Report on CISA-2022-0010

(Cyber Incident Reporting For Critical Infrastructure Rule)

Prepared by

Patrick W. Seibert, CISSP, Cysa+

Executive Summary:

The Cyber Incident Reporting for Critical Infrastructure Act of 2022, signed into law March 15, 2022 requires covered entities to report cyber incidents, ransom payments, and any significant cybersecurity information to the Cybersecurity and Infrastructure Security Agency (CISA). The CIRCIA NPRM is a 447 page document outlining public participation, an executive summary, background and purpose, discussion of the proposed rule, statutory and regulatory analysis, and proposed regulatory Text. This Notice of Proposed Rule Making discusses in detail the requirements outlined and open for comment. The proposed rule is being published on 4/4/2024, and public comment will end on 6/1/2024.

This document and presentation prepared today is an attempt to distill this information into a concise format for Executives while Legal and Compliance make comment and review the rule in it’s entirety. The proposed rule aims to define reporting requirements for covered entities, establish deadlines, reporting formats, and procedures for submission. It also addresses enforcement mechanisms, data preservation, liability protection, and privacy concerns related to the CIRCIA Reports. Additionally, the proposal includes provisions for penalties for fraudulent statements and a severability clause.

At a high level the CIRCIA states (pp 341 of 2024-06526)

* A covered entity that experiences a covered cyber incident must report that incident to CISA no later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.
* A covered entity that makes a ransom payment, or has another entity make a ransom payment on its behalf, as a result of a ransomware attack against the covered entity must report that payment to CISA no later than 24 hours after the ransom payment has been disbursed.
* A covered entity that experiences a covered cyber incident and makes a ransom payment, or has another entity make a ransom payment on its behalf, that is related to the covered cyber incident may report both events to CISA in a joint report no later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.
* A covered entity must promptly submit a supplemental report about a previously reported covered cyber incident if substantial new or different information becomes available.
* A covered entity must submit a supplemental report if the covered entity makes a Ransom payment, or has another entity make a ransom payment on its behalf, that relates to a covered cyber incident that was previously reported. The covered entity must submit the Supplemental report to CISA no later than 24 hours after the ransom payment has been disbursed.

Who are covered entities?

Covered entities, as defined by Presidential Policy Directive 21 as "critical infrastructure sector", and further designated as a part of critical infrastructure.  If an entity exceed the "small business" threshold set by SBA.

CISA interprets the word “entity” to be a broad term, generally including any person, partnership, business, association, corporation, or other organization (whether for-profit, not-for-profit, nonprofit, or government) regardless of governance model that has legal standing and is uniquely identifiable from other entities.

 1**. Chemical Sector** - Any entity in a critical infrastructure sector that owns or operates a covered chemical facility subject to the CFATS.

 2.  **Communication Sector** - Any entity that provides communications services by wire or radio communications, as defined in 47 U.S.C. 153(40), 153(59) to the public, business, or government.

3. **Critical Manufacturing** -  such as Primary Metal Manufacturing (NAICS Subsector 331); Machinery Manufacturing (NAICS Subsector 333); Electrical Equipment, Appliance, and Component Manufacturing (NAICS Subsector 335); and Transportation Equipment Manufacturing (NAICS Subsector 336).

4**. Defense Industrial Base Sector** - Any entity that is a contractor or subcontractor required to report cyber incidents to DOD pursuant to the definitions and requirements of the DFARS Safeguarding Covered Defense Information and Cyber Incident Reporting clause located at 48 CFR 252.204-7012

5. **Emergency Services Sector** - Any entity that provides one or more of five listed emergency services or functions to a population equal to or greater than 50,000 individuals. These five disciplines—law enforcement, fire and rescue services, emergency medical services, emergency management, and public works that contribute to public health and safety—and the types of entities that provide these services are described in the 2015 Emergency Services SSP.

 6.  **Energy Sector** - Any entity that is required to report cybersecurity incidents under NERC’s CIP Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report OE-417 form, or any successor form, to DOE.

7.  **Financial Services Sector** - Any Entity (1) all of the Financial Services Sector entities that are required to report cybersecurity incidents to their respective primary Federal regulator (e.g., national banks; savings and loans holding companies; FICUs), (2) Financial Services Sector entities for whom the primary Federal regulator has indicated an intention to require cybersecurity incident reporting (e.g., futures commission merchants; security-based swap data repositories), and (3) Financial Services Sector entities encouraged or expected to report cybersecurity incidents to their primary Federal regulator pursuant to an Advisory Bulletin (e.g., Fannie Mae and Freddie Mac; money services businesses).

 8.  **Government Facilities Sector** - Any SLTT Government entity for a jurisdiction with a population equal to or greater than 50,000 individuals or any entity that qualifies as either (A) a local educational agency (LEA), educational service agency (ESA), or state educational agency (SEA), as defined under 20 U.S.C. 7801, with a student population of 1,000 or more students; or (B) an institute of higher education  (IHE) that receives funding under Title IV of the Higher Education Act. Third, CISA is proposing to include in the description of covered entity any entity that manufactures, sells, or provides managed service for information and communications technology specifically used to support election processes or report and display results on behalf of SLTT governments, including but not limited to voter registration databases; voting systems; and information and communication technologies (ICT) used to report, display, validate, or finalize election results. As discussed in greater detail in Section IV.D.iii in this document, CISA is proposing to except from required reporting Federal agencies already required to report incidents to CISA under FISMA, such that these sector-based criteria are focused on SLTT and private sector members of the Government Facilities sector.

9**.  Healthcare and Public Health Sector** - Entities within the Healthcare and Public Health Sector, along with Federal and SLTT Departments of Health and similar government entities that are part of the Government Facilities Sector, are essential to the maintenance of the public health of the nation, providing goods and services that are integral to maintaining local, national, and global health security. Entities within the sector provide various services, to include direct patient care, medical equipment and materials, laboratory support, health IT, health plans, and mass fatality management services.  Any entity that owns or operates (1) a hospital, as defined by 42 U.S.C. 1395x(e), with 100 or more beds, or (2) a critical access hospital, as defined by 42 U.S.C. 1395x(mm)(1), reporting from manufacturers of drugs listed in Appendix A of the report Essential Medicines Supply Chain and Manufacturing Resilience Assessment, Sponsored by the U.S. Department of Health and Human Services (HHS) Administration for Strategic Preparedness and Response (ASPR). Required reporting from manufacturers of Class II (moderate risk) and Class III (high risk) devices, as defined in 21 U.S.C. 360c.  

10.  **Information Technology Sector** - Any entity that meets one or more of four proposed Information Technology (IT) Sector sector-based criteria. First, CISA proposes including within the description of covered entity any entity that knowingly provides IT hardware, software, systems, or services to the Federal government. Second, CISA proposes including within the description of covered entity any entity that has developed and continues to sell, license, or maintain any software that meets the definition of “critical software” as that term was defined by NIST pursuant to Executive Order 14028 – Improving the Nation’s Cybersecurity (May 12, 2021). Third, CISA proposes to include within the description of covered entity, any entity that is an original equipment manufacturer (OEM), vendor, or integrator of OT hardware or software components. Fourth, CISA proposes to include within the description of covered entity any entity that performs functions related to domain name operations.

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** - Owners and operators of various non-maritime transportation system infrastructure, such as freight railroad, public transportation and passenger railroads (PTPR), pipeline facilities and systems, over-the-road bus (OTRB) operations, passenger and all-cargo aircraft, indirect air carriers, airports, and Certified Cargo Screening Facilities. Any entity that owns or operates a vessel, facility, or outer continental shelf facility subject to 33 CFR parts 104, 105, or 106. Those entities identified by TSA as requiring cyber incident reporting and (in some cases) enhanced cybersecurity measures for primarily the same reasons TSA relied upon in determining that these entities warranted such requirements. Reporting from owners and operators of freight railroad carriers identified under 49 CFR 1580.1(a)(1), (4), and (5) and PTPR identified in 49 CFR 1582.1. Reporting from Owners and operators of the critical pipeline facilities and systems, as identified in in 49 CFR part 1586 in TSA’s rulemaking, Surface Cybersecurity Risk Management. Any entity that is required to implement a TSA-approved security program under 49 CFR parts 1542, 1544, 1548, and 1549. Entities that own or operate assets subject to MTSA. MTSA, which is designed to protect the nation’s ports and waterways from a terrorist attack, requires certain vessels, facilities, and outer continental shelf facilities to perform various security-related activities.

 13. **Water and Wastewater Systems Sector** - Any entity that owns or operates a Community Water System, as defined in 42 U.S.C. 300f(15), or a Publicly Owned Treatment Works (POTWs), as defined in 40 CFR 403.3(q), that serve more than 3,300 people.

When will this rule be in effect?

The rule opens for public comment on 4/4/2024. 60 days after that the rule goes into review and Final Publication 18 months later. The reporting is expected to start in 2026.

What is covered in this rule, what is it?

CISA proposes the term 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 either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.  Including any cyber incident regardless of cause, including, but not limited to, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

6 U.S.C. 681b(c)(2)(A) states that the types of substantial cyber incidents that constitute covered cyber incidents must, “at a minimum, require the occurrence of (i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes; (ii) a disruption of business or industrial operations, including due to a denial-of-service attack, ransomware attack, or exploitation of a zero day vulnerability, against (I) an information system or network; or (II) an operational technology system or process; or (iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.”

It is from the above language that CISA has the directive to submit and approve the rule discussed herein.

When evaluating reporting requirements, it's necessary to keep in mind that only 1 of the 4 prongs presented in the rule need be met to trigger a requirement to report.   
The four prongs are:  
1. Substantial loss in the confidentiality, availability, or integrity of a covered entities Information Systems or Network.  
2. Serious impact on safety and resiliency of operational systems and processes.  (Does include OT, though not exclusively).  
3. Disruption of ability to Engage in Business or Industrial Operations.  
4. Unauthorized Access facilitated through or caused by a: 1.) Compromised CSP, MSP, or other Third-party data hosting provider, or 2.) supply chain compromise.

As stated above this rule also covers OT technologies in an environment so there needs to be especial attention paid to things such as environmental controls, security cameras, ancillary devices, door locks, and other lesser thought of IoT style devices that are now being integrated into networks. They are often overlooked and pose significant threat to environments. For further information on this seek out your security analysts.

It is also important to note that unauthorized access resultant from Third Party or CSP or Supply chain providers fall under prong 3 of the Significant Cybersecurity Events qualifier and must be reported per the CIRCIA requirements.

Under CIRCIA extortion by threat of attack is a reportable instance if payment is made and the threat is thought to be in good faith. This would trigger the 24 hour rule for reporting as if per Ransomware.

There are few notable exceptions to the rule for reporting:

* Events which were mitigated at the boundary of the network without meeting the threshold for a significant event, exploitation occurring, or loss of information required to meet threshold need not be reported.
* Events that occur within environments that are caused by known issues and or were authorized need not be reported, otherwise at the suspicion and reasonable belief of an incident, the covered entity must report to CISA.
* Exceptions to reporting are Federal or SLTT Government entities and authorized (third party or internal) parties conducting operations which disrupt or cause incident. (Red team, pentesting, internal development.)

Why is this rule being written, and why do we care?

On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law. See 6 U.S.C. 681 – 681g; Pub. L. 117-103, as amended by Pub. L. 117-263 (Dec. 23, 2022). CIRCIA requires covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report.  
  
 CIRCIA provides a variety of mechanisms for CISA to use if CISA believes that a covered entity has failed to submit a CIRCIA Report in accordance with CIRCIA regulatory requirements. See 6 U.S.C. 681d. The potential approaches CISA has to address noncompliance include issuance of an RFI (6 U.S.C. 681d(b)), issuance of a subpoena (6 U.S.C. 681d(c)(1)), referral to the Attorney General to bring a civil action to enforce the subpoena and/or pursue a potential contempt of court (6 U.S.C. 681d(c)(2)), and other enforcement mechanisms to include potential acquisition penalties, suspension, and debarment (6 U.S.C. 681b(c)(8)(B)(ii)). Section 681b(c)(8)(B) of title 6, United States Code, requires CISA to include in the final rule procedures to carry out these enforcement provisions.   
  
 Failure to report can results in being held in contempt of court, Proposed § 226.16 would require the Director to refer all circumstances concerning a covered entity’s noncompliance that may warrant suspension and debarment action to the DHS Suspension and Debarment Official. Suspension and debarment are meant to help protect the Federal government from fraud, waste, and abuse by supporting the Federal government’s ability to avoid doing business with non-responsible contractors. CISA would refer potential violations of this proposed provision to DOJ, and DOJ would determine whether to prosecute violators of 18 U.S.C. 1001.  
   
  The proposed rule separates these protections into two broad categories with the specific protections afforded to

(1) CIRCIA Reports or information submitted in CIRCIA Reports and responses to RFIs and

(2) reporting entities and persons detailed under each. Specifically, CISA proposes under the first category, Treatment of Information, the following protections which are consistent with 6 U.S.C. 681e: (a) Designation as Commercial, Financial, and Proprietary Information, (b) Exemption from Disclosure under FOIA, (c) No Waiver of Privilege or Protection Provided by Law, and (d) an Ex Parte Communications Waiver. Under Restrictions on Use, CISA proposes the following restrictions consistent with 6 U.S.C. 681e: (a) Prohibition on Use in Regulatory Actions, (b) Liability Protection and Evidentiary and Discovery Bar for CIRCIA Reports, and (c) Authorized Uses.

How is reporting supposed to occur?

CISA is proposing that a covered entity must submit CIRCIA Reports through the web-based CIRCIA Incident Reporting Form available on CISA’s website or in any other manner approved by the Director.  
  
**Expected Reporting Information**:  
**All CIRCIA reports**:  
1. **Report Type** -  This will help identify if a report is a Covered Cyber Incident Report, a Ransom Payment Report, a Joint Covered Cyber Incident and Ransom Payment Report, or a Supplemental Report.  
  
2**. Identity of the Covered Entity** - This must include, as applicable, the State of incorporation or formation of the covered entity, trade names, legal names, or other identifiers. Other types of information that CISA intends on requesting in this section of the form include the entity type (e.g., Federal, State, local, Territorial, Tribal, ISAC, private sector); physical address; organization’s website; any internal incident tracking number used by the entity for the reported event (if one exists); any applicable business numerical identifiers, such as a NAICS code, General Services Administration-Issued Unique Entity Identifier (GSA-UEI), Dun & Bradstreet Data Universal Numbering System (D-U-N-S) Number, Tax ID Number, EPA Facility ID number; Chemical Security Assessment Tool (CSAT) ID Number, or MTSA Facility ID Number; the name of the covered entity’s parent corporation or organization, if applicable; and the critical infrastructure sector or sectors of which the covered entity considers itself a part.  
  
3. **Contact Information** - Name, phone number, email, and title of the reporting party and, if different, the point of contact for the covered entity. Or the name, phone number, email address, and title of the covered entity’s registered agent, if that individual is different than the identified point of contact. Or in cases where a third party is submitting a report on behalf of a covered entity, the aforementioned contact information must be provided for both the third-party submitter and the covered entity point of contact. Additionally and optionally: contact information for a 24/7 point of contact could be provided to better enable incident response support and emergency follow-up engagement.  
  
4. **When Applicable, Third Party Authorization to Submit** - a third party that submits a report on behalf of a covered entity to include in the submission an attestation that it has been expressly authorized by the covered entity to submit the report.  
  
**Description of the Covered Incident (Covered Cyber Incident Report Specific)** - a narrative description of the incident or specific aspects of the incident along with a series of questions containing radio buttons, drop-down menus, or limited data fields (e.g., dates) to ensure the provision of certain information.   
1.) The name and a description of the impacted systems, networks, and/or devices, to include technical details and physical locations of the impacted systems, networks, and/or devices. CISA also would like to know if any of the impacted systems, networks, and/or devices contain or process information created by or for any element of the Intelligence Community or contain information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y).   
2.) whether the incident involved any unauthorized access (whether or not the access involves an attributed or unattributed cyber intrusion), whether there were any informational impacts, or whether any information was compromised. If the answer to any of those questions is “yes,” CISA proposes requiring the covered entity to answer a small number of follow-up questions to elicit additional details. CISA also intends to request information regarding what network location(s) the activity was observed in. While the statutorily enumerated element incorporates the “substantial loss” standard from the first prong of the definition of substantial cyber incident, CISA is proposing to require covered entities to describe any unauthorized access once an incident meets the reportable threshold so that CISA and other Federal agencies can have a broader understanding of potential impacts to the CIA of information systems, networks, or the information therein. CISA believes the “disruption of business or industrial operations” portion of this statutorily enumerated element is sufficiently addressed by the fourth statutorily enumerated element, discussed below.   
3.) The date the covered cyber incident was detected, the date the covered cyber incident began (if known), the date the covered cyber incident was fully mitigated and resolved (if it has been), and the timeline of compromised system communications with other systems. For incidents involving unauthorized access, CISA also proposes asking about the suspected duration of the unauthorized access prior to detection and reporting. While CISA is proposing to ask for more details than just the incident date range (i.e., the beginning and end of the incident), understanding the key timeline of events that comprised the incident is key to enhancing the Federal government’s understanding of the incident as a whole.   
4.) Various questions to understand both the level of impact and specific impacts, such as whether any known or suspected physical or informational impacts occurred. Questions related to the nature of the impact, i.e., was the system, network, device, or data accessed, manipulated, exfiltrated, destroyed, or rendered unavailable.  Information on impacts of the incident beyond simply the operations of the covered entity. Also questions that will help CISA assess the economic impacts of the incident and the potential impacts of the incident on public health and safety, national security, economic security, and any of the NCFs.  
5.) Include in its Covered Cyber Incident Report the “category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

a.)Require the submission of information on the vulnerabilities exploited, including but not limited to the specific products or technologies and versions in which the vulnerabilities were found.

b.) Require the submission of information on the covered entity’s security defenses, including but not limited to any controls or measures that resulted in detection or mitigation of the incident. As part of this, CISA is likely to ask what, if any, security controls or control families (e.g., NIST Special Pub 800-171 controls; NIST Cybersecurity Framework measures; CISA Cybersecurity Performance Goal activities) the covered entity had in place on the compromised system, and, to the extent known, which controls or control families failed, were insufficient, or not implemented that may have been a factor in this incident. As well as questions about what, if any, detection methods were utilized to discover the incident, and if the covered entity has identified the point of compromise / initially infected device(s).

c.) Require information on the type of incident (e.g., denial-of-service; ransomware attack; multi-factor authentication interception); the TTPs used to cause the incident, to include any TTPs that were used to gain initial access to the covered entity’s system; indicators of compromise observed in connection with the covered cyber incident; and a description and copy or sample of any malicious software the covered entity believes is connected with the covered cyber incident. what, if any, attack vectors did the covered entity identify; to the covered entity’s knowledge, were any advanced persistent threat actors involved; were any malicious software, malicious scripts, or other indicators of compromise found, and, if so, what specific variants or strains were used. A description of any malware samples or indicators of compromise observed or captured by the covered entity,   and provide indicators of compromise identified as well as copies of any malware samples related to the covered cyber incident that the covered entity has in its possession.

d.) In cases where the covered cyber incident involves a ransomware attack but the covered entity did not make a ransom payment,  CISA intends to ask specific questions related to ransomware attack-specific TTPs, such as information on the ransom payment demand and instructions, that a covered entity would otherwise have been required to provide in a Ransom Payment Report were one required.

6.) Include in this section questions seeking any attribution-related information the covered entity may possess.

7.) Questions regarding the mitigation and response activities a covered entity is taking or has taken in response to a covered cyber incident. What mitigation measures the covered entity had in place, what responsive actions the covered entity has taken, what phase of incident response (e.g., detection, analysis, containment, eradication, recovery, and post-incident activity) the covered entity is currently in, and what is the covered entity’s assessment of the efficacy of those mitigation and response activities. Engagement with law enforcement agencies, if the covered entity reached out to another entity for mitigation or response assistance, and, if so, to whom.  
  
**Ransom Payment Report Specific Conten**t -   
a.) Description of the Ransomware Attack - Same as the Covered Cyber Incident.  
b.) Vulnerabilities, Security Defenses, and TTPs.  
c.) Information Related to the Identification of the Perpetrators of the Attack.  
d.) Information on the Ransom Payment.  
e.) Results of Ransom Payment Report information regarding what occurred as the result of the covered entity making the ransom payment.  
f.) Additional Data or Information

i.) Whether the covered entity requested assistance from another entity in responding to the ransomware attack or making the ransom payment and, if so, the identity of such entity or entities.

ii.)  Provide information on any engagement the covered entity has had with any law enforcement agency related to the ransom payment or underlying ransomware attack.

iii.) Any other data or information required by the web-based CIRCIA Incident Reporting Form or any other authorized manner and form of reporting.

**Supplemental Report Specific Content -**   
  
a.) Given that the purpose of a Supplemental Report is to provide CISA with additional or updated information regarding a previously reported covered cyber incident, the content required in a Supplemental Report generally will be a subset of the content required to be reported and optional content in a Covered Cyber Incident Report and/or Ransom Payment Report, tailored to the reason for the submission of the Supplemental Report and the information previously provided by the covered entity in the previously submitted CIRCIA Report.  
  
**Content in the DHS-Developed Model Reporting Form Not Included in Proposed CIRCIA Reporting Forms**  
  
a.)  A section where a reporting entity is afforded the opportunity to indicate if it believes one or more FOIA exemptions should apply to the information being submitted. (CIRCIA Reports are Exempt from FOIA.)  
b.)  Questions regarding whether the reporting entity has notified any governmental entities (e.g., regulators or other departments or agencies, law enforcement, Congress) and, in the case of consumer data breaches or privacy breaches, if the reporting entity has notified impacted individuals and provided them with guidance on how to take steps to protect themselves during an ongoing incident. CISA has no requirement for this beyond LEA.  There will be a field for optional disclosure.  
  
Upon an incident being resolved CISA is requesting that a supplemental report be filed notifying them.