CHIME Cheat Sheet – April 1, 2024

Cybersecurity and Infrastructure Security Agency (CISA) Proposed Rule:
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements
Brief Overview & Impact on the Healthcare and Public Health (HPH) Sector

On March 27, 2024, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released the proposed regulation "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements." Comments are due June 4, or 60 days after publication in the *Federal Register*. You can find CISA's press release on the proposal here.

Additionally, you can find CHIME and AEHIS's response to CISA's 2022 Request for Information (RFI) on the proposed rulemaking here. The final rule is estimated to be released around September of 2025.

Background

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires CISA to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities. CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements. CISA is seeking public comments on all of the proposed definitions, as well as responses to specific questions, listed on pages 111 – 113 of the proposed rule.

CISA is aware that the term covered entity is also a defined term in the HIPAA regulations. Whenever the term "covered entity" is used in this proposed rule, it is referring to the statutory term in CIRCIA and/or the proposed definition of covered entity in CIRCIA, and not to entities that meet the existing HIPAA regulatory definition of covered entity or any other existing definition of the term covered entity.

Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident – Definitions

CISA is proposing to define "cyber incident" to mean an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system.

CIRCIA requires CISA to include within the proposed rule a definition for the term "covered cyber incident." Given that the law requires covered entities to report only those cyber incidents that qualify as "covered cyber incidents" to CISA – this definition is essential for triggering the reporting requirement. CISA is proposing to define the term "covered cyber incident" to mean a substantial cyber incident experienced by a covered entity. CISA is proposing a definition for "substantial cyber incident" – such that a covered cyber incident will include all substantial cyber incidents experienced by a covered entity. Under this approach, a covered entity simply needs to determine if a cyber incident is a substantial cyber incident for it to be reported.

In other words, CISA is proposing to define a covered cyber incident as a substantial cyber incident experienced by a covered entity. The term substantial cyber incident is essential to the CIRCIA regulation as it identifies the types of incidents, that when experienced by a covered entity, must be reported to CISA.

CISA is proposing that the term "substantial cyber incident" means 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) disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or
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.

CISA is further proposing that a substantial cyber incident resulting in one of the listed impacts include 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.

Additionally, CISA is proposing that the term substantial cyber incident does not include: a) any lawfully authorized activity of a United States Government entity or state, local, tribal, and territorial (SLTT) Government entity, including activities undertaken pursuant to a warrant or other judicial process; b) any 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; or c) the threat of disruption as extortion, (i.e., meeting the definition of "ransomware attack").[1]

Ransom payment is a key term in the proposed regulation as CIRCIA requires that covered entities report ransom payments to CISA within 24 hours of the payment being made. Notably, this exclusion clarifies that the threat of disruption of a system to extort a ransom payment that does not result in the actual disruption of a system is an "imminent," but not "actual," event, and is therefore not required to be reported as a covered cyber incident. Only such a threat where no ransom payment is made and the disruption never materializes into a substantial cyber incident would remain excluded from mandatory reporting.

The proposed **definition of "substantial cyber incident"** contains the following elements:

1) a set of four threshold impacts which, if one or more occur as the result of a cyber incident, would qualify that cyber incident as a substantial cyber incident;
2) an explicit acknowledgment that substantial cyber incidents can be caused through compromises of third-party service providers or supply chains, as well as various techniques and methods; and
3) three separate types of incidents that, even if they were to meet the other criteria contained within the substantial cyber incident definition, would be excluded from treatment as a substantial cyber incident.

Minimum Requirements for a Cyber Incident to be a Substantial Cyber Incident

CISA is proposing to use existing statutory "minimum requirements"[2] to create what they assert is a sufficiently high threshold to prevent overreporting by making it clear that routine or minor cyber incidents do not need to be reported. Thus, they are proposing to use these requirements as the basis for the first part of the definition of substantial cyber incident, with minor modifications for clarity and for greater consistency with the Cyber Incident Reporting Council (CIRC) Model Definition of a reportable cyber incident.

[1] 6 U.S.C. 650
[2] Enumerated in 6 U.S.C. 681b(c)(2)(A)

Ultimately, CISA is proposing four types of impacts that, if experienced by a covered entity as a result of a cyber incident, would result in the incident being classified as a substantial cyber incident and therefore reportable under the CIRCIA regulation. **Each of these impact types is described in its own prong of the substantial cyber incident definition.**

- **Impact 1:** Substantial Loss of Confidentiality, Integrity, or Availability
- **Impact 2:** Serious Impact on Safety and Resiliency of Operational Systems and Processes
- **Impact 3:** Disruption of Ability to Engage in Business or Industrial Operations
- **Impact 4:** Unauthorized Access Facilitated Through or Caused by a: 1) Compromise of a Cloud Service Provider (CSP), Managed Service Provider, or Other Third-Party Data Hosting Provider, or 2) Supply Chain Compromise

Guidance for Assessing Whether an Impact Threshold is Met

When evaluating whether a cyber incident meets one of the four proposed impact thresholds that would qualify it as a substantial cyber incident, a covered entity should keep in mind several principles. First, an incident needs to meet only one of the four prongs, not all four of the prongs, for it to be a substantial cyber incident. For an incident to be a substantial cyber incident that meets the threshold of a covered cyber incident it only has to meet one of the enumerated criteria listed in the proposed rule, not all the enumerated criteria. This approach is also consistent with the CIRC Model Definition, with which CISA attempted to align to the extent practicable.

For an incident to qualify as a substantial cyber incident, CISA interprets CIRCIA to require the incident to "actually result" in one or more of the four impacts described. A number of other cyber incident reporting regulations do not require actual impacts for an incident to have to be reported; rather, some require reporting if an incident results in imminent or potential harm, or identification of a vulnerability. CISA believes that statute[3] limits reportable incidents under CIRCIA to those that have actually resulted in at least one of the impacts described. **Therefore, if a cyber incident jeopardizes an entity or puts the entity at imminent risk of threshold impacts but does not actually result in any of the impacts included in the proposed definition, the cyber incident does not meet the definition of a substantial cyber incident.**

CISA has elected not to limit the definition of substantial cyber incident to impacts to specific types of systems, networks, or technologies. CISA is proposing that if a cyber incident impacting a system, network, or technology that an entity may not believe is critical nonetheless results in actual impacts that meet the level of one or more of the threshold impact prongs, then the incident should be reported to CISA.

In addition to helping ensure CISA receives reports on substantial cyber incidents even if they were perpetrated against a system, network, or technology deemed non-critical by the impacted covered entity, this approach also has the benefit of alleviating the need for a covered entity to proactively determine which systems, networks, or technologies it believes are "critical" and instead focus solely on the actual impacts of an incident as the primary determining factor as to whether a cyber incident is a reportable substantial cyber incident. Thus, CISA is proposing to include, but not specifically distinguish, cyber incidents with impacts to Operational Technology (OT). While it may be the case that cyber incidents affecting OT are more likely to meet the impact thresholds in the definition of substantial cyber incident, CISA did not want to artificially scope out cyber incidents that primarily impact business systems, yet result in many of the same type of impacts that could result from a cyber incident affecting OT.

CISA is aware that in some cases, a covered entity will not know for certain the cause of the incident within the first few days following the occurrence of the incident. A covered entity does not need to know

[3] 6 U.S.C. 681b(c)(2)(A)

the cause of the incident with certainty for it to be a reportable substantial cyber incident. For incidents where the covered entity has not yet been able to confirm the cause of the incident, the covered entity must report the incident if it has a "reasonable belief" that a covered cyber incident occurred.

If an incident meets any of the impact-based criteria, it would be reportable if the covered entity has a "reasonable belief" that the threshold impacts occurred as a result of activity without lawful authority, even if the specific cause is not confirmed. For the fourth prong, a reasonable belief that unauthorized access was caused by a third-party provider or a supply chain compromise would be sufficient to trigger a reporting obligation, even if the cause of the cyber incident was not yet confirmed.

For the purposes of this proposed rule, timely reporting is of the essence for CISA to be able to quickly analyze incident reports, identify trends, and provide early warnings to other entities before they can become victims. Accordingly, CISA believes its ability to achieve the regulatory purposes of CIRCIA would be greatly undermined if covered entities were allowed to delay reporting until an incident has been confirmed to have been perpetrated without lawful authority. Therefore, an incident whose cause is undetermined, but for which the covered entity has a reasonable belief that the incident may have been perpetrated without lawful authority, must be reported if the incident otherwise meets the reporting criteria. If, however, the covered entity knows with certainty the cause of the incident, then the covered entity only needs to report the incident if the incident was perpetrated without lawful authority.

Finally, CISA expects a covered entity to exercise reasonable judgment in determining whether it has experienced a cyber incident that meets one of the substantiality thresholds. If a covered entity is unsure as to whether a cyber incident meets a particular threshold, CISA encourages the entity to either proactively report the incident or reach out to CISA to discuss whether the incident needs to be reported.

CIRCIA Reports

CIRCIA requires a covered entity to submit (either directly or through a third party) a report to CISA when it reasonably believes a covered cyber incident occurred, makes a ransom payment, or experiences one of a number of circumstances that requires the covered entity to update or supplement a previously submitted Covered Cyber Incident Report. CISA is proposing to define "CIRCIA Report" to be an umbrella term that encompasses all four types of covered entity reports collectively – Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report. CIRCIA allows covered entities that make a ransom payment associated with a covered cyber incident to submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements. CISA is proposing to call this joint submission a Joint Covered Cyber Incident and Ransom Payment Report.

Applicability & Definition of a Covered Entity

The proposed Applicability section includes two primary means by which an entity in a critical infrastructure sector qualifies as a covered entity, the first based on the size of the entity and the second based on whether the entity meets any of the enumerated sector-based criteria. An entity in a critical infrastructure sector only needs to meet one of the criteria to be considered a covered entity. CISA is not proposing to scope the term covered entity so broadly as to include virtually every entity within one of the critical infrastructure sectors within the description of covered entity. Thus, they are proposing a description for covered entity that would capture both entities of a sufficient size (based on number of employees or annual revenue) as well as smaller entities that meet specific sector-based criteria.

For example, an entity in a critical infrastructure sector that exceeds the size standard and meets none of the sector-based criteria will be considered a covered entity. Conversely, an entity that meets one or more of the sector-based criteria will be a covered entity regardless of whether it exceeds the size standard. An entity in a critical infrastructure sector does not have to meet both the size-based criterion and one of the sector-based criteria to be considered a covered entity.

Accordingly, CISA proposes to include an equivalently wide variety of types of entities within the scope of the CIRCIA regulatory description of "covered entity" to reflect the same diversity of entities that are in a critical infrastructure sector within the context of Presidential Policy Directive 21 (PPD-21), the National Infrastructure Protection Plan (NIPP), and each sector's Sector-Specific Plan (SSP). CISA is not proposing to limit the scope of the Applicability section to owners and operators of critical infrastructure.

CISA estimates the cost of this proposed rule would be $2.6 billion over ten years, and that 316,244 entities will potentially be affected by these proposals (i.e., covered entities). These impacted covered entities will submit an estimated total of 210,525 CIRCIA Reports – resulting in $1.4 billion in cost to industry and $1.2 billion in cost to the Federal Government.

Healthcare and Public Health (HPH) Sector Proposals

CISA is proposing to include in the description of covered entity multiple sector-based criteria related to the Healthcare and Public Health (HPH) Sector. CISA notes that entities within this sector routinely experience cyber incidents, with U.S. healthcare entities experiencing the seventh most cyber incidents of any industry in 2022.[4] Many entities within the sector currently are required to report certain cyber incidents to HHS under the HIPAA Breach Notification Rule[5] and to the Federal Trade Commission (FTC) under the HITECH Act Health Breach Notification Rule[6]; however, those requirements are generally focused solely on data breaches and do not require reporting of other types of cyber incidents that do not involve unauthorized acquisition of or access to personal health information. Due to the HPH Sector's broad importance to public health, the diverse nature of the entities that compose the sector, the historical targeting of the sector, and the current lack of required reporting unrelated to data breaches or medical devices, CISA is proposing requiring reporting from multiple parts of this sector.

The first criterion CISA proposes related to this sector will mean that certain entities providing direct patient care will be considered covered entities. **Specifically, CISA proposes including in the description of covered entity any entity that owns or operates: 1) a hospital,[7] with 100 or more beds, or 2) a critical access hospital (CAH).[8]**

CISA notes that while many different types of entities provide direct care to patients, such as hospitals, clinics, urgent care facilities, medical offices, surgical centers, rehabilitation centers, nursing homes, and hospices – the size of the facilities, the number of patients cared for daily, and the types of services provided can vary dramatically across these entities. CISA does not believe it is prudent or cost-effective to require covered cyber incident and ransom payment reporting from every individual provider of patient care. CISA is proposing "to focus on hospitals, as they routinely provide the most critical care of these various types of entities, and patients and communities rely on them to remain operational, including in the face of cyber incidents affecting their devices, systems, and networks to keep them functioning."

CISA is proposing requiring reporting from larger hospitals (i.e., those with more than 100 beds) and critical access hospitals (CAHs), as they believe it is "worthwhile to focus on larger hospitals for required reporting, as they are more likely than smaller hospitals to experience substantial impacts if they fall victim to a covered cyber incident given their size and the correspondingly greater number of patients they are caring for on any given day." Additionally, CISA notes that focusing on larger hospitals is supported by much of the same rationale behind CISA's decision to propose an overall size-based criterion based on the SBA small business size standards in the Applicability section (e.g., larger hospitals are more likely to have in-house or access to cyber expertise; larger hospitals are likely to be better equipped to simultaneously respond to and report a cyber incident).

---

[4] See *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.
[5] 45 CFR 164.400-414
[6] 16 CFR 318
[7] As defined by 42 U.S.C. 1395x(e)
[8] As defined by 42 U.S.C. 1395x(mm)(1)

While CISA is not generally proposing to require reporting from smaller hospitals, CISA is proposing to require reporting from CAHs. CISA is making this proposal as CAHs are "typically are the only source of emergency medical care for individuals living within certain rural areas. As a result, a substantial cyber incident at a critical access hospital may have disproportionate impacts to its size given the limited alternative emergency healthcare options for individuals within its service area."

The second HPH Sector-based criterion CISA is proposing would require reporting from manufacturers of drugs listed in Appendix A of the report Essential Medicines Supply Chain and Manufacturing Resilience Assessment, sponsored by the HHS Administration for Strategic Preparedness and Response (ASPR). CISA is proposing that the third HPH Sector-based criterion would require reporting from device manufacturers of Class II (moderate risk) and Class III (high risk) devices. Based on discussions with FDA, CISA believes that requiring reporting from manufacturers of Class II and III devices provides a risk-based means balancing reporting from medical device manufacturers while supporting the collection of an adequate amount of reporting to understand cyber threats, vulnerabilities, and tactics, techniques, and procedures (TTPs) for this industry segment.

CISA believes that the inclusion of all three HPH sector-based criteria is supported by a consideration of the three factors – consequence, threat, and disruption of the reliable operation of critical infrastructure. They note the DHS 2024 Homeland Security Threat Assessment[9] indicates that threats against this sector include Russian and Chinese government-affiliated actors, who are likely to continue to target the HPH Sector.

In establishing these proposed criteria, CISA also considered including criteria related to health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities. Ultimately, CISA determined it was not necessary to include specific sector-based criteria for any of those three industry segments. Specifically, for health insurance companies and entities operating laboratories or other medical diagnostics facilities, CISA believes a sufficient number of entities already will be captured under the size-based criterion that applies across all critical infrastructure sectors.

However, if as a result of public comment, CISA determines that it must modify or eliminate any aspect of the description of covered entity through which health insurance companies and entities operating laboratories or other medical diagnostics facilities are currently captured as part of this proposed rule, including the size-based criterion, CISA may incorporate a sector-based criterion or multiple criteria focused on criteria capturing these entities as part of the final rule to ensure that they remain covered entities.

If CISA were to include one or more sector-based criteria that would cover health insurance companies and laboratories and other medical diagnostics facilities, it would likely set a threshold based on annual revenue, number of employees, or some other metric and only entities that exceed the threshold would be considered covered entities. Such a threshold would be set by CISA to ensure that the largest of these types of entities would be considered covered entities and CISA likely would look at the SBA Size Standards for context and to develop relevant averages using NAICS codes applicable to such entities and may consult with the HPH Sector Risk Management Agency (SRMA) to develop the final criterion or criteria.

CISA believes that, regarding the health IT community, the most common type of cyber incident such entities will face are data breaches. As data breaches are not the primary focus of CIRCIA, and as they are already required to report data breaches of unsecured protected health information (PHI) under existing regulations, CISA does not believe it is necessary to include a specific criterion for these entities.

[9] *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.