Nuclear	Transportation	Water & Wastewater

In developing a definition of "covered entity," CIRCIA requires CISA to consider three broad factors: (1) the consequences that a particular cyber incident might have on national or economic security, public health and safety; (2) the likelihood that the entity could be targeted for attack; and (3) the extent to which an incident is likely to disrupt the reliable operation of critical infrastructure.[6] Based on these criteria, most, if not all, companies operating in these 16 sectors should be prepared to comply with CIRCIA's new reporting rules.

What Types of "Covered Cyber Incidents" Must Be Reported Within 72 Hours?

CIRCIA requires covered entities to report "covered cyber incidents." Although the precise definition of "covered cyber incident" is left to later rulemaking, CIRCIA provides extensive guidance about the types of incidents that should be reported.

First, CIRCIA defines a "cyber incident" as an incident that "actually" jeopardizes an information system or the information contained on such a system.[7] A threat of imminent harm to an information system, therefore, is not covered.

Second, CIRCIA provides that a "covered cyber incident" must be a "substantial" cyber incident.[8] Again, although CIRCIA does not define "substantial," it states that a "substantial" cyber incident must include, "at a minimum," the following types of incidents:

- incidents that lead to "substantial loss of confidentiality, integrity, or availability of an affected information system or network, or a serious impact on the safety and resiliency of operational systems and processes;"
- incidents that disrupt business or industrial operations, including due to a DDoS attack, ransomware attack or exploitation of a zero day vulnerability; or

- Incidents that involve "unauthorized access to or disruption of business or industrial operations" triggering a loss of service that is caused by the compromise of a cloud service provider, other third-party data hosting provider or by a supply chain compromise.[9]

In addition to these minimum criteria, CIRCIA also requires CISA to consider other factors in establishing the types of "substantial" incidents that will be considered "covered cyber incidents" They include: (i) the tactics used; (ii) the type of data at issue; (iii) the number of individuals potentially affected; and (iv) the potential impact of the incident on industrial control systems.[10] In short, a broad range of incidents are likely to be considered "substantial" cyber incidents that will have to be reported within 72 hours.

What Types of Ransom Payments Must Be Reported Within 24 Hours?

The ransom payment reporting obligation is clearly defined in the statute and does not depend on future rule-making to understand its scope. CIRCIA defines a "ransom payment" broadly as the "transmission of any money or other property or asset, including a virtual currency" which has "at any time been delivered as ransom in connection with a ransomware attack."[11]

A "ransomware attack," in turn, is defined as an incident that includes the "use or threat of use" of unauthorized or malicious code or some other mechanism "to interrupt or disrupt" the operations of an information system or to compromise the data on an information system "to extort a demand for a ransom payment."[12] A "ransomware attack," however, does not include an event in which the demand for payment is "not genuine" or is made in good faith in response to a specific request by the owner or operator of the information system.[13]

What Must Be Included in the Reports?

The specific information to be included in these reports, as well as the procedures for submitting them, are left for the rulemaking process. Nevertheless, extensive guidance about what should be included in these reports is set forth in the Act.[14] For instance, "covered cyber incident" reports must contain, among many other things, a description of the impacted information systems or networks, the unauthorized access and the impact to the covered entity's operations.[15] Reports of ransom payments also must contain a description of the attack, the vulnerabilities and tactics used to perpetrate the attack, any known criminal identifiers, entity contact information, and information relating to the ransom demand itself.[16]

Does CIRCIA Impose Any Continuing Obligations?

Yes. CIRCIA requires covered entities to provide supplemental reports if "substantial new or different information becomes available" or if the covered entity makes a ransom payment after submitting a covered cyber incident report.[17] Covered entities are obligated to provide these

updated reports until they notify CISA that the covered cyber incident "has concluded and has been fully mitigated and resolved."[18] CIRCIA also requires covered entities to preserve data relevant to any reported matters.[19] The deadlines and criteria for submitting these supplemental reports and the procedures for preserving data will be established during the rulemaking process.[20]

What Are The Consequences of Failing to Report?

If a covered entity fails to report a covered cyber incident or ransom payment, CISA may issue a request for information to the covered entity.[21] If the covered entity fails to respond or to respond adequately to CISA's information request within 72 hours, CISA may issue a subpoena to compel disclosure.[22] If the covered entity fails to comply with the subpoena, CISA may refer the matter to the Attorney General who may bring a civil action to enforce the subpoena; failure to comply with the subpoena may be punishable by contempt.[23] Once again, however, specific procedures for carrying out these enforcement provisions and "other available enforcement mechanisms" will be developed during the rulemaking process.[24]

Are There Any Criminal Ramifications?

CIRCIA provides that information reported to CISA pursuant to the statute may be used by the federal government for several broadly stated purposes, such as identifying cyber threats or vulnerabilities, responding to or preventing specific threats of death or serious bodily harm or economic harm, or prosecuting offenses arising out of a reported cyber incident.[25] In addition, if information provided in response to a subpoena issued pursuant to the Act identifies grounds for a regulatory enforcement action or criminal prosecution, CIRCIA authorizes CISA to provide such information to the Attorney General or appropriate federal agency official for such purposes.[26] Notably, CIRCIA also contains a catch-all provision which says that nothing in the Act shall be construed to limit the authority of the U.S. Government to take action "with respect to the cybersecurity of an entity."[27]

Does CIRCIA Provide Any Protections or Safe Harbors?

CIRCIA provides several protections for reporting entities. CIRCIA prohibits federal, state and local governments, in certain limited circumstances, from regulating covered entities and pursuing enforcement actions based on submitted reports.[28] CIRCIA also provides that reports will not be publicly available through FOIA or similar information disclosure laws or constitute a waiver of any applicable privilege or protection.[29] In addition, no report shall be the basis of litigation, admitted into evidence, subject to discovery or otherwise used in any judicial, federal or state regulatory proceeding, except when brought by the federal government to enforce a subpoena pursuant to this Act.[30] Finally, entities that are required to provide substantially similar reports to another federal agency within a substantially similar timeframe are not required to submit the reports required by

CIRCIA, provided that the agency to which the report was submitted has an agreement and sharing mechanism in place with CISA.[31]

What Should Critical Infrastructure Entities Be Doing Now?

Once CIRCIA's final regulations are implemented, entities that operate within the critical infrastructure sectors will be required to meet several new and stringent incident reporting obligations. The potentially lengthy rulemaking process, however, should not delay preparatory actions. The Act contains detailed guidance about the types of incidents that should be reported within very short time frames and the types of information that should be included in those reports. Companies in the critical infrastructure sectors should use this time now to review their incident response plans, procedures and playbooks and conduct relevant tabletop exercises to ensure that their teams are prepared to react as quickly and efficiently as possible when these cyber incidents and ransomware attacks occur.

---

[1] H.R. 2471 § 2242(a)(7), (b). The Act requires CISA to publish proposed regulations not later than 24 months following enactment (i.e., by March 2024), and to issue final regulations not later than 18 months thereafter (i.e., by September 2025).

[2] H.R. 2471 § 2242(a)(1).

[3] H.R. 2471 § 2242(a)(2).

[4] H.R. 2471 § 2242(a)(5)(A).

[5] H.R. 2471 § 2240(5).

[6] H.R. 2471 § 2242(c)(1). Specifically, CISA must consider: "A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure."

[7] H.R. 2471 § 2240(6).

[8] H.R. 2471 § 2240(4).

[9] H.R. 2471 § 2242(c)(2)(A).

[10] H.R. 2471 § 2242(c)(2)(B).

[11] H.R. 2471 § 2240(13).

[12] H.R. 2471 § 2240(14)(A).

[13] H.R. 2471 § 2240(14)(B).

[14] H.R. 2471 § 2242(a)(6).

[15] H.R. 2471 § 2242(c)(4)(A)-(F).

[16] H.R. 2471 § 2242(c)(5).

[17] H.R. 2471 § 2242(a)(3).

[18] Id.

[19] H.R. 2471 § 2242(a)(4).

[20] H.R. 2471 § 2242(a)(4), (c)(6).

[21] H.R. 2471 § 2244(a), (b).

[22] H.R. 2471 § 2244(c)(1).

[23] H.R. 2471 § 2244(c)(2).

[24] H.R. 2471 § 2242(c)(8)(B).

[25] H.R. 2471 § 2245(a)(1)(A)-(E).

[26] H.R. 2471 § 2244(d)(1).

[27] H.R. 2471 § 2242(h).

[28] H.R. 2471 § 2245(a)(5)(A).

[29] H.R. 2471 § 2245(b).

[30] H.R. 2471 § 2245(c).

[31] H.R. 2471 § 2242(a)(5)(B).

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Gabrielle A. Harwell

Chicago

gabrielle.harwell@bclplaw.com
+1 312 602 5143
