ALERT MEMORANDUM

Regulation Proposed to Implement *Cyber Incident Reporting for Critical Infrastructure Act*

April 24, 2024

On April 4, 2024, the Federal Register published the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's ("CISA") notice of proposed rulemaking, including the text of the proposed regulation that would implement the key provisions of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA" or the "Act"). The proposed regulation defines the scope of the Act's requirement that covered entities in critical infrastructure businesses report covered cyber incidents to CISA. The Act requires covered entities to report incidents within 72 hours of forming a reasonable belief that a substantial cyber incident has occurred, report ransom payments within 24 hours of making such a payment, and preserve related data and records for at least two years. The proposed regulation defines the covered entities subject to the reporting obligations to include entities within 16 critical infrastructure sectors that either (i) exceed the U.S. Small Business Administration's Small Business Size Regulations or (ii) meet one of 16 different sets of criteria in the proposed regulation. The proposed regulation is subject to public comment and further modification. The reporting obligations will not take effect until a final version of the regulation is published in the next 18 months.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Michael Kowiak
+1 212 225 2929
mkowiak@cgsh.com

© Cleary Gottlieb Steen & Hamilton LLP, 2024. All rights reserved.
This memorandum was prepared as a service to clients and other friends of Cleary Gottlieb to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Cleary Gottlieb" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions, and the term "offices" includes offices of those affiliated entities.

Background

As we discussed in a prior alert memorandum, President Biden signed the CIRCIA into law on March 15, 2022.[1] The Act provides that certain entities in critical infrastructure sectors ("Covered Entities") must report certain substantial cyber incidents ("Covered Cyber Incidents") and payments associated with ransomware attacks to CISA within 72-hour and 24-hour timeframes, respectively. In addition, the Act provides that Covered Entities are subject to certain data and record preservation requirements. However, the Act's requirements did not take effect immediately. The requirements will only become operational after CISA enacts a regulation to implement the Act's provisions, including by defining key terms that will determine the final scope of the legislation and the attendant reporting requirements.[2] CISA's recent publication of the proposed regulation (the "Proposed Regulation") is an intermediate step in this process, whereby CISA discloses a provisional version of the proposed regulation and invites public comment on the proposal. CISA must issue a final regulation within 18 months of the publication of the Proposed Regulation. Despite its preliminary nature, the Proposed Regulation serves as a useful indication of the form that the final regulation may take. Entities that meet the current proposed definition of Covered Entities should consider whether to engage in the comment process. Further, Covered Entities should assess whether they have adequate policies, procedures, and systems in place to comply with the Act's reporting requirements, which will take effect upon publication of the final regulation.

The Proposed Regulation: Key Definitions

Definition of Covered Entity

The Proposed Regulation provides CISA's proposed criteria for determining which entities are Covered Entities to whom the Proposed Regulation's cyber incident and ransom payment reporting requirements will apply. Under the Proposed Regulation, an entity is a Covered Entity if it is (i) in one of 16 critical infrastructure sectors and *either* (ii) exceeds an industry-specific "small business size standard" *or* meets a "sector-based criterion."[3]

Critical Infrastructure Sector: As a threshold matter, an entity is only a Covered Entity if it belongs to one of 16 industries that qualify as critical infrastructure sectors under the Act. These sectors include the following: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.[4] If an entity is not part of one of these sectors, it is not a Covered Entity. If an entity is in one of these sectors, the entity must then determine whether it satisfies either of the two subsequent criteria, each of which independently suffices to make an entity a Covered Entity.

Small Business Size Standard: For purposes of the Proposed Regulation, the small business size standard is a list of sector-specific thresholds, organized by NAICS Codes,[5] and based on the "number of employees or annual receipts in millions of dollars" that an entity has (unless otherwise noted). For example, the small business size standard for

[1] The Act was amended on December 23, 2022 by Public Law 117–263, which implemented several technical and clarificatory revisions to the text of the statute.

[2] *See* 6 U.S.C. §§ 681, 681b (leaving "Covered Entity" and "Covered Cyber Incident" to be more fully defined during the rulemaking process, and limiting reporting obligations to Covered Entities).

[3] *See* Proposed Regulation § 226.2.

[4] The Act adopted the definition of critical infrastructure sector from Presidential Policy Directive 21. *See* 6 U.S.C. § 681. The directive is available online. *See* https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf.

[5] NAICS Codes are the industry-specific numeric identifiers associated with the North American Industry Classification System.

Commercial Banking is $850 million in assets and the standard for Surgical and Medical Instrument Manufacturing is 1,000 employees.[6] If an entity is in a critical infrastructure sector and exceeds the small business standard for its industry, it is a Covered Entity to which the Proposed Regulation applies, without regard to the additional sector-based criterion discussed below. Although there are hundreds of NAICS Codes, each with their own small business thresholds, the below chart provides the small business size standards for a few select industries.

NAICS Code	NAICS U.S. Industry Title	Size (USD)	Size (Employees)
211120	Crude Petroleum Extraction	N/A	1,250
221113	Nuclear Electric Power Generation	N/A	1,150
334111	Electronic Computer Manufacturing	N/A	1,250
334413	Semiconductor and Related Device Manufacturing	N/A	1,250
336110	Automobile and Light Duty Motor Vehicle Manufacturing	N/A	1,500
339112	Surgical and Medical Instrument Manufacturing	N/A	1,000
445110	Supermarkets and Other Grocery Retailers (except Convenience Retailers)	$40 million	N/A
481111	Scheduled Passenger Air Transportation	N/A	1,500
522110	Commercial Banking	$850 million (in assets)	N/A
522210	Credit Card Issuing	$850 million (in assets)	N/A
523150	Investment Banking and Securities Intermediation	$47 million	N/A
622110	General Medical and Surgical Hospitals	$47 million	N/A

Sector-Based Criterion: In addition, the Proposed Regulation defines 16 sector-specific criteria. If an entity in a critical infrastructure sector satisfies the relevant sector-based criteria for at least one category, it is a Covered Entity to which the Proposed Regulation applies, "regardless of the specific critical infrastructure sector of which the entity considers itself to be part" and notwithstanding the entity's size under the small business standards discussed above.[7] In other words, these below categories *expand* the scope of the Proposed Regulation to include critical infrastructure sector entities that would not otherwise be covered due to their small size. The 16 sector-based criterion that the Proposed Regulation defines, and the accompanying details of the criteria, are summarized in the following table.[8]

Sector-Based Criterion Category	Summary of Criterion Details
Owns or Operates a Covered Chemical Facility	The entity owns or operates a covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards pursuant to 6 C.F.R. part 27.
Provides Wire or Radio Communications Service	The entity provides communications services by wire or radio communications, as defined in 47 U.S.C. §§ 153(40), 153(59), to the public, businesses, or government, as well as one-way services and two-way services.
Owns or Operates Critical Manufacturing Sector Infrastructure	The entity owns or has business operations that engage in one or more of the following categories of manufacturing: (i) Primary metal manufacturing; (ii) Machinery manufacturing; (iii) Electrical equipment, appliance, and component manufacturing; or (iv) Transportation equipment manufacturing.
Provides Operationally Critical Support to the Department of Defense or Processes, Stores, or Transmits Covered Defense Information	The entity is a contractor or subcontractor required to report cyber incidents to the Department of Defense pursuant to the definitions and requirements of the Defense Federal Acquisition Regulation Supplement 48 C.F.R. §§ 252.204-7012.

[6] *See* 13 C.F.R. § 121. This sector-specific list is available online at https://www.ecfr.gov/current/title-13/chapter-I/part-121.

[7] *See* Proposed Regulation at § 226.2.

[8] *See* Proposed Regulation at § 226.2. Here and elsewhere in this Alert Memorandum, we summarize and excerpt portions of the Proposed Regulation for brevity. Entities that seek to understand whether they are Covered Entities and what the relevant requirements for Covered Entities are under the Act should refer to the full text of the Act and the Proposed Regulation.

Performs an Emergency Service or Function	The entity provides one or more of the following emergency services or functions to a population equal to or greater than 50,000 individuals: (i) Law enforcement; (ii) Fire and rescue services; (iii) Emergency medical services; (iv) Emergency management; or (v) Public works that contribute to public health and safety.
Bulk Electric and Distribution System Entities	The entity is required to report cybersecurity incidents under the North American Electric Reliability Corporation Critical Infrastructure Protection Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report OE-417 form, or any successor form, to the Department of Energy.
Owns or Operates Financial Services Sector Infrastructure	The entity owns or operates any legal entity that qualifies as one or more of the financial services entities specified in the Proposed Regulation, including (i) A banking or other organization regulated by the OCC, the Federal Reserve Board, or the FDIC under certain regulations; (ii) A federally insured credit union regulated by the NCUA under a specific regulation; (iii) A designated contract market, swap execution facility, derivatives clearing organization, or swap data repository regulated by the CFTC under specific regulations; (iv) A futures commission merchant or swap dealer regulated by the CFTC under specific regulations; (v) A systems compliance and integrity entity, security-based swap dealer, or security-based swap data repository regulated by the SEC under a specific regulation; (vi) A money services business as defined in 31 C.F.R. § 1010.100(ff); or (vii) Fannie Mae and Freddie Mac as defined in 12 C.F.R. § 1201.1.
Qualifies as State, Local, Tribal, or Territorial Government Entity	The entity is a State, Local, Tribal, or Territorial government entity for a jurisdiction with a population equal to or greater than 50,000 individuals.
Qualifies as an Education Facility	The entity qualifies as any of the following types of education facilities: (i) A local educational agency, educational service agency, or state educational agency . . . with a student population equal to or greater than 1,000 students; or (ii) An institute of higher education that receives funding under Title IV of the Higher Education Act.
Involved with Information and Communications Technology to Support Elections Processes	The entity manufactures, sells, or provides managed services for information and communications technology specifically used to support election processes or report and display results on behalf of State, Local, Tribal, or Territorial governments.
Provides Essential Public Health-Related Services	The entity provides one or more of the following essential public health-related services: (i) Owns or operates a hospital . . . with 100 or more beds, or a critical access hospital . . . (ii) Manufactures drugs listed in Appendix A of the Essential Medicines Supply Chain and Manufacturing Resilience Assessment . . . or (iii) Manufactures a Class II or Class III device as defined by 21 U.S.C. § 360(c).
Information Technology Entities	The entity meets one or more of the following criteria: (i) Knowingly provides or supports information technology hardware, software, systems, or services to the Federal government; (ii) Has developed and continues to sell, license, or maintain any software that has, or has direct software dependencies upon, one or more components with at least one of the attributes specified in the Proposed Regulation; (iii) Is an original equipment manufacturer, vendor, or integrator of operational technology hardware or software components; (iv) Performs functions related to domain name operations.
Owns or Operates a Commercial Nuclear Power Reactor or Fuel Cycle Facility	The entity owns or operates a commercial nuclear power reactor or fuel cycle facility licensed to operate under the regulations of the Nuclear Regulatory Commission, 10 C.F.R. chapter I.
Transportation System Entities	The entity is required by the Transportation Security Administration to report cyber incidents or otherwise qualifies as one or more of the transportation system entities specified in the Proposed Regulation.
Subject to Regulation under the Maritime Transportation Security Act	The entity owns or operates a vessel, facility, or outer continental shelf facility subject to 33 C.F.R. parts 104, 105, or 106.
Owns or Operates a Qualifying Community Water System or Publicly Owned Treatment Works	The entity owns or operates a community water system, as defined in 42 U.S.C. § 300(f)(15), or a publicly owned treatment works, as defined in 40 C.F.R. § 403.3(q), for a population greater than 3,300 people.

Definitions of Substantial and Covered Cyber Incidents

The Proposed Regulation also articulates a definition of "Substantial Cyber Incidents," which when experienced by Covered Entities constitute Covered Cyber Incidents, and must be reported to CISA. Under the Proposed Regulation, a Substantial Cyber Incident includes a cyber incident that leads to:

— A substantial loss of confidentiality, integrity, or availability of a Covered Entity's information system or network;

— A serious impact on the safety and resiliency of a Covered Entity's operational systems and processes;

— A disruption of a Covered Entity's ability to engage in business or industrial operations, or deliver goods or services;

— 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 Proposed Regulation clarifies that a cyber incident that causes one of the results described in the first three bullets above qualifies as a Substantial Cyber Incident "regardless of cause."[9]

However, the Proposed Regulation also excludes certain incidents from the definition of Substantial Cyber Incident, including "[a]ny event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system." This exception is meant in part to clarify that the Proposed Regulation does not implicate instances where Covered Entities hire and authorize security researchers to attempt to compromise the security of the entity's environment (*e.g.*, penetration testing).[10]

Definitions of Ransom Payment and Ransomware Attack

The Proposed Regulation also includes definitions of ransom payment and a ransomware attack, which establish the contours of when a Covered Entity must report a payment to CISA. The Proposed Regulation defines ransom payment as meaning "the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack."

In turn, the definition of a ransomware attack is "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or that actually or imminently jeopardizes, without lawful authority, an information system." Such an attack "involves, but need not be limited to":

— The use or the threat of use of (i) unauthorized or malicious code on an information system; or (ii) another digital mechanism such as a denial-of-service attack;

— To interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system; and

— To extort a ransom payment.

The definition of ransomware attack specifically excludes "any event where the demand for a ransom payment is . . . [n]ot genuine[] or . . . [m]ade in good faith by an entity in response to a specific request by the owner or operator of the information system."[11]

The Proposed Regulation: Key Reporting Obligations

Reporting Obligations of Covered Entities for Covered Cyber Incidents

A Covered Entity that has experienced a Substantial Cyber Incident (*i.e.* a Covered Cyber Incident) must comply with certain deadlines outlined in the Act and the Proposed Regulation.[12] Specifically, the Covered Entity must report the incident to CISA "no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred."[13] The

[9] As noted above, the Proposed Regulation defines "covered cyber incident" to "mean[] a substantial cyber incident experienced by a covered entity." *See* Proposed Regulation § 226.1.

[10] Proposed Regulation § 226.1. The published commentary on the Proposed Rule also provides several specific examples of incidents that would or would not likely be considered Substantial Cyber Incidents.

[11] Proposed Regulation § 226.1.

[12] Proposed Regulation § 226.3(a).

[13] Proposed Regulation § 226.5. There are certain exceptions to when a Covered Entity must submit a Covered Cyber Incident Report or Ransom Payment Report, including where the Covered Entity submits a report to another federal agency that has entered an agreement with CISA. CISA may enter an agreement with another federal agency where it has determined that the other federal agency requires reporting of substantially similar information within

Covered Entity must submit the required reporting form (the "Covered Cyber Incident Report") through "the web-based . . . Reporting Form available on CISA's website or in any other manner and form of reporting approved by the Director [of CISA]."[14]

The Covered Cyber Incident Report that the Covered Entity submits must include basic information regarding the Covered Entity's identity and the critical infrastructure sector(s) to which the Covered Entity considers itself to belong.[15]

In addition, the Covered Cyber Incident Report must disclose specific details about the Covered Cyber Incident, "to the extent such information is available and applicable." The required information includes details about the scope, timing, and impact of the Covered Cyber Incident, the categories of potentially compromised information, any identifying information as to the actor responsible for the Covered Cyber Incident, and the mitigation and response activities that the Covered Entity took.[16]

Reporting Obligations of Covered Entities for Ransom Payments

If a Covered Entity makes a ransom payment in connection with a ransomware attack, it must also submit a report (a "Ransom Payment Report") to CISA.[17] A Covered Entity is required to submit a Ransom Payment Report to CISA "no later than 24 hours after the ransom payment has been disbursed."[18] This obligation exists even where the Covered Entity made the ransom payment in connection with a cyber incident that did not initially require submission of a Covered Cyber Incident Report.[19]

In submitting a Ransom Payment Report, a Covered Entity must provide all of the basic information referred to above in connection with the Covered Cyber Incident Report.[20] In addition, the Covered Entity must provide other information "to the extent . . . available and applicable," including details about how the ransomware attack occurred, any identifying information as to the actor responsible for the ransomware attack, information about the payment of the ransom and associated outcomes, and the mitigation and response activities that the Covered Entity took.[21]

The Proposed Regulation: Data and Records Retention

Categories of Information for Retention

There are also certain data and records retention requirements that apply to Covered Entities that are required to submit a CIRCIA Report. Under the Proposed Regulation, the categories of data that a Covered Entity must retain include:

- Communications with any threat actor, notes taken during any interactions, and relevant information on the communications facilities used;
- Indicators of compromise;
- Relevant log entries;
- Relevant forensic artifacts;
- Network data;
- Data and information that may help identify how a threat actor compromised or potentially compromised an information system;

a substantially similar timeframe as CISA, and that CISA and the other agency have an "information sharing mechanism." *See* Proposed Regulation § 226.4.

14 Proposed Regulation § 226.6.

15 Proposed Regulation § 226.7.

16 Proposed Regulation § 226.8. Covered Entities should consult the Proposed Regulation for a complete list of the information that they will be required to submit as part of a "CIRCIA Report" (which is the generic term for the reports that a Covered Entity may need to submit).

17 Proposed Regulation § 226.3(b).

18 Proposed Regulation § 226.5.

19 Proposed Regulation § 226.3(b).

20 Proposed Regulation §§ 226.7, 226.9.

21 Proposed Regulation § 226.9. In addition to the Covered Cyber Incident Report and Ransom Payment Report, Covered Entities are required to file a report to CISA when they acquire "substantial new or different information" about a Covered Cyber Incident about which they have already submitted a prior report.

— System information that may help identify exploited vulnerabilities;

— Information about exfiltrated data;

— All data or records related to the disbursement or payment of any ransom payment;

— Any forensic or other reports concerning the incident.

Covered Entities must preserve the data and records described above starting from either the date the Covered Entity establishes "a reasonable belief" that a Covered Cyber Incident took place or disburses a ransom payment (whichever occurs earlier). The preservation period continues "[f]or no less than two years from the submission of the most recently required CIRCA Report."[22]

The Proposed Regulation: Mechanisms to Enforce Compliance

Issuance of Requests for Information and Subpoenas, and Penalties for Non-Compliance

The Proposed Regulation also details the processes through which CISA and other government agencies may enforce the applicable regulations. Specifically, CISA may issue a request for information to a Covered Entity "if there is reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment" as required. If the Covered Entity fails to respond to the request for information or provides an inadequate response, CISA may issue a subpoena to seek the information.[23] If the Covered Entity does not comply with the subpoena, CISA may refer the issue to the Attorney General for enforcement of the subpoena through a civil action.[24] Non-compliance with a subpoena may be treated as contempt of court.

In addition, CISA must refer instances of non-compliance "that may warrant suspension and debarment action" to the Suspension and Debarment Official of the Department of Homeland Security.[25] CISA may also refer information to "the cognizant contracting official or the Attorney General for civil or criminal enforcement" where there is non-compliance with requirements that relate to an entity's performance under a federal procurement contract.[26] Individuals who "knowingly and willfully make[] a materially false or fraudulent statement or representation" in a CIRCIA Report or in related circumstances are subject to criminal liability under 18 U.S.C. § 1001.[27]

Incentives to File CIRCIA Reports and Respond to Requests for Information

Under the Proposed Regulation, information that Covered Entities submit through a CIRCIA Report or in response to a request for information is subject to certain protections. For example, information that the Covered Entity submits is not subject to disclosure under the Freedom of Information Act. In addition, the Covered Entity "does not waive any applicable privilege or protection provided by law" when it submits information in a CIRCIA Report or in response to a request for information.[28]

When Covered Entities submit information as part of a CIRCIA Report or in response to a request for information, restrictions apply that limit other government entities' abilities to use that information to regulate and bring enforcement proceedings against the Covered Entity. Likewise, there are restrictions on when such information may be used as the basis for litigation, introduced as evidence in litigation, or subject to discovery. The Proposed Regulation limits the uses that the federal government may make of the information that a Covered Entity submits. Importantly, all of the foregoing protections do not apply to information that the Covered Entity submits in response to a subpoena, a civil enforcement action regarding a subpoena, or certain other disciplinary measures.

22 Proposed Regulation § 226.13.
23 Proposed Regulation § 226.14.
24 Proposed Regulation § 226.15.
25 Proposed Regulation § 226.16.
26 Proposed Regulation § 226.17.
27 Proposed Regulation § 226.20.
28 Proposed Regulation § 226.18.

Key Takeaways

As noted above, although the Act did provide the general contours of the reporting requirements for Covered Entities, the Proposed Regulation provides important new details regarding the scope of the Act's requirements. Defining Covered Entities to include all entities in critical infrastructure sectors that either exceed the relevant small business threshold or otherwise satisfy sector-based criteria means that the Act's 72-hour and 24-hour reporting obligations will apply to a wide range of entities, including some entities that may not have previously expected to be subject to the Act. Further, the two-year data and records preservation period may require Covered Entities to modify retention policies and practices to ensure compliance with these obligations. Entities that qualify as Covered Entities under the Proposed Regulation should assess whether to engage in the rulemaking process by providing public comment, and should otherwise assess whether their policies, procedures, and systems must be updated to ensure compliance with the final rule when it takes effect.

Comments on the Proposed Regulation are due by June 3, 2024 and we expect the final regulation will be published no later than October 2025.

…

CLEARY GOTTLIEB