CHIME Cheat Sheet – April 4, 2024

Cybersecurity and Infrastructure Security Agency (CISA) Proposed Rule
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

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 3, 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. CIRCIA requires that a covered entity that experiences a covered cyber incident must submit a report to CISA "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred." Additionally, a covered entity that makes a ransom payment must submit a report to CISA "not later than 24 hours after the ransom payment has been made."

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 also seeking public comments on all of the proposed definitions, as well as responses to specific questions listed throughout the proposal.

CISA is aware that covered entity also is 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 experience 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 (CSP), 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, which are detailed further below:

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

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

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.

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 CSP, Managed Service Provider, or Other Third-Party Data Hosting Provider, or 2) Supply Chain Compromise

Impact 1: Substantial Loss of Confidentiality, Integrity, or Availability
Under the first proposed threshold impact, a cyber incident would be considered a substantial cyber incident if it resulted in a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network. Although this prong does not explicitly mention operational technology (OT), CISA is using the term "information system," (which, per the proposed definition, includes OT) in this threshold and proposes to interpret this aspect of the regulation to also specifically cover cyber incidents that lead to substantial loss of confidentiality, integrity, or availability of a covered entity's OT.

The concepts of confidentiality, integrity, and availability (CIA), often referred to as the "CIA triad," represent the three pillars of information security. "Confidentiality" refers to "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. "Integrity" refers to "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity." And "availability" refers to "ensuring timely and reliable access to and use of information."

The loss of CIA of an information system, including OT, or network can occur in many ways, and there are many types of incidents that can lead to a loss of CIA – and would be reportable if the impacts are "substantial." CISA outlines some examples – including, if an unauthorized individual steals credentials or uses a brute force attack to gain access to a system, they have caused a loss of the confidentiality of a system. If that unauthorized individual uses that access to modify or destroy any information on the system, they have caused a loss of the integrity of the system and potentially a loss of the availability of the information contained therein. Additionally, a denial-of service (DoS) attack that renders a system or network inaccessible is another example of an incident that leads to a loss of the availability of the system or network.

Whether a loss of CIA constitutes a "substantial" loss will likely depend on a variety of factors, such as the type, volume, impact, and duration of the loss. One example of a cyber incident that typically would meet the "substantial" threshold for this impact type is a distributed denial-of-service (DDoS) attack that renders a covered entity's service unavailable to customers for an extended period of time. Similarly, a ransomware attack or other attack that encrypts one of a covered entity's core business or information systems substantially impacting the confidentiality, availability, or integrity of the entity's data or services likely also would meet the threshold of a substantial cyber incident under this first impact type and would need to be reported under the CIRCIA regulation.

Persistent access to information systems by an unauthorized third party would typically be considered a substantial loss of confidentiality. By contrast, even time limited access to certain high-value information systems, such as access to privileged credentials or to a domain controller, could also be considered a

substantial loss of confidentiality. A large-scale data breach or otherwise meaningful exfiltration of data typically would also be considered a substantial cyber incident as it would reflect a substantial loss of the confidentiality of an information system. A theft of data that may or may not itself meet the "substantial" impact threshold by nature of the data theft alone (based on the type or volume of data stolen) could become a substantial cyber incident if the theft is followed by a data leak or a credible threat to leak data. Conversely, CISA would not expect a denial-of-service attack or other incident that results in a covered entity's public-facing website being unavailable for a few minutes to typically rise to the level of a substantial cyber incident under this impact.

Impact 2: Serious Impact on Safety and Resiliency of Operational Systems and Processes
The second impact type of the proposed substantial cyber incident definition would require a covered entity to report a cyber incident that results in a serious impact on the safety and resiliency of a covered entity's operational systems and processes.

Safety is a commonly understood term, which the National Institute of Standards and Technology (NIST) defines as "[f]reedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment." NIST defines resilience as "[t]he ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption," and operational resilience as "[t]he ability of systems to resist, absorb, and recover from, or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of the ability to perform mission-related functions."[3]

Similar to the interpretation of the word "substantial" in the first impact type, whether an impact on the safety and resiliency of an operational system or process is "serious" will likely depend on a variety of factors, such as the safety or security hazards associated with the system or process, and the scale and duration of the impact. CISA states that one example would be a cyber incident that noticeably increases the potential for a release of a hazardous material used in chemical manufacturing or water purification likely would meet this definition. Additionally, a cyber incident that compromised or disrupted a BES cyber system that performs one or more reliability tasks would also likely meet this prong of the substantial cyber incident definition. Further, a cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls, would meet this definition.

While CISA anticipates that the types of incidents that will actually lead to a serious impact to the safety and resilience of operational systems and processes may frequently involve OT, CISA does not interpret "operational systems and processes" to be a reference to OT. CISA interprets this prong broadly as not being limited to only incidents impacting OT, and covered entities should report incidents that are covered cyber incidents under this prong of the definition even if the impacts that meet the threshold are not to OT.

Impact 3: Disruption of Ability to Engage in Business or Industrial Operations
The third impact of the proposed substantial cyber incident definition would require a covered entity to report an incident that results in a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services.

In drafting this prong, CISA has added two clauses to the statutory criteria relating to an entity's ability to engage in business operations or deliver goods or services. They are proposing adding these clauses to this prong of the substantial cyber incident definition as it is their understanding that a disruption of business operations includes a disruption to an entity's ability to engage in business operations and the ability to deliver goods or services.

[3] NIST, *Developing Cyber-Resilient Systems*, NIST Special Publication 800-160 Vol. 2 Rev. 1, at 67 (Dec. 2021), available at https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final.

NIST defines a disruption as "[a]n unplanned event that causes a . . . system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction)."[4] Differing from the statutory source for the first two prongs of this definition, the portion of CIRCIA from which this prong is drawn does not contain a qualifier such as "substantial" or "serious." However, because this prong is part of the threshold for a "substantial" cyber incident, CISA believes it is appropriate to read into the prong some level of significance.

Like the previous prongs, whether a disruption rises to the level of reportability may depend on a variety of factors and circumstances – such as the scope of the disruption and what was disrupted. A relatively minor disruption to a critical system or network could rise to a high level of substantiality, while a significant disruption to a non-critical system or network might not. Generally, cyber incidents that result in minimal or insignificant disruptions (e.g., short-term unavailability of a business system or a temporary need to reroute network traffic) are unlikely to rise to the level of a substantial cyber incident reportable under this prong; however, the specific circumstances of the disruption should be taken into consideration.

Examples of cyber incidents that would meet this prong include the exploitation of a zero-day vulnerability resulting in the extended downtime of a covered entity's information system or network, a ransomware attack that locks a covered entity out of its industrial control system, or a distributed denial-of-service attack that prevents customers from accessing their accounts with a covered entity for an extended period of time. CISA states that another example would be where a critical access hospital (CAH) is unable to operate due to a ransomware attack on a third-party medical records software company on whom the CAH relies; the CAH, and perhaps the medical records software company as well if it also is a covered entity, would need to report the incident.

Impact 4: Unauthorized Access Facilitated Through or Caused by a: 1) Compromise of a CSP, Managed Service Provider, or Other Third-Party Data Hosting Provider, or 2) Supply Chain Compromise

The fourth prong of the proposed substantial cyber incident definition would require a covered entity to report an incident that results in 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 compromise of a Cloud Service Provider (CSP), managed service provider, other third-party data hosting provider, or by a supply chain compromise.

NIST defines unauthorized access as occurring when an individual "gains logical or physical access without permission to a network, system, application, data, or other resource."[5] Unauthorized access causes actual jeopardy to information systems and the information therein by compromising the first pillar of the CIA triad – confidentiality – and by providing an adversary with a launching off point for additional penetration of a system or network. Like the third prong, the source language in CIRCIA does not contain any qualifier such as "substantial" or "serious."

However, unlike that prong, CISA understands the absence of a qualifier here to be a reflection of the seriousness of unauthorized access through a third party (such as a managed service provider or CSP) or a supply chain compromise. Such cyber incidents uniquely have the ability to cause significant or substantial nation-level impacts, even if the impacts at many of the individual covered entities are relatively minor.

CISA notes that "the legislative intent makes clear that supply chain compromises such as the "SUNBURST" malware that compromised legitimate updates of customers using the SolarWinds Orion product, and third-party incidents like the compromise of the managed service provider Kaseya, were

[4] NIST, *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Rev. 1, Appendix G, (May 2010), available at https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final.
[5] NIST, *Guide to Industrial Control Systems Security*, NIST Special Publication 800-82 Rev. 3, at 168 (Sept. 2023), available at https://csrc.nist.gov/pubs/sp/800/82/r3/final.

major drivers of the passage of CIRCIA." Therefore, this prong reflects a recognition that CISA needs visibility into the breadth of a third-party incident or supply chain compromise to adequately meet its obligations under CIRCIA.

Examples of cyber incidents that CISA typically would consider meeting this prong include a detected, unauthorized intrusion into an information system or the exfiltration of information as a result of a supply chain compromise. Similarly, unauthorized access that was achieved through exploitation of a vulnerability in the cloud services provided to a covered entity by a CSP or by leveraging access to a covered entity's system through a managed service provider would meet this prong.

Conversely, because the statute requires the unauthorized access to have been facilitated through or caused by a compromise of a third-party service provider or supply chain compromise, unauthorized access that results from a vulnerability within proprietary code developed by the covered entity or a gap in the covered entity's access control procedures that allows an unauthorized employee administrative access to the system would not constitute a substantial cyber incident under this prong (though could still qualify as a substantial cyber incident under one of the first three prongs if it resulted in the requisite impact levels).

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. In other words, 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, 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.

Second, 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[6] 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.

Similarly, if malicious cyber activity is thwarted by a firewall or other defensive or mitigative measure before causing the requisite level of impact, it would not meet the proposed definition of a substantial cyber incident and would not have to be reported. Consequently, blocked phishing attempts, failed attempts to gain access to systems, credentials reported missing but that have not been used to access the system and have since been rendered inactive, and routine scanning that presents no evidence of penetration are examples of events or incidents that typically would not be considered substantial cyber incidents. To both convey this intention and to more closely align with the language used in the CIRC Model Definition, CISA is proposing "a cyber incident that leads to" as the introductory language before the enumerated threshold prongs – which conveys that a covered entity must have experienced one of the enumerated impacts for an incident to be considered a substantial cyber incident.

Third, the type of Tactics, Techniques, and Procedures (TTP) used by an adversary to perpetrate the cyber incident and cause the requisite level of impact is typically irrelevant to the determination of whether an incident is a substantial cyber incident. The primary exception to this is the fourth prong, which is limited to instances where unauthorized access was facilitated through or caused by a

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

compromise of a CSP, managed service provider, or another third-party data hosting provider, or by a supply chain compromise. However, even within this vector-specific prong, the specific TTPs used by the threat actor to compromise a third-party provider or the supply chain is not relevant to whether the incident is reportable.

CISA believes that the specific attack vector or TTP used to perpetrate the incident (e.g., malware, denial-of-service, spoofing, phishing) should not be relevant to determining if an incident is a substantial cyber incident if one of the impact threshold prongs are met. They note that one of the primary purposes of the CIRCIA regulation is to allow CISA the ability to identify TTPs being used by adversaries to cause cyber incidents. Thus, limiting reporting to a specific list of TTPs that CISA currently is aware of would inhibit their ability to fully understand the dynamic cyberthreat landscape as it evolves over time or be able to warn infrastructure owners and operators of novel or reemerging TTPs.

Fourth, 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 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 but nevertheless result in many of the same type of impacts that could result from a cyber incident affecting OT.

Fifth, 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 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.

Exclusions

CISA is proposing to incorporate three exclusions into the definition of substantial cyber incident, taken almost verbatim from the CIRC Model Definition.

Lawfully Authorized Activities of a United States Government Entity or SLTT Government Entity
CISA is proposing to exclude from the definition of substantial cyber incident any lawfully authorized United States Government entity or SLTT Government entity activity, including activities undertaken pursuant to a warrant or other judicial process. This exclusion is intended to except from reporting any incident that occurs as the result of a lawful activity of a Federal or SLTT law enforcement agency, Federal intelligence agency, or other Federal or SLTT Government entity.

This exception does not, however, allow a covered entity to delay or forgo reporting a covered cyber incident to CISA because it has reported a covered cyber incident to, or is otherwise working with, law enforcement. It simply says that a lawful activity conducted by a Federal or SLTT governmental entity, such as a search or seizure conducted pursuant to a warrant, is not itself a substantial cyber incident. This exception also provides further clarity on the scope of cyber incident, which is defined as an occurrence "without lawful authority."

Incidents Perpetrated in Good Faith by an Entity in Response to a Specific Request by the Owner or Operator of the Information System
CISA is proposing to incorporate the exclusory language[7] verbatim into the proposed definition of substantial cyber incident to exclude "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."

CISA notes that there are a variety of situations in which a cyber incident could occur at a covered entity as the result of an entity acting in good faith to a request of the owner or operator of the information system through which the cyber incident was perpetrated. Examples include if a third-party service provider acting within the parameters of a contract with the covered entity unintentionally misconfigures one of the covered entity's devices leading to a service outage, or if a properly authorized penetration test inadvertently results in a cyber incident with actual impacts.

This also excludes reporting cyber incidents that result from security research testing conducted by security researchers who have been authorized by the covered entity or the owner or operator of the impacted information system to attempt to compromise the system, such as in accordance with a vulnerability disclosure policy or bug bounty programs published by the owner or operator. This exception would only apply to this type of research where the bug bounty program, vulnerability disclosure policy, or other form of authorization preceded the discovery of the incident. That said, CISA anticipates that this example would occur rarely, as good faith security research should generally stop at the point the vulnerability can be demonstrated and should not typically engage in activity that would result in a covered cyber incident.

Regarding this exclusion, the request that causes the incident need not necessarily come from the impacted covered entity itself, but rather from the owner or operator of the information system at issue. While the owner or operator of the information system through which the incident was caused will often be the covered entity, that may not always be the case. For example, in some situations involving a

[7] Section 681b(c)(2)(C)(i) of title 6, United States Code

CSP or managed service provider, the service provider may duly authorize a penetration test on its own systems or software. If such testing inadvertently resulted in a cyber incident at the service provider, it could have downstream effects on one or more of the service provider's customers (such as by taking out of operation a key cloud-based software that the customers rely upon for core operations). Such downstream effects could themselves constitute substantial cyber incidents, and, absent this exclusion, could be considered a covered cyber incident, subject to reporting under the proposed CIRCIA regulation if an impacted customer was a covered entity. However, because such a substantial cyber incident would have been perpetrated in good faith pursuant to a penetration test duly authorized by the information system's owner or operator (even if the owner or operator is not the sole impacted entity), neither the covered entity nor the service provider would be required to report the incident.

Conversely, circumstances could occur where a covered entity or the information system's owner or operator authorizes an action that results in a reportable impact despite the immediately precipitating action being approved by the covered entity or information system's owner or operator. For example, if a covered entity, in response to a ransomware attack or other malicious incident, decides to take an action itself resulting in reportable level impacts, such as shutting down a portion of its system or operations, to prevent possibly more significant impacts, this would still be considered a reportable substantial cyber incident. In such a case, because the cyber incident itself was not perpetrated in good faith, and the threshold level impacts would not have occurred but for the initial cyber incident, CISA would not consider the covered entity's actions to meet the "good faith" exception even though the covered entity directed the immediately precipitating action in a good faith attempt to minimize the potential impacts of a cyber incident.

The Threat of Disruption as Extortion, as Described in 6 U.S.C. 650(22)

CIRCIA provides that the description of the types of substantial cyber incidents that constitute covered cyber events shall exclude "the threat of disruption as extortion." CISA is proposing incorporating this exclusion verbatim into the proposed definition of substantial cyber incident with a minor technical correction to include the updated citation to the definition for ransomware attack in CIRCIA.[8] Current statute defines "ransomware attack" as "an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of 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 to extort a demand for a ransom payment."

Although the definition of cyber incident excludes incidents where jeopardy is "imminent" but not "actual," the definition of ransomware attack includes threatened disruptions as a means of extortion. 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.

However, if a covered entity makes a ransom payment in response to such a threat, even if the disruption never materializes into a substantial cyber incident subject to covered cyber incident reporting required by this Part, the payment itself would still be subject to ransom payment reporting required by this Part. 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.

Further, this exclusion would not prevent a cyber incident involving a threat to disclose information obtained from an information system without authorization from being a reportable substantial cyber incident if the cyber incident otherwise meets the threshold for being a substantial cyber incident – for example, under prong (a)(1) of the substantial cyber incident definition due to the initial loss of confidentiality of the information system.

[8] Section 650(22) of title 6, United States Code; 6 U.S.C. 650

Examples of Cyber Incidents that Meet the Definition of Substantial Cyber Incident

To help covered entities determine what might and might not be considered a substantial cyber incident under the proposed definition, CISA is providing examples of a) cyber incidents that are likely to be considered substantial cyber incidents, and b) cyber incidents that are unlikely to be considered substantial cyber incidents. Inclusion on either list is not a formal declaration that a similar incident would or would not be a substantial cyber incident if CISA finalizes the definition as proposed. Inclusion simply indicates the relative likelihood that such an incident would or would not rise to the level of a reportable substantial cyber incident. Determinations as to whether a cyber incident qualifies as a substantial cyber incident would need to be made on a case-by-case basis considering the specific factual circumstances surrounding the incident. CISA notes that they continue to encourage reporting or sharing of information about all cyber incidents, even if it would not be required under the proposed regulation.

Examples of Incidents That Likely Would Qualify as Substantial Cyber Incidents

1) A distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time.
2) Any cyber incident that encrypts one of a covered entity's core business systems or information systems.
3) A cyber incident that significantly increases the potential for a release of a hazardous material used in chemical manufacturing or water purification.
4) A cyber incident that compromises or disrupts a BES cyber system that performs one or more reliability tasks.
5) A cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls.
6) The exploitation of a vulnerability resulting in the extended downtime of a covered entity's information system or network.
7) A ransomware attack that locks a covered entity out of its industrial control system.
8) Unauthorized access to a covered entity's business systems caused by the automated download of a tampered software update, even if no known data exfiltration has been identified.
9) Unauthorized access to a covered entity's business systems using compromised credentials from a managed service provider.
10) The intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose, such as through compromise of identity infrastructure or unauthorized downloading to a flash drive or online storage account.

Examples of Incidents That Would Likely Not Qualify as Substantial Cyber Incidents

1) A denial-of-service attack or other incident that only results in a brief period of unavailability of a covered entity's public-facing website that does not provide critical functions or services to customers or the public.
2) Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic.
3) The compromise of a single user's credential, such as through a phishing attempt, where compensating controls (such as enforced multifactor authentication) are in place to preclude use of those credentials to gain unauthorized access to a covered entity's systems.
4) Malicious software is downloaded to a covered entity's system, but antivirus software successfully quarantines the software and precludes it from executing.
5) A malicious actor exploits a known vulnerability, which a covered entity has not been able to patch but has instead deployed increased monitoring for TTPs associated with its exploitation, resulting in the activity being quickly detected and remediated before significant additional activity is undertaken.

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 – 1) Covered Cyber Incident Report; 2) Ransom Payment Report; 3) Joint Covered Cyber Incident and Ransom Payment Report; or 4) 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."

References to a CIRCIA Report or any of the four types of reports in this proposal are intended to refer to the submission as a whole. However, references to information (either in a CIRCIA Report or about cyber incidents, covered cyber incidents, or ransom payments) are intended to refer to discrete pieces of facts and ideas – which sometimes may be contained within a CIRCIA Report, perhaps along with other pieces of information – rather than the submission as a whole.

Covered Cyber Incident Report Definition
CIRCIA requires a covered entity that experiences a covered cyber incident to report that incident to CISA. CISA is proposing to refer to this type of report as a "Covered Cyber Incident Report" and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to report a covered cyber incident as required by this Part. CISA is further proposing that a Covered Cyber Incident Report also includes any additional, optional information submitted as part of a Covered Cyber Incident Report. Additionally, a covered entity may voluntarily include within this report additional information – which will be considered part of the Covered Cyber Incident Report.

Ransom Payment Report Definition
CIRCIA requires a covered entity that makes a ransom payment, or has another entity (i.e., third party) make a ransom payment on the covered entity's behalf, to report that payment to CISA. CISA is proposing to refer to this type of report as a "Ransom Payment Report," and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to report a ransom payment as required by this Part.

Additionally, CISA is proposing for this report to also include any additional, optional, and voluntary information submitted as part of a Ransom Payment Report. Any voluntarily provided information will be considered part of the Ransom Payment Report. If the ransom payment being reported is the result of a covered cyber incident that the covered entity or a third party acting on its behalf has already reported to CISA, then the Ransom Payment Report also would be considered a Supplemental Report and must meet any requirements associated with Supplemental Reports as well.

Joint Covered Cyber Incident and Ransom Payment Report Definition
Covered entities that make a ransom payment associated with a covered cyber incident prior to the expiration of the 72-hour reporting timeframe for reporting the covered cyber incident may 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," and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to simultaneously report both a covered cyber incident and ransom payment related to the covered cyber incident being reported. CISA is proposing that a Joint Covered Cyber Incident and Ransom Payment Report can also include any additional, optional, and voluntary information submitted as part of the report – and will be considered part of the report.

Supplemental Report Definition
CIRCIA requires a covered entity to promptly submit an update or supplement to a previously submitted Covered Cyber Incident Report under certain circumstances. CISA is proposing to refer to this type of report as a "Supplemental Report," and that the term Supplemental Report will be used to describe a submission made by a covered entity or a third party on behalf of a covered entity to update or supplement a previously submitted Covered Cyber Incident Report or to report a ransom payment made by the covered entity after submitting a Covered Cyber Incident Report as required by this Part. CISA is also proposing that a Supplemental Report can also include any additional, optional information submitted as part of a Supplemental Report.

Ransomware Attack – Definition

CIRCIA requires a covered entity that makes a ransom payment as the result of a ransomware attack to report the ransom payment to CISA within 24 hours of making the payment. CISA believes including a definition for the term ransomware attack will help covered entities determine whether they are required to submit a Ransom Payment Report to CISA.

Current law[9] defines the term ransomware attack as "(A) [] an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of 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 to extort a demand for a ransom payment; and (B) does not include any such event where the demand for payment is (i) not genuine; or (ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system." Because this definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing to use this definition with a few minor modifications described in the proposal.

The proposed definition of ransomware attack contains language mirroring the CIRCIA authorizing legislation that excludes from the definition any event where the demand for a ransom payment is "not genuine" or is "made in good faith by an entity in response to a specific request by the owner or operator of the information system." Circumstances in which an entity may determine a ransom demand is "not genuine" include if the demand is a known hoax or the demand lacks necessary information for the receiving entity to comply, such as an amount demanded or payment instructions. Ransom demands "made in good faith by an entity in response to a specific request by the owner or operator of the information system" typically would include those that are part of red teaming, penetration testing, vulnerability analysis, training exercises, or other authorized activities designed to test prevention, detection, response, or other capabilities of the requesting entity.

In both exclusions, while there may facially be a demand that would otherwise meet the definition of ransomware attack, the demand is made without expectation or desire to actually receive a ransom payment from the covered entity. Similar to the parallel "good faith" exclusion in the definition of substantial cyber incident, because the exception only applies to instances where the demand for ransom payment was made "in response to a specific request by" the information system owner or operator, this exception would only apply to situations where the request or authorization preceded the demand for ransom payment.

Even though the definition of a ransomware attack specifically addresses cyber incidents involving interruption or disruption of operations and threats to do the same, it does not include other forms of extortionate cyber incidents that are similar to ransomware attacks; specifically, extortionate demands for payment based on threats to leak sensitive information obtained without authorization from an information system. While such incidents – without more – do not fall within the definition of a ransomware attack, they would still be reportable under CIRCIA, if the incident otherwise qualifies as a

[9] Section 650(22) of title 6, United States Code

covered cyber incident, as proposed to be defined (e.g., if the underlying incident – including any actual disclosure in line with those threats – leads to the substantial loss of confidentiality of an information system or network.)

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.

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). Further, this is why CISA is not proposing to limit the scope of the Applicability section to owners and operators of critical infrastructure.

CISA is not, however, 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.

Specific Proposed Applicability Criteria – Size-Based & Sector-Based Criterion

CIRCIA requires CISA to include in the final rule "A clear description of the types of entities that constitute covered entities, based on – A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure."

All three factors were central to the determination of the sector-based criteria CISA is proposing to augment the group of entities that would be considered covered entities under the first prong of the criteria contained in the Applicability section based on their size. These factors also drove CISA's proposal to exclude entities in a critical infrastructure sector that fall below the size standards – unless they meet a sector-based criteria – while including entities in a critical infrastructure sector that are larger (even if not otherwise a covered entity based on the sector-based criteria).

Proposed Size-Based Criterion

The first group of entities that CISA is proposing to include as covered entities are entities within a critical infrastructure sector that exceed the U.S. Small Business Administration's (SBA) small business size standard based on either number of employees or annual revenue, depending on the industry. While size is not alone indicative of criticality, larger entities' larger customer bases, market shares, number of employees, and other similar size-based characteristics mean that cyber incidents affecting

them typically have greater potential to result in consequences impacting national security, economic security, or public health and safety than cyber incidents affecting smaller companies.

CISA is proposing that the description of covered entity include any entity in a critical infrastructure sector that exceeds the small business size standard specified by the applicable North American Industry Classification System Code in the SBA Size Standards.[10] These standards "define whether a business is small and, thus, eligible for Government programs and preferences reserved for 'small business' concerns."

SBA Size Standards vary by industry (as designated by NAICS 202 code) and are generally based on the number of employees or the amount of annual receipts (i.e., annual revenue) the business has. SBA reviews and updates the Size Standards every five years via rulemaking. The current SBA Size Standards are contained in the SBA's Table of Small Business Size Standards, effective January 1, 2022, which can be found in statute[11] and here.

Currently, the threshold for those industries where small business status is determined by number of employees is between 100 and 1,500 employees depending on the industry. The threshold for those industries where small business status is determined by annual revenue is between $2.25 million and $47 million depending on the industry. It is estimated that, as of 2022, there are more than 32 million small businesses in the U.S., and that small businesses comprise 99.9% of all American businesses.

CISA believes larger entities will be better situated to simultaneously report and respond to or mitigate an incident, which is a situation many, if not most, reporting entities will be faced with given the statutorily mandated 72-hour reporting requirement for Covered Cyber Incident Reports and 24-hour reporting requirement for Ransom Payment Reports. Finally, larger entities generally will be better situated to absorb costs associated with reporting, even if per report costs are relatively minimal, as CISA believes they will be.

Proposed Sector-Based Criteria

CISA is also proposing to include as part of the description of covered entity in the Applicability section a series of criteria that are based on characteristics typically associated with entities in one or more specific critical infrastructure sectors or subsectors. Specifically, CISA is proposing to include in the scope of covered entity any entity that meets one or more of a set of specified sector-based criteria. These criteria apply regardless of the specific critical infrastructure sector of which the entity considers itself to be part.

CISA is proposing these additional, sector-based criteria for a variety of reasons – namely, that an entity's size does not necessarily reflect its criticality. CISA is proposing sector-based criteria for entities operating in each of the critical infrastructure sectors listed in the proposed rule. During the development of these proposed criteria, CISA engaged each of the SRMAs to consult on potential criteria for their respective sector, as well as other Federal agencies with cybersecurity-related regulatory authorities focused on specific sectors. CISA also considered the input received from the public through both the CIRCIA listening sessions and in response to the CIRCIA RFI.

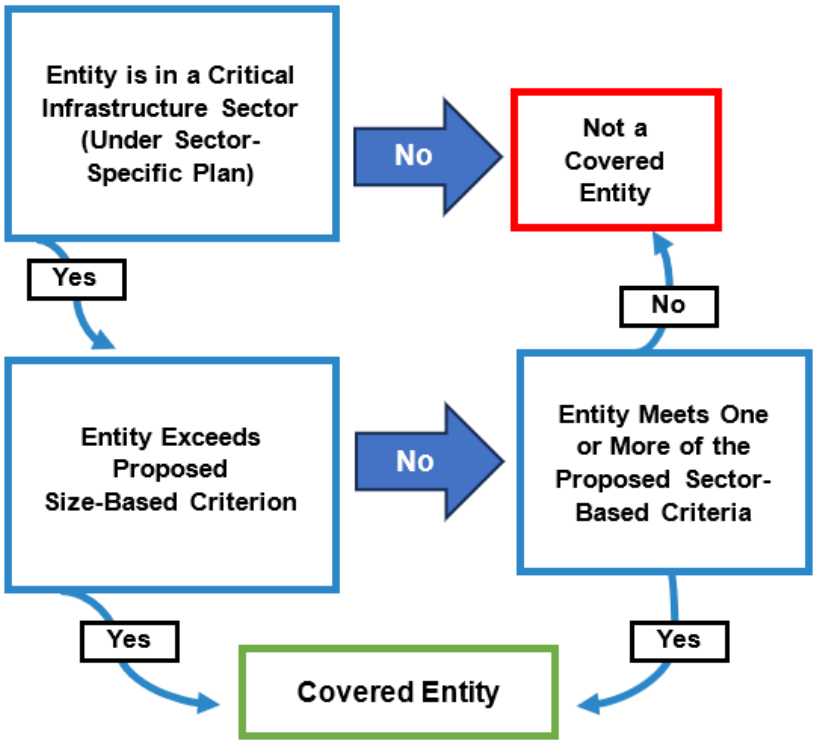
For the proposed sector-based criteria, CISA proposes to cover entities that own or operate certain types of facilities or entities that perform certain functions as covered entities. For example, if an entity manufactures Class II or III medical devices, in addition to other functions that do not meet one of the sector-based criteria, the entire entity is the covered entity, and any substantial cyber incident experienced by any part of the entity would need to be reported, regardless of whether the underlying incident impacted the manufacturing of Class II or III medical devices.

[10] 13 CFR part 121
[11] 13 CFR 121.201

Considering the entire entity (e.g., corporation, organization), and not an individual facility or function, as the covered entity will also avoid delays in reporting that could be caused if entities had to wait to specifically determine whether particular facilities or functions were impacted by a substantial cyber incident.

CISA estimates that 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.

Proposed Covered Entities – Decision Tree



Determining if an Entity is in a Critical Infrastructure Sector

If an entity is unsure as to whether or not it is part of a critical infrastructure sector, CISA recommends the entity review the SSP for the sector or sectors that most closely align with the line of activities in which the entity is engaged. Once the final rule has been issued, entities will also be able to reference informational materials that will be published as part of CISA's outreach and education campaign. If after taking these steps, an entity still is unsure as to whether it is in a critical infrastructure sector, CISA recommends the entity contact CISA so that they can assist the entity in determining if it is in a critical infrastructure sector.

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 the HPH 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.

CISA further 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.[12] Many entities within the sector currently are required to report certain cyber incidents to HHS under the HIPAA Breach Notification Rule[13] and to the Federal Trade Commission (FTC) under the HITECH Act Health Breach Notification Rule[14]; 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,[15] with 100 or more beds, or 2) a critical access hospital (CAH).[16]**

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).

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

[12] See *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.
[13] 45 CFR 164.400-414
[14] 16 CFR 318
[15] As defined by 42 U.S.C. 1395x(e)
[16] As defined by 42 U.S.C. 1395x(mm)(1)

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 TTPs for this industry segment.

CISA believes that the inclusion of all three Healthcare and Public Health Sector 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[17] 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.

CISA would specifically be interested in receiving comments on:

1) The scope of entities that would and would not be considered covered entities based on the three criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the criteria; and
2) The proposal to forgo including specific criteria focused on health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities.

Personal Information – Definition

CISA is proposing to define the term “personal information” to mean information that identifies a specific individual or information associated with an identified or identifiable individual. Under this definition, personal information would include, but are not limited to, both identifying information such as

[17] *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.

photographs, names, home addresses, direct telephone numbers, and Social Security numbers as well as information that does not directly identify an individual but is nonetheless personal, nonpublic, and specific to an identified or identifiable individual.

Examples would include medical information, personal financial information (e.g., an individual's wage or earnings information; income tax withholding records; credit score; banking information), contents of personal communications, and personal web browsing history. This proposed definition would include "personally identifiable information," as defined in OMB Memorandum M-17-12 as referring to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, but also proposes to include information that might not be clearly linkable to an individual but would nonetheless relate to a specific individual and be considered personal and nonpublic, such as an individual's web browsing history or the content of an email.

CISA is proposing this definition to encompass the broad range of personally sensitive information that a cybersecurity incident might implicate, including the content of personal communications, which might not be able to be used on its own to identify an individual, to ensure that all personally sensitive information is handled appropriately. CISA is not proposing to include in this definition information that does not relate to a specific individual – information such as general business telephone numbers or business financial information would generally not be considered personal information under this definition.

This proposed definition of "personal information" would be different and broader than the approach taken by the Cybersecurity Information Sharing Act of 2015,[18] which more narrowly requires removal of information that is "known at the time of sharing" to be "personal information" that identifies a specific person or belongs to a specific person – rather than information that is linked or linkable to a specific person. CISA is seeking public comment on this proposed definition, and whether they should instead adopt the approach taken by the Cybersecurity Information Sharing Act of 2015.

Instructions for Personal Information

CISA is proposing steps to minimize the collection of unnecessary personal information in CIRCIA Reports and in responses to RFIs. First, CISA is proposing that covered entities should only include personal information that is requested in the reporting form or in the RFI and should exclude any unnecessary personal information. CISA would include on the CIRCIA Incident Reporting Form instructions and guidance on when personal information should and should not be included in a CIRCIA Report.

While some personal information, such as the contact information for the covered entity and information about the identity of the actor perpetrating the incident (if known), will be required for the CIRCIA Incident Reporting Form, CISA will endeavor to provide clear guidance to help covered entities avoid submitting extraneous personal information. For example, while the CIRCIA Report would require categories of information that were believed to have been accessed or acquired by an unauthorized person, CISA would provide guidance that CIRCIA Reports should not include any specific personal information that was accessed. Thus, while a covered entity might indicate whether, for example, medical or driver's license information was accessed in the incident, the covered entity should not provide the medical information itself nor a list of the compromised driver's license numbers or images.

CISA would also include privacy-preserving measures in the CIRCIA Incident Reporting Form tool itself to help prevent covered entities from including unnecessary personal information. Such measures could include limiting the number of fields requiring open-ended responses, as well as mechanisms to scan for indicators that unnecessary personal information might be included (e.g., information in standard social security number format) and prompts for the covered entity to verify whether the information is necessary to submit before proceeding with the report submission.

[18] (6 U.S.C. 1501 et seq.). 6 U.S.C. 1503(d)(2)

CISA would make the guidance publicly available, likely by publishing the guidance on its website at the same time as the publication of the final rule for this rulemaking. CISA proposes to review the effectiveness of the guidance one year after publication to ensure it is appropriate to the needs for retention, use, and dissemination of personal information for mitigation and protection against cybersecurity threats and appropriately protect privacy and civil liberties of individuals. CISA proposes to conduct periodic subsequent reviews after the initial review. The CISA Chief Privacy Officer will also conduct an initial review of CISA's compliance with the guidance after one year and subsequent periodic reviews not less than every three years. Where reviews result in a change needed to the guidance, CISA would publish updated guidance on its website. CISA has included the draft CIRCIA Privacy and Civil Liberties Guidance document in the docket for this proposed rule, and is seeking public comment on any aspect of the draft guidance.

Requirements & Procedures – Required Reporting on Covered Cyber Incidents and Ransom Payments

As required by CIRCIA, CISA is proposing four circumstances which require covered entities – or third parties on their behalf – to submit a report to CISA, subject to certain proposed exceptions or limitations.

First, CIRCIA requires a covered entity that experiences a covered cyber incident to report that incident to CISA. **Second**, CIRCIA requires a covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity to report that payment to CISA. **Third**, CIRCIA requires that, until a covered entity notifies CISA that the covered cyber incident in question has concluded and been fully mitigated and resolved, a covered entity must submit an update or supplement to a previously submitted report on a covered cyber incident if substantial new or different information becomes available. **Fourth**, CIRCIA requires that a covered entity submit an update or supplement to a previously submitted report on a covered cyber incident if the covered entity makes a ransom payment after submitting a Covered Cyber Incident Report.

A covered entity would comply with the first reporting requirement by submitting, or having a third party submit on their behalf, a Covered Cyber Incident Report or a Joint Covered Cyber Incident and Ransom Payment Report. CISA notes that cyber incidents do not occur in a single moment in time but span from the initial moment of compromise until the cyber incident is fully mitigated and resolved. Because of this, CISA interprets the word "experiences" to include the full lifecycle of a cyber incident, such that this reporting requirement applies to any entity that qualifies as a covered entity at any point during the occurrence of the covered cyber incident.

Additionally, CISA is proposing to require a covered entity to report a ransom payment regardless of whether the covered entity itself makes the ransom payment or has a third party make the ransom payment on the covered entity's behalf. Because this reporting requirement is tied to a single action that occurs at a specific moment in time (i.e., the making of a ransom payment) CISA interprets the word "makes" to apply this reporting requirement to any entity that qualifies as a covered entity at the moment in time that it makes a ransom payment as the result of a ransomware attack.

Depending on the circumstances surrounding and timing of the ransom payment, including whether the ransomware attack is a covered cyber incident, the type of CIRCIA Report a covered entity (or third party on behalf of a covered entity) might use to comply with this proposed requirement may vary. For example, if the ransom payment was made as the result of an incident that did not qualify as a covered cyber incident, the covered entity would submit a Ransom Payment Report. If the ransom payment was made as the result of a covered cyber incident that has not yet been reported, the covered entity may opt to submit a Joint Covered Cyber Incident and Ransom Payment Report instead of a Covered Cyber Incident Report, and a separate Ransom Payment Report. A covered entity that makes a ransom payment associated with a covered cyber incident prior to the expiration of the 72-hour reporting

timeframe for reporting the covered cyber incident may submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements.

CISA is proposing to include the statutory reporting requirements that mandate a covered entity provide CISA with updates or supplements in certain circumstances. CIRCIA refers to these types of reports as Supplemental Reports, which a covered entity is obligated to provide unless and until it has notified CISA that the underlying covered cyber incident has concluded and been fully mitigated and resolved. Additionally, a covered entity may submit a Supplemental Report to inform CISA that a covered cyber incident previously reported has concluded and been fully mitigated and resolved – but notifying CISA is optional.

There are two scenarios that CISA is proposing that will require the submission of a Supplemental Report. The first scenario resulting in the requirement is when substantial new or different information becomes available to a covered entity. As with the covered cyber incident reporting requirement, CISA interprets this requirement as applying to an entity that is a covered entity during any point in the incident lifecycle, such that any entity that qualifies as a covered entity for the purposes of the covered cyber incident reporting requirement is also subject to the supplemental reporting requirement to the extent new or different information becomes available.

The second scenario resulting in the requirement to submit a Supplemental Report is when a covered entity makes a ransom payment related to a covered cyber incident for which the covered entity has already submitted a Covered Cyber Incident Report. As with the ransom payment reporting requirement, CISA interprets this requirement as applying to an entity that is a covered entity at the time a ransom payment is made, assuming they also were subject to the covered cyber incident reporting requirement described above.

Reporting of Single Incidents Impacting Multiple Covered Entities

CISA anticipates that occasions will occur where a single cyber incident causes substantial cyber incident-level impacts to multiple covered entities. Who must report, and the number of reports that must be submitted in those situations may vary depending on the relationship between the impacted entities. In cases where a single cyber incident impacts multiple unaffiliated covered entities, each covered entity that experiences substantial cyber incident-level impacts must submit a Covered Cyber Incident Report to CISA.

For example, if a compromise of a CSP causes substantial cyber incident level-impacts at multiple unaffiliated customers of the CSP, more than one of whom is a covered entity, then each of the impacted customers that are covered entities are responsible for submitting (or having a third party submit on their behalf) a Covered Cyber Incident Report. The covered entity customers could, however, authorize the CSP to submit Covered Cyber Incident Reports on their behalf if the CSP has or is provided with sufficient information to complete the Covered Cyber Incident Reports. The CSP may also have to separately submit a Covered Cyber Incident Report if it is itself a covered entity and it experiences threshold impacts that meet the definition of a substantial cyber incident.

Conversely, in cases where a single cyber incident causes substantial cyber incident-level impacts at multiple affiliated covered entities, the covered entities can meet their reporting obligations through either a) the submission of a single Covered Cyber Incident Report that provides the required information on all of the impacted entities, or b) multiple Covered Cyber Incident Reports, with one or more covered entities submitting their own reports. In these and similar cases, the impacted covered entities may satisfy their reporting requirements under CIRCIA through the submission of a single Covered Cyber Incident Report so long as that report details the impacts experienced by each of the affected covered entities, any other required covered entity-specific details, and point(s) of contact who individually or collectively represent all of the covered entities on whose behalf the Covered Cyber Incident Report is being submitted.

Exceptions to Required Reporting on Covered Cyber Incidents and Ransom Payments

CIRCIA contains three scenarios in which a covered entity is excepted from having to report a separate covered cyber incident or ransom payment. The first of these exceptions authorizes a covered entity to submit a single CIRCIA Report containing information on both a covered cyber incident and ransom payment when the covered entity makes a ransom payment related to a covered cyber incident within the 72-hour window for reporting the covered cyber incident.

The second exception allows a covered entity to forgo providing an otherwise required CIRCIA Report to CISA if it is legally required to report substantially similar information within a substantially similar timeframe to another Federal agency with whom CISA has an information sharing agreement and mechanism. The third exception states that CIRCIA reporting requirements shall not apply to certain covered entities, or specific functions of those entities, that are owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System (DNS). Additionally, CISA is proposing a fourth exception that would except Federal agencies from having to submit a CIRCIA Report to CISA if the Federal agency is required to report the incident in question to CISA pursuant to the Federal Information Security Management Act (FISMA).[19]

Substantially Similar Reporting Exception

If a covered entity that is required by law, regulation, or contract to report substantially similar information on a covered cyber incident or ransom payment to another Federal agency in a substantially similar timeframe as that required under CIRCIA, it does not have to submit a Covered Cyber Incident Report or Ransom Payment Report to CISA on that covered cyber incident or ransom payment if CISA has an information sharing agreement and mechanism in place with that Federal agency.

Under that same provision of CIRCIA, a covered entity is excepted from having to submit a Supplemental Report to CISA if the entity is required to provide to another Federal agency substantially similar information to that which the entity would otherwise be obligated to provide to CISA in a Supplemental Report, must do so in a substantially similar timeframe as that required under CIRCIA, and CISA has both an information sharing agreement and mechanism in place with the other Federal agency. This reporting exception (hereinafter the “substantially similar reporting exception”) will allow covered entities subject to more than one Federal cyber incident reporting requirement to avoid having to report duplicative information to both CISA and another Federal agency when certain conditions are met.

CISA interprets the statutory language to require five criteria for the application of the substantially similar reporting exception to apply:

1) the report must be required to contain substantially similar information to that required to be included in the applicable CIRCIA report;
2) the report must be required to be provided to the other Federal agency in a timeframe that allows CISA to receive the report in a substantially similar timeframe to that which the covered entity would otherwise have been obligated to provide the report to CISA pursuant to CIRCIA;
3) CISA and the Federal agency to which the covered entity submits the report must have an information sharing agreement in place that satisfies the requirements of 6 U.S.C. 681g(a) (hereinafter a CIRCIA Agreement);
4) CISA and the Federal agency to which the covered entity submits the report must have a mechanism in place by which the Federal agency can share the report with CISA within the required timeframe; and
5) the covered entity must have submitted the report to the other Federal agency pursuant to a legal, regulatory, or contractual obligation.

[19] 44 U.S.C. 3551 et seq.

CISA is proposing to only enter into a CIRCIA Agreement when CISA has determined that the Federal agency with whom CISA is entering into the agreement receives cyber incident reports from one or more CIRCIA covered entities pursuant to a legal, regulatory, or contractual obligation, and the reporting obligation requires the submission of substantially similar information in a substantially similar timeframe. When assessing whether another reporting obligation requires reporting of substantially similar information in a substantially similar timeframe to CIRCIA, CISA intends to coordinate with the Federal department or agency responsible for the non-CIRCIA reporting obligation which will inform CISA's decision making process. If and when CISA has entered into a CIRCIA Agreement, CISA will announce and catalogue the existence of the CIRCIA Agreement on a public-facing website.

Substantially Similar Information

To qualify for the substantially similar reporting exception, the information reported by a covered entity on a covered cyber incident or ransom payment to another Federal agency must be substantially similar to the information that the covered entity would be required (but for the exception) to report to CISA under this Part. CISA does not intend to define what constitutes substantially similar information in the final rule; but rather, is proposing to retain discretion in making this determination. In determining whether information is substantially similar, CISA will consider whether the information required by the fields in CISA's CIRCIA Report forms is functionally equivalent to the information required to be reported by the covered entity to another Federal agency. CISA views functionally equivalent as meaning that the information or data serves the same function or use, provides the same insights or conclusions, and enables the same analysis as the information or data requested in the relevant CIRCIA Report form fields.

CISA does not believe that the substantially similar information qualifier requires information to be reported in the same format to the other Federal agency, as their reporting forms are unlikely to precisely mirror the CIRCIA Report. A covered entity could submit information in another Federal agency's reporting form that, while not directly aligning with a specify query in a CIRCIA Report form, nonetheless provides functionally equivalent data. CISA's determination that information is substantially similar will hinge on whether the data and information required to be submitted in a CIRCIA Report form are substantively included in the report to the other Federal agency.

Substantially Similar Timeframe

To qualify for this exception, the covered entity must also be required to report this information to another Federal agency under law, regulation, or contractual provision in a substantially similar timeframe. In interpreting this requirement, CISA must keep in mind the limitations related to sharing of reports pursuant to a CIRCIA Agreement. Specifically, the section of CIRCIA which requires that Federal agencies who share reports with CISA pursuant to a CIRCIA Agreement must do so "in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments."

CISA interprets these statutory requirements to render the substantially similar reporting exception available only if CISA receives the report on a covered cyber incident or ransom payment from the other Federal agency within the same timeframe in which the covered entity would have been required to submit the report to CISA under CIRCIA had the covered entity reported directly to CISA. Thus, for a law, regulation, or contractual provision to require reporting within a "substantially similar timeframe" of CIRCIA, it must require a covered entity to report a covered cyber incident within 72 hours from when the covered entity reasonably believes that the covered cyber incident has occurred and a ransom payment within 24 hours after the ransom payment has been disbursed, leaving the Federal agency time to share the report with CISA – unless a mechanism is in place that allows CISA to receive the report at the same time as the other Federal agency.

Supplemental Reporting

Supplemental Reports may also qualify for the substantially similar reporting exception, provided that the supplemental report provided to the other Federal agency meets the relevant requirements. As with

a Covered Cyber Incident Report or Ransom Payment Report, the exception is only available if the covered entity is required to submit substantially similar information in a substantially similar timeframe to another Federal agency under law, regulation, or contract and CISA and the other agency have a CIRCIA Agreement and information sharing mechanism in place to meet the CIRCIA Report deadlines. CIRCIA requires Supplemental Reports be submitted "promptly," which CISA interprets as within 24 hours of the triggering event. A covered entity remains responsible for submitting Supplemental Reports to CISA as required under this Part unless the covered entity submits any substantial new or different information to another Federal agency and CISA has published a CIRCIA Agreement with that Federal agency that specifically covers Supplemental Reports.

Manner, Form, and Content of Reports

Covered entities must make CIRCIA Reports in the manner and form prescribed in the final rule. CIRCIA requires CISA to include procedures for submitting these reports in the final rule, including the manner and form thereof. CIRCIA gives CISA broad discretion in determining the manner and form for submission of CIRCIA Reports, it requires CISA to "include, at a minimum, a concise, user-friendly web-based form" as one manner for submission of required reports.

CISA is proposing that a covered entity must submit CIRCIA Reports through the web-based CIRCIA Incident Reporting Form, to be available on CISA's website – or in any other manner approved by the Director. CISA intends to offer an electronic, web-based form as the preferred manner of submission of CIRCIA Reports.

CISA notes that a web-based form is a cost-effective way to gather information from large numbers of submitters both simultaneously and over time. If designed properly, it allows for significant standardization of data (in both form and content) and tailoring of circumstance-specific questions using dynamic prompts and responses incorporating conditional logic filters and conditional or branching questions. Also, a web-based form can also reduce the likelihood of human error in various ways – examples of which are listed in the proposal – during the data submission process. Additionally, a web-based form only requires the involvement of a single individual (i.e., the person entering the information into the form on behalf of the covered entity) and allows for that individual to review information after entry but prior to submission, greatly reducing the potential for such errors.

CISA notes that a cyber incident at a covered entity could make it impossible or insecure for a covered entity to use its own information system(s) to report via a web-based form. However, CISA believes that this is a relatively minor concern, as organizations and individuals today typically have a variety of ways to access the internet. Additionally, CISA intends to make the web-based form available via a web browser so that incident reports can be submitted from any internet-connected device. This should allow covered entities various ways to access the form even if the entity's IT system is rendered inoperable by a cyber incident. Furthermore, CIRCIA permits a third party to submit CIRCIA Reports on a covered entity's behalf, such that even if the covered entity itself cannot report via a web-based form using its own information system(s) or any other internet connected device, any number of third parties should be able to submit the CIRCIA Report on the covered entity's behalf.

There is the potential that an incident at CISA could render the web-form unavailable for use by covered entities for a period of time. However, CISA has extensive experience building systems that operate with high availability and intends to build in redundancy to ensure the 24/7 availability of the reporting system. CISA also intends to maintain a capability to support reporting via telephone as a back-up option so that, in the unlikely event of an extended interruption of the availability of the web-based form, any impacted covered entities will have an alternative mechanism available to submit CIRCIA Reports in a timely manner. This or any other approved alternative mechanism also may be used in lieu of the web-based reporting system should a covered entity wish to submit a CIRCIA Report during any short-term unavailability of the system, for example, if CISA must temporarily restrict access to the web-based form for routine maintenance.

CISA is also proposing to include the statement that covered entities may also submit CIRCIA Reports in any other manner and form of reporting approved by the Director. This provision would allow CISA to operate a telephonic reporting capability as a backup system and maintain flexibility to offer alternative manners of submission in the future on a short-or long-term basis. CISA believes that this flexibility is important for several reasons. The "any other manner and form of reporting approved by the Director" clause will allow CISA the agility to more rapidly authorize entities to submit CIRCIA Reports via machine-to-machine reporting should CISA determine that is a viable, cost-effective approach in the future without having to undertake additional rulemaking. Similarly, this provision will allow CISA the flexibility to consider and adopt new submission mechanisms that may become feasible as technology advances. CISA will publicize any additional manners of submission on its website and through notifications to stakeholders – should the CISA Director approve any.

Form for Reporting

CISA is proposing to use the "concise, user-friendly web-based form" to offer as the preferred and primary means for submitting CIRCIA Reports. CISA is proposing to name this web-based form the "CIRCIA Incident Reporting Form." CISA is proposing to use the same user interface for the CIRCIA Incident Reporting Form regardless of which of the four types of discrete mandatory reports identified in CIRCIA (i.e., Covered Cyber Incident Report; Ransom Payment Report; Joint Covered Cyber Incident and Ransom Payment Report; and Supplemental Report) that must be submitted by a covered entity. Additionally, CISA is proposing to use the same user interface regardless of whether a covered entity itself is submitting a CIRCIA Report or if a third party is submitting a report on behalf of a covered entity.

To facilitate this approach, CISA is proposing to use a dynamic, user friendly, web-based form with conditional logic filters, with questions that adjust based on the answers to gateway or filtering questions used throughout the form. For instance, an early question might ask the submitter to indicate what type of report is being submitted – and the questions that follow will be tailored based on the response provided by the submitter.

CISA believes that numerous benefits exist in using the same user interface for all CIRCIA Reports – and potentially for voluntarily provided reports as well. First, this approach would allow all entities to go to a single location to comply with their CIRCIA reporting obligations regardless of what type of CIRCIA Report they need to submit. Second, it would prevent the covered entity from having to choose from multiple different forms to determine which is the correct set of questions for their particular reporting situation.

There are a variety of circumstances under which a covered entity may be submitting a CIRCIA Report, such as a covered cyber incident that does not involve a ransom payment, a covered cyber incident for which a ransom payment has been made, a ransom payment being reported via a Supplemental Report after a covered cyber incident has been submitted, or a ransom payment made in response to a cyber incident that does not meet the criteria of a covered cyber incident. Instead of creating unique forms for each possible reporting scenario and requiring the covered entity to correctly identify which one applies, having a single user interface that can be used to address any potential reporting circumstance eliminates both the need for the covered entity to expend resources identifying the correct form and the possibility of the covered entity selecting the incorrect form.

Finally, a single user interface also reduces the burden in situations where the covered entity's reporting requirements change during the preparation of the report. For instance, a covered entity may begin to report a covered cyber incident and, before submitting it to CISA, the entity makes a ransom payment as part of its response to the incident. Having a dynamic user interface may make it possible to allow the covered entity to modify its responses to certain questions and/or add the additional information related to the ransom payment rather than recreate all of its previous work in a separate form designed specifically for submitting a Joint Covered Cyber Incident and Ransom Payment Report.

In the user interface, CISA intends to use a mixture of input options, such as radio buttons, drop-down menus, and text boxes. Tailoring the response format and options for individual questions will allow CISA to advance various goals simultaneously, to include reducing the burden of completing the report, supporting consistency in terminology to facilitate analysis of data, facilitating the logic-flow based tailoring of questions, and offering opportunities for covered entities to provide additional pertinent details via narratives where useful. CISA's proposed approach of using a dynamic reporting user interface for all CIRCIA Reports would enable a covered entity to submit information on both a covered cyber incident and ransom payment (i.e., a Joint Covered Cyber Incident and Ransom Payment Report) at the same time using the same form – satisfying CIRCIA requirements.

Proposed Content to be Included in All CIRCIA Reports

CISA is proposing certain content – the majority explicitly required by CIRCIA – which must be submitted by a covered entity regardless of the type of CIRCIA Report being submitted, while other content will be required only in certain types of CIRCIA Reports. Additionally, CISA is proposing other categories of content for inclusion in a specific type of report, organized by report type.

Covered Cyber Incident Report Specific Content
CISA is proposing requiring submission of information in the following categories of content in a Covered Cyber Incident Report: a) Description of the Covered Incident; b) Vulnerabilities, Security Defenses, and TTPs; c) Information related to the Identity of the Perpetrator of the Incident; d) Mitigation/Response; and e) Additional Data or Information.

As noted in the individual content categories, CISA is proposing that some of the proposed data elements within the individual content categories are required while other proposed data elements are optional. CISA intends to ask for all the required information in an initial Covered Cyber Incident Report; however, they understand that a covered entity may not know all of the required information within the initial 72-hour reporting timeframe. Accordingly, answers of "unknown at this time" or something similar will be considered acceptable for certain questions in initial reporting. A covered entity must, however, comply with its Supplemental Reporting requirements and provide previously unknown information promptly to CISA once discovered if the information meets the "substantial new or different information" threshold. That includes any information required to be submitted in an initial Covered Cyber Incident or Joint Covered Cyber Incident and Ransom Payment Report that a covered entity subsequently learns after initially responding that the information was unknown at the time of reporting.

CISA is proposing that a covered entity ultimately must provide all applicable required content in either the initial Covered Cyber Incident Report or a Supplemental Report to be considered fully compliant with its reporting obligations under CIRCIA.

Ransom Payment Report Specific Content
CIRCIA is proposing and outlines the required specific content that is to be included in a Ransom Payment Report. Two of the items, information identifying the covered entity that made the ransom payment (or on whose behalf the ransom payment was made) and contact information for the covered entity or an authorized agent thereof, are part of the categories of information that must be included – regardless of report type.

The additional items specific to inclusion in Ransom Payment Reports include: a) Description of the Ransomware Attack; b) Vulnerabilities, Security Defenses, and TTPs; c) Information Related to the Identification of the Perpetrator of the Attack; d) Information on the Ransom Payment; e) Results of Ransom Payment; and f) Additional Data or Information.

Supplemental Report Specific Content
While CIRCIA includes some specific categories of content that a covered entity must include in a Covered Cyber Incident Report or Ransom Payment Report, CIRCIA does not contain any similar

requirements regarding what content must be included in a Supplemental Report. 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.

A unique content request proposed to be contained in a Supplemental Report is information on the purpose for filing the Supplemental Report. CISA envisions providing a list of possible answers for this question, which may include: a) providing CISA with newly discovered information that makes a previously submitted Covered Cyber Incident Report or Supplemental Report more complete; b) providing CISA with information that corrects or amends a previously submitted Covered Cyber Incident Report or Supplemental Report; c) informing CISA that the covered entity has made a Ransom Payment related to a previously reported covered cyber incident; or d) informing CISA that the covered entity considers a previously reported covered cyber incident concluded and fully mitigated and resolved. CISA is also proposing to require that a Supplemental Report include the case identification number provided by CISA for the covered cyber incident with which the Supplemental Report is associated. This will facilitate pre-population of the Supplemental Report form and help CISA ensure that the Supplemental Report is properly assigned and maintained.

For Supplemental Reports being submitted by a covered entity for the purposes of informing CISA that the covered entity considers a previously reported covered cyber incident concluded and fully mitigated and resolved, CISA proposes including optional questions in the form that would allow a covered entity to provide information on the actual recovery date and time, and an estimate of the costs incurred to fully mitigate the incident, as well as any other financial losses (e.g., losses in productivity; losses in revenue) incurred due to the incident.

Timing of Submission of CIRCIA Reports

Timing for Submission of Covered Cyber Incident Reports

CIRCIA requires that a covered entity that experiences a covered cyber incident must submit a Covered Cyber Incident Report to CISA "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred." CISA is proposing language establishing this timeframe.

CISA acknowledges that the point at which a covered entity should have "reasonably believed" a covered cyber incident occurred is subjective, and will depend on the specific factual circumstances related to the particular incident. Accordingly, CISA is not proposing a specific definition for the term "reasonably believes," nor is CISA attempting to prescribe a specific point in the incident life cycle at which a "reasonable belief" will always be realized. Rather, CISA is providing the following guidance to help covered entities understand when a "reasonable belief" generally is expected to have occurred.

CISA does not expect a covered entity to have reached a "reasonable belief" that a covered cyber incident occurred immediately upon occurrence of the incident, although this certainly may be true in some cases (e.g., an entity receives a ransom demand simultaneously with discovery that it has been locked out of its system). Oftentimes, an entity may need to perform some preliminary analysis before coming to a "reasonable belief" that a covered cyber incident occurred. This preliminary analysis may be necessary, for instance, to quickly rule out certain potential benign causes of the incident or determine the extent of the incident's impact. CISA believes that in most cases, this preliminary analysis should be relatively short in duration (i.e., hours, not days) before a "reasonable belief" can be obtained, and generally would occur at the subject matter expert level and not the executive officer level. As time is of the essence, CISA expects a covered entity to engage in any such preliminary

analysis as soon as reasonably practicable after becoming aware of an incident and is proposing including this requirement.

Timing for Submission of Ransom Payment Reports

Under CIRCIA, a covered entity that makes a ransom payment must submit a Ransom Payment Report to CISA "not later than 24 hours after the ransom payment has been made." CISA is proposing language establishing this timeframe. CISA is proposing to interpret payment to have been made upon disbursement of the payment by the covered entity or a third party directly authorized to make a payment on the covered entity's behalf. CISA is proposing to select payment disbursement instead of payment settlement or clearance as the trigger for when the reporting timeline begins for several reasons, including that it prevents a covered entity from having to try to determine when a payment has actually been received by or otherwise made available to the payee.

CISA recognizes that in certain situations, more than one third party may be involved in the disbursement of a ransom payment. For instance, a covered entity might send funds to an intermediate third party, who might then transmit the funds to a financial institution, who then transfers the payment to the account specified by the party demanding the ransom payment. In interpreting this regulatory provision, the reporting timeline shall be deemed to be initiated at the earliest instance of disbursement. Thus, in the example provided, disbursement has occurred and the timeline for reporting would be triggered when the covered entity sent funds to the intermediate third party. Where a covered entity authorizes an intermediate third party to transmit funds on its behalf to make a ransom payment but does not actually disburse funds itself at that time, the reporting timeline shall be deemed to be initiated when the intermediate third party disburses funds.

Timing for Submission of Supplemental Reports

CIRCIA requires that a covered entity that has previously submitted a Covered Cyber Incident Report must "promptly" submit to CISA an update or supplement to that report if either: a) "substantial new or different information becomes available"; or b) "the covered entity makes a ransom payment after submitting a covered cyber incident report." A covered entity is subject to these supplemental reporting obligations unless and until the covered entity notifies CISA that the incident that is the subject of the original Covered Cyber Incident Report "has concluded and has been fully mitigated and resolved."

CISA is proposing to use the statutory language contained in CIRCIA verbatim to identify the timeframe and associated trigger for providing Supplemental Reports to CISA. As opposed to the statutory language for Covered Cyber Incident Reports and Ransom Payment Reports that contain specific numerical timeframes, CIRCIA requires Supplemental Reports to be submitted "promptly" upon the occurrence of either of the two identified triggering events. CISA defines "promptly" to generally mean what it means colloquially – without delay or as soon as possible.

CISA notes that one of the two potential triggering events for a Supplemental Report has a separate timeframe for reporting mandated in CIRCIA. Specifically, making a ransom payment following the submission of a Covered Cyber Incident Report triggers a requirement for the covered entity to submit a Supplemental Report. Given that CIRCIA requires covered entities to submit Ransom Payment Reports within 24 hours of making the ransom payment, CISA believes it is appropriate to interpret "promptly" to mean no longer than 24 hours after disbursement of the payment.

CISA proposes interpreting "substantial new or different information" as meaning information that: 1) is responsive to a required data field in a Covered Cyber Incident Report that the covered entity was unable to substantively answer at the time of submission of that report or any Supplemental Report related to that incident, or 2) shows that a previously submitted Covered Cyber Incident Report or Supplemental Report is materially incorrect or incomplete in some manner. Together, these two provisions will help ensure that a covered entity has provided to CISA all required information related to a covered cyber incident in a timely fashion and that any material inaccuracies in a previously submitted Covered Cyber Incident Report or Supplemental Report are promptly corrected.

A covered entity's supplemental reporting requirements remain in effect until the covered entity notifies CISA "that the covered cyber incident at issue has concluded and has been fully mitigated and resolved." Although the point at which an incident is concluded and fully mitigated and resolved may vary based on the specific facts of the incident, reaching the following milestones is a good indication that an incident has been concluded and fully mitigated and resolved: 1) the entity has completed an investigation of the incident, gathered all necessary information, and documented all relevant aspects of the incident; and 2) the entity has completed steps required to address the root cause of the incident (e.g., completed any necessary containment and eradication actions; identified and mitigated all exploited vulnerabilities; removed any unauthorized access). For an incident to be concluded and fully mitigated and resolved, a covered entity should have a good-faith belief that further investigation would not uncover any substantial new or different information about the covered cyber incident.

Who May Serve as a Third-Party Submitter

CIRCIA provides a list of entities that covered entities might use to report Covered Cyber Incident Reports or Ransom Payment Reports on the covered entity's behalf. Specifically, CIRCIA states a covered entity that is required to submit a Covered Cyber Incident Report or a Ransom Payment Report "may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm," to submit the required report. This list is simply illustrative examples – and not a closed list of which categories of third parties a covered entity may use to submit CIRCIA Reports on its behalf.

CISA is not proposing limiting the types of organizations or individuals that a covered entity can choose to submit a report on their behalf, especially considering that the responsibility for complying with the regulation remains with the covered entity – even if it uses a third party to submit a report on its behalf. CISA believes that allowing a covered entity the flexibility to determine which party is best situated to submit CIRCIA Reports on its behalf offers value and is thus proposing that a covered entity may use any organization or individual it chooses to submit a CIRCIA Report on its behalf.

Any report submitted by a third party that has not been expressly authorized by the covered entity to submit the report will not be imputed to the covered entity or considered by CISA for purposes of CIRCIA compliance. To better ensure that a report being submitted by a third party is being submitted subject to the express authorization of the covered entity, CISA is proposing requiring the third party to include in the submission an attestation that it has been expressly authorized by the covered entity to submit the report. This likely would be accomplished by requiring a third party to check a box in the online form attesting to this, or some other similar electronic mechanism. As a general legal prohibition against knowingly providing false information to the Federal government exists[20], requiring this attestation from the third party is a sufficient deterrent to prevent individuals or organizations from seeking to submit a CIRCIA Report on behalf of a covered entity without express authorization. CIRCIA makes clear that any enforcement action for noncompliance is to be brought against the covered entity, not a third party that submitted (or failed to submit) a report on the covered entity's behalf. Thus, CISA interprets it to be the covered entity's responsibility to ensure that any CIRCIA Report submitted by a third party on the covered entity's behalf is accurate and to correct any inaccurate or update incomplete information through the submission of any report.

Data and Records Preservation Requirements

Under CIRCIA, any covered entity that submits a CIRCIA Report must preserve data relevant to the reported covered cyber incident or ransom payment in accordance with procedures established in the final rule. To implement this requirement, CISA is to include in the final rule a clear description of the types of data that covered entities must preserve, the period of time for which the data must be preserved, and allowable uses, processes, and procedures.

[20] 18 U.S.C. 1001

CISA is proposing requiring covered entities to preserve a variety of data and records related to any covered cyber incidents or ransom payments reported to CISA in a CIRCIA Report. Specifically, CISA is proposing to require covered entities preserve data and records relating to communications between the covered entity and the threat actor; indicators of compromise; relevant log entries, memory captures, and forensic images; network information or traffic related to the cyber incident; the attack vector; system information that may help identify vulnerabilities that were exploited to perpetrate the incident; information on any exfiltrated data; data and records related to any ransom payment made; and any forensic or other reports about the cyber incident produced or procured by the covered entity. CISA is not proposing that a covered entity be required to preserve copies of all of the exfiltrated data; rather, that a covered entity preserve information related to the data, such as the type and amount of data exfiltrated.

A covered entity that has any of the data or records listed above must preserve those data or records regardless of what format they are in, whether they are electronic or not, located onsite or offsite, found in the network or in the cloud, etc. A covered entity is not, however, required to create any data or records it does not already have in its possession based on this regulatory requirement. The requirement for a covered entity to preserve data or records applies only to the extent the entity already has created, or would be creating them, irrespective of CIRCIA.

CISA is aware that retaining data and records is not without cost. Rather than requiring covered entities to retain all log entries or memory captures from the time of the incident in case any of them may have contained pertinent data, CISA is proposing to limit this to log entries, memory captures, or forensic images that the covered entity believes in good faith are relevant to the incident. CISA is not proposing that a covered entity be required to preserve copies of all data that was exfiltrated during an incident, but rather simply proposes that it preserves information sufficient to understand what type of and how much data was exfiltrated.

CISA is proposing that covered entities that submit CIRCIA Reports must begin preserving the required data at the earlier of either a) the date upon which the entity establishes a reasonable belief that a covered cyber incident has occurred, or b) the date upon which a ransom payment was disbursed, and must preserve the data for a period of no less than two years from the submission of the latest required CIRCIA Report submitted – including any Supplemental Reports. Unless substantial new or different information is discovered or additional actions occur that require the submission of a Supplemental Report, then a commensurate extension of the data preservation timeframe will occur.
CISA is proposing to give covered entities significant flexibility in determining how to preserve the data and records, so long as the preservation method retains all salient details. This may include electronic or non-electronic (i.e., hard copy) storage, onsite or offsite storage, network or cloud storage, and active or cold (i.e., archived) storage. However – there are two limitations on this proposed flexibility. First, CISA is proposing that the covered entity must store the data and records in a manner that allows the data and records to be readily accessible and retrievable, within a reasonable amount of time, by the covered entity in response to a lawful government request. Second, CISA is proposing to require covered entities to employ reasonable safeguards to protect the data and records against unauthorized access or disclosure, deterioration, deletion, destruction, and alteration. These safeguards must include protections against both natural and man-made, intentional and unintentional events, including cyber incidents. NIST Special Publication 1800-25 provides examples of the types of best practices that a covered entity might employ to meet this proposed requirement.

Enforcement

CIRCIA provides a variety of mechanisms for CISA to use if they believe that a covered entity has failed to submit a CIRCIA Report in accordance with any of these regulatory requirements. The potential approaches CISA has to address noncompliance include issuance of an Request For Information (RFI), issuance of a subpoena, referral to the Attorney General to bring a civil action to enforce the subpoena and/or pursue a potential contempt of court, and other enforcement mechanisms to include potential

acquisition penalties, suspension, and debarment. CIRCIA further requires CISA to include in the final rule procedures to carry out these enforcement provisions. The proposed rule details CISA's proposed procedures for each of these enforcement mechanisms.

CISA must consider certain factors when determining whether to exercise any of these enforcement authorities. Specifically, CIRCIA mandates the Director take into consideration the complexity of determining whether a covered cyber incident occurred, and the covered entity's prior interaction with CISA or its understanding of the policies and procedures for reporting for covered cyber incidents and ransom payments, as part of the process for evaluating whether to exercise an enforcement mechanism. CISA is proposing to include this statutory requirement verbatim; and will develop policies and procedures to ensure that the factors are applied similarly to covered entities in similar circumstances.