SheppardMullin

CISA Cyber Incident Reporting for Critical Infrastructure Will Significantly Impact Government Contractors, Suppliers, and Service Providers

By: Townsend Bourne

The Cybersecurity and Infrastructure Security Agency ("CISA") recently released its new Proposed Rule pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), which was published in the Federal Register on April 4, 2024 and is **open for public comment through June 3, 2024**. The Proposed Rule will be published in Part 6 of the Code of Federal Regulations, in a new Section 226, as part of the Department of Homeland Security's regulations on Domestic Security.

We read the 400-plus page document so you don't have to, and outline the "Who, What, When, Where, Why & How" of CISA reporting for critical infrastructure below.

Who is "Covered"?

CISA's new Proposed Rule will require cyber incident reporting for covered entities in all 16 critical infrastructure sectors. Entities that meet certain threshold criteria – regardless of size – are covered by the rule. Businesses that are small per the Small Business Administration's size standards not otherwise covered by the threshold criteria are excluded from the definition of "covered entities." Large entities in each of the critical infrastructure sectors are covered by the rule regardless of whether they meet the threshold criteria.

The Proposed Rule includes threshold criteria for entities in 13 of the 16 critical infrastructure sectors. These are listed below – threshold criteria for sectors of key interest to government contractors are set forth in more detail.

1. **Chemical Sector** – any entity that owns or operates a covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards
2. **Communications Sector** – any entity that provides communications services by wire or radio communications to the public, business, or government
   - *This will apply to telecommunications carriers, and wireless and internet service providers to the Federal government.*
3. **Critical Manufacturing Sector** – any entity that owns or has business operations that engage in one or more of four key manufacturing industries that make up this sector

4. **Defense Industrial Base Sector** – any entity that is a contractor or subcontractor required to report cyber incidents to DoD per DFARS 252.204-7012
   - This pulls in any DoD contractor or subcontractor, regardless of size, that handles Controlled Unclassified Information ("CUI").
5. **Emergency Services Sector** – any entity that provides one or more of certain emergency services or functions to a population equal to or greater than 50,000 individuals
6. **Energy Sector** – any entity that is required to report cybersecurity incidents under NERC's CIP Reliability Standards or file an Electric Emergency Incident and Disturbance Report OE-417 form, or any successor form, to the Department of Energy
7. **Financial Services Sector** – three categories of entities that have the potential to impact the economic security of the nation
8. **Government Facilities Sector** – entities that meet one of three criteria relating to state, local, tribal, and territorial government; education; or election processes
9. **Healthcare and Public Health Sector** – any entity that meets certain criteria relating to patient services, and certain drug and device manufacturers
10. **Information Technology Sector** – any entity that meets one or more of four criteria, including any entity that (a) knowingly provides IT hardware, software, systems, or services to the Federal government; (b) has developed and continues to sell, license, or maintain any software that meets the definition of "critical software" as defined by NIST; (c) is an OEM, vendor, or integrator of OT hardware or software components; or (d) performs functions related to domain name operations.
    - *This pulls in all government IT product and services providers as well as companies that develop or resell "critical software" as defined per Executive Order 14028.*
11. **Nuclear Reactors, Materials, and Waste Sector** – any entity that owns or operates a commercial nuclear power reactor or fuel cycle facility
12. **Transportation Systems Sector** – certain entities that meet criteria relating to non-maritime transportation, or own or operate a vessel, facility, or outer continental shelf facility
13. **Water and Wastewater Systems Sector** – certain owners and operators of a Community Water System or a Publicly Owned Treatment Works ("POTWs")

For entities in the other three sectors, **Commercial Facilities Sector, Dams Sector,** and **Food and Agriculture Sector,** CISA is not proposing sector-based threshold criteria, but large businesses in these sectors will be considered "covered entities."

It is estimated the Proposed Rule will impact over 300,000 entities.

What needs to be reported?

The Proposed Rule will require covered entities to report "substantial cyber incidents" in addition to ransom payments, and to provide supplemental reports when new or material information is identified. The proposed definition for a "substantial cyber incident" focuses on outcomes rather than the cause of an incident, and 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 the safety and resiliency of a covered entity's operational systems and processes;
3. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or
4. Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.

Note items #1 and #2 above include a further qualifier of "substantial" or "serious" loss or impact, a somewhat subjective standard that companies will need to examine. For #3, while there is no additional express qualifier, CISA says it "believes it is appropriate to read into the prong some level of significance." However, for #4, due to the "seriousness of unauthorized access through a third party," such as a cloud service provider ("CSP") or managed services provider ("MSP"), CISA takes a different view and does not further qualify the need to report. Where the cause is unknown, an entity should report if there is a "reasonable belief" that unauthorized access was caused by a third-party provider or supply chain compromise.

Unlike the current DoD cyber incident reporting provision and others currently in effect (which require reporting for "potential" effects), CISA will only require reports where the incident ***actually results in one or more of the above impacts***.

The Proposed Rule contemplates certain exceptions to the reporting requirement, including when a covered entity reports "substantially similar information in a substantially similar timeframe" to another agency and CISA has a CIRCIA Agreement in place with that agency. We expect the DoD to be at the very top of this list where many DoD contractors already have an obligation to report cyber incidents within 72 hours.

Note the Proposed Rule explicitly allows a third party (such as an Incident Response ("IR") company, insurance or other service provider, or law firm) to submit reports on behalf of a covered entity, a practice that already occurs in the cyber reporting world and is now explicitly acknowledged here by CISA. The third party will have to attest that it has consent to submit the report. Separately, CISA continues to encourage voluntary reporting for incidents that may not be covered under the new rules.

When does the reporting period begin?

Covered entities will be required to report covered cyber incidents within 72 hours after having a "reasonable belief" that a covered cyber incident has occurred and report ransom payments within 24 hours of the payment being made. As noted above, CISA seems to be trying to take a reasonable approach here, further stating that a reasonable belief "is subjective and will depend on the specific factual circumstances related to the particular incident" and it "does not expect a covered entity to have reached a 'reasonable belief' that a covered cyber incident occurred immediately upon occurrence of the incident…"

Supplemental reports are to be provided "promptly" where the covered entity obtains "substantial new or different information." CISA says this means where additional information responsive to a data field in the CIRCIA Report is available or it becomes known that information included in a previously submitted report is materially incorrect or incomplete. This approach seems to be much more workable than that currently contemplated in the FAR Council's proposed rule for *Cyber Threat and Incident Reporting and Information Sharing*, which would require covered contractors to provide updates every 72 hours regardless of whether new key or material information is available.

Where might I end up if I fail to follow the rule?

CISA discusses several enforcement mechanisms for covered entities that fail to report in accordance with the rule. These include (1) issuance of an RFI for more information; (2) issuance of a subpoena; (3) referral to the Attorney General for potential civil court action; and (4) initiation of suspension and debarment procedures. And, false or fraudulent statements in a CIRCIA Report or other response to CISA could result in penalties under 18 U.S.C. § 1001, a criminal statute.

The Proposed Rule also includes a data preservation component to require preservation of data relevant to a covered entity's reporting (such as communications with the threat actor; indicators of compromise; log entries and forensic images; etc.) for two years from submission of the CIRCIA Report or supplemental report.

Why are we getting these new regulations?

The proposed regulations are being promulgated under CIRCIA, an act passed in 2022 to address cyber threats posed to U.S. critical infrastructure, which may impact national security, economic security, and public health and safety.

How do I submit comments?

Comments may be submitted through June 3, 2024 through the Federal eRulemaking Portal available at http://www.regulations.gov (Docket No. CISA-2022-0010). CISA is interested in comments on all aspects of the Proposed Rule.

For More Information, Please Contact:

Townsend Bourne
Partner | Washington, D.C.
202.747.2184
tbourne@sheppardmullin.com