April 3, 2024

CISA Issues Highly Anticipated, Far-Reaching Rules for Cyber Incident Reporting

On March 27, the Cybersecurity and Infrastructure Agency ("CISA") released a notice of proposed rulemaking ("NPRM") setting out its initial approach to new reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA").

Prior to the passage of CIRCIA, the federal government lacked a mandate to systematically collect cyber incident information reliably and at the scale necessary to provide situational awareness of cyber threats across critical infrastructure. CIRCIA established a new mandatory incident reporting requirement to fill this gap, but left CISA to define precisely which entities will be covered and what information they will be required to report. The NPRM fills in these details and moves CISA one step closer to a final rule, which will be due by October 2025 but could be finalized earlier.

Under the NPRM, CISA would require certain entities in critical infrastructure sectors—defined broadly enough to sweep in most large and medium (and some small) businesses—to promptly report covered cyber incidents and ransomware payments to CISA. Whether an incident is reportable would generally turn on the severity of the impact of the incident, except that all supply chain compromises or other incidents facilitated by third parties must be reported. The NPRM goes on to specify in detail the information that CISA proposes to collect through these reports. If adopted, the NPRM will require far more detail than is required under many existing incident reporting regimes. It will also provide protections and limitations on how this information can be used.

This is a significant regulatory development for many U.S. companies, including those already subject to a patchwork of reporting requirements related to cyber incidents. CISA's own estimate is that this rule will cover more than 300,000 companies and other covered entities when it goes into effect, and the proposed rules would require faster and more detailed reporting than many of the existing incident reporting regimes. And the NPRM's enforcement provisions suggest that CISA intends to aggressively follow up with companies, including by issuing subpoenas and enlisting the Department of Justice ("DOJ") to bring a civil action to enforce such subpoenas when necessary, to ensure that CISA receives all of the information it is entitled to under the proposed rules.

Background

Enacted in 2022, CIRCIA established additional mechanisms to improve reporting of cybersecurity incidents and ransomware payments by companies in critical infrastructure sectors, while also introducing ways for CISA to coordinate among federal agencies in order to share information and harmonize practices.[1]

For private companies, the core of CIRCIA's new regulations involves reporting obligations. However, the statute left it to CISA to clarify many of the key requirements in subsequent rulemaking. Under CIRCIA, any "covered entity" must report a "covered cyber incident" to CISA within 72 hours after the entity reasonably believes that the covered cyber incident occurred; similarly, a covered entity that makes a ransom payment "as the result of a ransomware attack" must report that payment to CISA within 24 hours.[2] But CISA was tasked with determining the specifics as to which entities qualify as "covered entities" (with reference to 16 critical infrastructure sectors)[3]; which incidents constitute "covered cyber incidents"; what information should be included in a report; what data must be preserved by covered entities that experience an incident; and what the details of reporting and enforcement procedures should be.[4]

CIRCIA gave CISA two years to prepare its NPRM. During that time, other federal cybersecurity regulations evolved. Among the most notable was the SEC's 2023 adoption of requirements for public companies to disclose material cybersecurity incidents on Form 8-K and details about cybersecurity risk management on Form 10-K.[5] During this two-year period, CISA conducted a series of listening sessions across the country and with different critical infrastructure sectors.[6] It also solicited written comments on the issues involved in the upcoming rulemaking, including the definition of key terms, the content of required reports, the costs of reporting regimes on private companies, and entities' experiences under other federal and state regulatory regimes.[7]

The NPRM

In the NPRM, CISA details and invites comment on proposed regulations to implement CIRCIA's covered cyber incident and ransom payment reporting requirements.

1. Covered Entities

The definition of entities covered by CIRCIA's reporting requirements is far from straightforward, requiring reference to industry-specific planning documents, the size of an entity, and consideration of more than a dozen specific sector-based criteria.

CIRCIA defines "covered entity" as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive ("PPD") 21, that satisfies the definition established by [CISA]."[8] Thus the first step is to consider whether an entity is in a critical

---

1 6 U.S.C. §§ 681–681g. For another overview of CIRCIA prepared by CISA, *see* https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf.

2 6 U.S.C. § 681b(a).

3 *See* Presidential Policy Directive 21 (Feb. 12, 2013) (listing sixteen critical infrastructure sectors).

4 6 U.S.C. § 681b(b).

5 *See* https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/sec-adopts-new-cybersecurity-disclosure-requirements?id=47481. The White House is reportedly considering whether to take additional steps beyond the reporting requirements under CIRCIA, to potentially include a ban on ransomware payments. *See* Matt Kapko, *White House considers ban on ransom payments, with caveats*, Cybersecurity Dive (May 8, 2023), https://www.cybersecuritydive.com/news/white-house-considers-ransom-payment-ban/649673/.

6 *See* https://www.cisa.gov/news-events/news/circia-one-year-look-behind-scenes.

7 *See* Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022*, 87 Fed. Reg. 55833 (Sept. 12, 2022), https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

8 6 U.S.C. § 681(4).

infrastructure sector. PPD 21, a 2013 executive action designed to unify the federal government's actions to harden critical U.S. infrastructure from both physical and cyber threats, identified 16 critical sectors.[9] The National Infrastructure Protection Plan required each of those sectors to update its Sector-Specific Plan ("SSP") as part of an overall joint planning effort involving representatives of government and the private sector. Each of those SSPs, which are available on the CISA website, includes a "sector profile" that describes entities that are in the respective critical infrastructure sector.

The breadth of entities in these sectors is startling. According to the 2015 Food and Agriculture SSP, for example, the sector included 2.1 million farms, 935,000 restaurants, and an estimated 114,000 supermarkets, grocery stores, and other food outlets. The 2015 Commercial Facilities SSP included 1.1 million shopping centers and retail establishments, 1 million office buildings, and 5.6 million multi-family rental buildings, among other entities. The financial services sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. The information technology sector broadly includes entities that provide IT hardware, software, systems, and services, with services including development, integration, operations, communications, testing, and security. CISA notes that "[t]he overwhelming majority of entities . . . are considered part of one or more critical infrastructure sectors."

Under the NPRM, covered entities subject to CIRCIA's reporting requirements will include all entities that (1) are in a critical infrastructure sector and (2) are not small businesses. The NPRM adopts the Small Business Administration's size standards, which vary by industry and are generally based on the number of employees or the amount of annual revenue. Currently, the threshold for those industries for which small business status is determined by the number of employees is between 100 and 1,500 employees, depending on the industry. The threshold for those industries for which small business status is determined by annual revenue is between $2.25 million and $47 million, depending on the industry.

But small businesses do not enjoy a blanket exception. Small businesses in critical infrastructure sectors may still be subject to CIRCIA if they meet one or more of 16 sector-based criteria, regardless of which specific sector the entity is in. These broad criteria sweep in small businesses that provide internet or telecommunications service, engage in certain categories of manufacturing, are financial services entities such as banks and credit unions, school districts with at least 1,000 students, and certain information technology entities, among others.[10] Additionally, all contractors and subcontractors required to report cyber incidents to the Department of Defense under 48 C.F.R. § 252.204-7012 are also covered entities under CIRCIA.

CISA estimates that there are approximately 316,000 covered entities that will be required to comply with the proposed rule.

2. Covered Cyber Incidents

CIRCIA requires covered entities to report those cyber incidents that qualify as covered cyber incidents, and the law defines a covered cyber incident as "a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria

[9] The White House is reportedly revising PPD 21, a process that could update the definitions of critical sectors before the CIRCIA regulation is finalized. *See* Tim Starks, *A presidential critical infrastructure protection order is getting a badly needed update, officials say*, The Washington Post (May 11, 2023), https://www.washingtonpost.com/politics/2023/05/11/presidential-critical-infrastructure-protection-order-is-getting-badly-needed-update-officials-say/.

[10] The complete list of sector-based criteria identifies entities that (1) own or operate a covered chemical facility, (2) provide wire or radio communications service, (3) own or operate critical manufacturing sector infrastructure, (4) provide operationally critical support to the Department of Defense or processes, stores, or transmits covered defense information, (5) perform an emergency service or function, (6) are bulk electric and distribution system entities, (7) own or operate financial service sector infrastructure, (8) qualify as a state, local, tribal, or territorial government entity, (9) qualify as an educational facility, (10) are involved with information and communications technology to support elections processes, (11) provide essential public health-related services, (12) are information technology entities, (13) own or operate a commercial nuclear power reactor or fuel cycle facility, (14) are transportation system entities, (15) are subject to regulation under the Maritime Transportation Security Act, and (16) own or operate a qualifying community water system or publicly owned treatment works.

established by [CISA]."[11] Consistent with the minimum requirements in CIRCIA, CISA proposes "substantial cyber incident" to mean "a cyber incident that leads to any of the following:

(a) A **substantial loss** of confidentiality, integrity or availability of a covered entity's information system or network;

(b) A **serious impact** on the safety and resiliency of a covered entity's operational systems and processes;

(c) A **disruption** of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;

(d) **Unauthorized access** to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a:

(i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

(ii) Supply chain compromise."

The *first two* threshold impacts that would qualify an incident as substantial—and therefore reportable—cyber incident turn on the interpretation of the qualifiers "substantial" and "serious." CISA explains that whether a loss of confidentiality, integrity, or availability constitutes a "substantial" loss will likely depend on a variety of factors, such as the type, volume, impact, and duration of the loss or impact. The NPRM includes examples of cyber incidents that typically would meet the "substantial" threshold, including:

- A distributed denial-of-service ("DDoS") attack that renders a covered entity's service unavailable to customers for an extended period of time.
- A ransomware attack or other attack that encrypts one of a covered entity's core businesses or information system substantially impacting the confidentiality, availability, or integrity of the entity's data or services.
- Persistent access to information systems by an unauthorized third party.
- Time-limited access to certain high-value information systems, such as access to privileged credentials or to a domain controller.
- A large-scale breach or otherwise meaningful exfiltration of data.
- A theft of data that may not itself be "substantial" could become a substantial cyber incident if the theft is followed by a data leak or a credible threat to leak data.

A "serious impact" to safety and resiliency would similarly depend on a variety of factors, such as the safety or security hazards associated with the system or process, and the scale and duration of the impact. Examples of serious impact include incidents that increase the potential for release of hazardous materials used in chemical manufacturing or incidents that disrupt 911 calls. Despite using the distinct terms "information system" and "operational systems," CISA intends the first two threshold impacts to cover both IT systems and operational technology ("OT") systems.

Although the *third* threshold impact for business disruption does not include a qualifier such as "substantial" or "serious," "CISA believes it is appropriate to read into the prong some level of significance. . . . Generally speaking, incidents that result in

[11] 6 U.S.C. § 681(3).

minimal or insignificant disruptions are unlikely to rise to the level of a substantial cyber incident reportable under this prong; however, the specific circumstances of the disruption should be taken into consideration."

By contrast, CISA regards the absence of a materiality qualifier in the *fourth* threshold impact regarding unauthorized access "to be a reflection of the seriousness of unauthorized access through a third party" such as a managed service provider or cloud service provider because incidents such as the "SUNBURST" malware that compromised the SolarWinds Orion product "uniquely have the ability to cause significant or substantial nation-level impacts, even if the impacts at many of the individual covered entities are relatively minor." Such incidents must be reported where the covered entity has a "reasonable belief" that the unauthorized access was caused by a third party, even if the cause of the incident is not yet confirmed.

To qualify as a substantial cyber incident, the incident must actually result in one or more of the identified impacts. Malicious activity blocked by a firewall or security tool, for example, would not have to be reported. Similarly, the compromise of a single user's credential, such as through a phishing attack, is unlikely to be a substantial cyber incident where there are compensating controls like multifactor authentication in place to preclude use of those credentials to gain unauthorized access to a covered entity's systems.

The proposed definition of "substantial cyber incident" excludes activity such as penetration tests that are conducted in good faith in response to a specific request by the owner or operator of an information system, as well as the mere threat of disruption as extortion.

Based on these criteria, CISA expects to receive a total of approximately 25,000 reports per year.

3. Reporting Requirements

There are two principal circumstances that require covered entities to submit a report to CISA: (1) a covered entity reasonably believes that a covered cyber incident occurred, in which case a report is required within 72 hours, and (2) a covered entity makes a ransom payment as a result of a ransomware attack against the covered entity, in which case a report is required within 24 hours.

CISA acknowledges that an entity may need to perform some preliminary analysis before coming to a "reasonable belief" that a covered cyber incident occurred, thereby starting the clock for the 72-hour reporting obligation. But CISA believes that in most cases, this preliminary analysis should be relatively short in duration (i.e., hours, not days) before a "reasonable belief" is established, and generally would occur at the subject matter expert level and not the executive officer level.

Reports must be submitted through a web-based reporting form (with a telephonic backup option), and may be submitted by a third party on behalf of a covered entity. Among other data, CISA proposes requiring submission of the following categories of information in each report:

- A description of the covered cyber incident, including identification and description of the affected systems, a description of the unauthorized access, the estimated date range of the incident, and the impact to the operations of the covered entity;
- The type of incident (e.g., DDoS, ransomware, multifactor authentication interception);
- Vulnerabilities exploited;
- The tactics, techniques, and procedures ("TTPs") used to cause the incident, including any TTPs that were used to gain initial access;
- Indicators of compromise;

- A description and copy or sample of any malicious software connected with the incident;
- Any attribution-related information;
- Information on the covered entity's security defenses, including controls or measures that resulted in detection or mitigation of the incident; and
- Information about the entity's mitigation and response, including what mitigation measures were in place, what responsive actions the entity has taken, which phase of incident response (e.g., detection, analysis, containment, eradication, recovery, and post-incident activity) the covered entity is currently in, and any engagement with law enforcement.

In the case of a ransomware incident, CISA proposes requiring details such as the date and amount of the ransom payment, the verbatim text of the ransom payment demand, payment instructions, information regarding what occurred as the result of making the ransom payment (e.g., whether exfiltrated data was returned or a decryption key provided), and the identity of any third parties that assisted in responding to the ransomware attack or making the ransom payment.

Given the short time frame in which to report, CISA will accept good faith answers of "unknown at this time" in an initial report, but the NPRM includes requirements to supplement these reports in certain circumstances. Until a covered entity notifies CISA that the covered cyber incident has concluded and been fully mitigated and resolved, a covered entity must submit an update or supplement to a previously submitted report if substantially new or different information becomes available, which includes any required information that an entity initially reported was unknown.

CIRCIA's reporting obligations do not exist in a vacuum—CISA identifies more than three dozen different federal cyber incident reporting requirements. Importantly, CIRCIA includes an exception to its reporting requirements if an entity is legally required to report substantially similar information within a substantially similar time frame to another federal agency with whom CISA has an information sharing agreement and mechanism. If and when CISA enters into an agreement with these other agencies, CISA will publicly identify these agreements on its website so that covered entities are aware when a report submitted to another agency qualifies for the exception under CIRCIA.

4. Preservation Requirements

CIRCIA requires a covered entity that submits a report to CISA to preserve data relevant to the reported cyber incident or ransom payment. The NPRM proposes to require entities to preserve for two years data and records relating to communications between the covered entity and the threat actor; indicators of compromise; relevant log entries, memory captures, and forensic images; network information or traffic related to the cyber incident; the attack vector; system information that may help identify vulnerabilities that were exploited to perpetrate the incident; information on any exfiltrated data (i.e., the type and amount of data, not copies of all of the exfiltrated data); data and records related to any ransom payment made; and any forensic or other reports about the cyber incident.

5. Enforcement Procedures

CISA proposes four primary enforcement mechanisms in the event an entity fails to comply with CIRCIA's reporting requirements:

(a) **Requests for information**: In the event that CISA believes a covered entity experienced a covered cyber incident or made a ransom payment but failed to report it, CISA can issue a request for information ("RFI"). CISA proposes also extending RFIs to scenarios in which CISA believes a covered entity's submissions are deficient. Information submitted in response to an RFI is subject to certain protections, including exemption from disclosure under the Freedom of

Information Act, retention of privilege, and certain restrictions on use, including in regulatory actions or as the basis for legal liability. An RFI cannot be appealed.

(b) **Subpoena**: CISA proposes that if it does not receive an adequate response to an RFI within 72 hours, it may in its discretion issue a subpoena. If a covered entity fails to respond to a subpoena, CISA may enlist DOJ to bring a civil action to enforce the subpoena. To encourage compliance with RFIs, the NPRM states that responses to subpoenas would not enjoy the same protections as responses to RFIs. Instead, subpoena responses can be passed to DOJ or other agencies for regulatory, civil, or criminal enforcement. A decision to share such information cannot be appealed. However, the issuance of a subpoena can be appealed to the CISA Director.

(c) **Acquisition penalties , suspension, and debarment**: CISA proposes referring noncompliance that may warrant suspension and debarment to the DHS Suspension and Debarment Official. Such proceedings have the potential to impact a covered entity's ability to do business with the federal government. Further, CISA can provide information regarding a noncompliant entity with a procurement contract with the government to the relevant contracting agency.

(d) **False statements and representations**: Although CIRCIA does not include standalone criminal penalties, CISA may refer any false statements in connection with a CIRCIA Report, RFI response, or reply to a subpoena that rise to the level of criminal prosecution to DOJ.

6. Protections and Restrictions on Use of Reported Information

CISA proposes several protections for information submitted in CIRCIA Reports and in response to RFIs. However, responses to subpoenas would not be subject to the same safeguards. For information disclosed in a Report or in response to an RFI, available protections include:

- **Designation as commercial, financial, and proprietary information**: CISA proposes to allow covered entities to designate information provided in a Report or in response to an RFI as commercial, financial, and propriety information belonging to the covered entity. Following designation, CISA will treat such information accordingly.

- **FOIA exemption**: Reports and responses to RFIs would be exempt from FOIA and any state, local, tribal or territorial laws governing freedom of information.

- **No waiver of privilege**: Under CIRCIA, a covered entity can still assert privilege or protections, such as the attorney-client and work product privileges, as well as the trade secret protection, for any information disclosed in a CIRCIA Report or response to an RFI.

CISA also proposes various restrictions on use of the information it receives through Reports by covered entities.

- **Restricted use in regulatory actions**: Generally, information obtained solely through a CIRCIA Report or through a response to an RFI cannot be used in an enforcement or other regulatory proceeding. However, if a federal, state, or local government entity streamlines its own independent reporting requirements by allowing a covered entity to meet a separate requirement through submission of a report to CISA, those government entities are permitted to use the reports for regulatory purposes.

- **Liability protection**: No civil cause of action can lie in court based solely on the fact of submission, or content, of a CIRCIA Report or response to an RFI. CISA also proposes an evidentiary and discovery bar related to CIRCIA Reports and responses to RFIs. However, this liability shield does not extend to underlying liability for covered cyber incidents, ransomware attacks, or ransom payments. The liability protection also does not extend to criminal acts.

- **Limitations on authorized uses**: CISA has delineated proposed authorized uses by the government of information submitted in conformance with CIRCIA. These authorized uses include to address events reported through CIRCIA submissions, take certain defensive measures, and assess cyber threat indicators. Information provided to CISA in a Report or in response to an RFI can generally be used only for these delineated purposes.

- **Privacy and civil liberties**: CISA proposes anonymizing, safeguarding, and (subject to lack of relevance) destroying personal information.

Implications

An accelerated, broadly applicable cyber incident reporting regime is coming to the United States. Nearly six years after the European General Data Protection Regulation ("GDPR") and its 72-hour breach reporting requirement went into effect, the U.S. is one step closer to its own 72-hour cyber incident reporting regime. Despite being framed in terms of critical infrastructure, the NPRM makes clear that the reporting requirements will apply broadly to most large and medium businesses, many of which have not traditionally considered themselves to be critical infrastructure. While public companies are now adjusting to new SEC disclosure requirements for material cyber incidents, the bar for reporting incidents to CISA under the NPRM will be significantly lower and require covered entities to report many more incidents than are disclosed under the SEC rule.

In many cases it may not be immediately clear whether an entity is covered by the CIRCIA reporting requirements. The uncertainty results not just from the breadth of sector-specific criteria in the NPRM, but also potential changes to the underlying definitions of critical infrastructure sectors in PPD 21. While CISA estimates that more than 315,000 entities will be covered, it estimates that a far higher number of entities—roughly 13 million—will not actually be covered but will incur some burden to complete the analysis to determine they are not covered entities.

Despite its broad applicability, the CIRCIA reporting regime will not immediately alleviate companies' burden to comply with other federal cyber incident reporting obligations. Overlapping reporting requirements may only exempt companies from the obligation to report under CIRCIA where CISA enters into an agreement with another federal regulator and determines that the other agency's reporting requirement requires entities to report substantially similar information within a substantially similar time frame—a high standard given the detailed reporting the NPRM would require within a 72-hour time frame.

The NPRM is a crucial step in a lengthy rule-making process—two years after CIRCIA became law and 18 months before final regulations are due. Although the NPRM does not impose any new reporting requirements immediately, the 60-day comment period represents the last best chance to offer input on CISA's proposed approach. Once in effect, CISA will face the daunting task of developing a strategy to ensure that hundreds of thousands of covered entities comply with their reporting obligations.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

L. Rush Atkinson
+1-202-223-7473
ratkinson@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Matthew J. Disler and Katherine Fang contributed to this Client Memorandum.