July 3, 2024

Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency, DHS
Docket number: CISA-2022-0010
circia@cisa.dhs.gov

Re: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements
(Docket# CISA-2022-0010)

The Cloud Service Providers-Advisory Board (CSP-AB) welcomes the opportunity to respond to this Cybersecurity and Infrastructure Security Agency (CISA) Notice of Proposed Rulemaking ("NPRM" or the "Proposal") regarding implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), specifically the statute's covered cyber incident and ransom payment reporting requirements for covered entities.

The CSP-AB is a trade organization representing the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them. Collectively, our members hold over 700 authorizations to operate (ATOs) across all service models and impact levels.

The CSP-AB shares CISA's objective of upholding and enhancing national security, and therefore we are supportive of the implementation of the CIRCIA reporting requirements to ensure early protections are in place to identify malicious cyber campaigns as well as longer-term threat trends. The CSP-AB also applauds CISA for extending the public comment period, reflecting the importance of, and interest in, this NPRM.

In order to best serve the Proposal's objectives, however, we do believe that specific amendments are necessary, primarily regarding the definitions and the breadth of firms that may be captured. We have provided specific comments below, as well as drafting suggestions to ensure the Proposal is as clear and targeted as possible.

Definition of a covered entity

The CSP-AB is concerned that the size-based criteria in § 226.2 is vague and will lead to an overbroad and unnecessary set of firms being captured by the reporting requirements. Instead, CISA should focus on sector-based criteria that clearly identifies entities meeting the statutory and PPD-21 definition of "critical infrastructure" as CIRCIA requires.

Further, we urge CISA to modify two of the IT sector's four sector-based criteria to align with CIRCIA's statutory factors for covered entities. Specifically, CISA should narrow the second criteria (related to "critical software") and the third criteria (related to operational hardware and software) to apply only to entities that knowingly provide or support the critical software or OT hardware or software components to another entity within the nation's critical infrastructure. We believe these amendments will ensure a clear nexus with the critical infrastructure definition of covered entities in the IT sector.

Definition of a substantial cyber incident

The CSP-AB notes the Proposal (§ 226.1.) defines a substantial cyber incident as anything that leads to any of the following:

A. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
B. A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
C. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
D. Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.

As a general matter, we are concerned that this scope is overbroad and will cause reporting to be triggered in a very large number of incidents. Overbroad reporting requirements undermine security by distracting resources and attention of both private and public sector staff, who should be focused on truly material risks and efforts to mitigate those risks. We would accordingly recommend that the definition of a "substantial cyber incident" be amended as follows:

- Include a new requirement, in addition to the four pronged test above, which stipulates that for an incident to meet the threshold it must be related to one of the 16 critical sectors listed in the NPRM.
- Regarding point A of the definition, we would welcome further definitional clarity as to what constitutes a 'substantial loss' in this context. We would also suggest that the word 'material' is added, to become what constitutes a 'substantial *and material* loss'.
- Regarding point C above:
    - While we acknowledge the Proposal's desire to "collect valuable information from a broader set of entities than relying on the sector-based criteria would allow", we nonetheless believe this requirement should be more properly informed by the

core concept of proportionality. The cost to including an overbroad set of reporting firms must be weighed against the benefits of inclusion.
    - Further, we believe this statement should be further qualified to target substantial incidents - we recommend the following amendment "A *serious and material* disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services".
- Regarding point D above:
    - We would welcome clarity that the definition of a substantial cyber incident facilitated by 'a compromise of a cloud service provider' relates to incidents within a CSP's or other third party's area of responsibility.
    - Similar to point C, we believe this statement should be further qualified to target substantial and material incidents - we recommend the following amendment "*substantial and material* unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, *resulting in a significant disruption to or loss of service* 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."

The CSP-AB also encourages CISA to clarify that an incident is not "facilitated through or caused by a compromise of" a third party if it merely occurs on a system hosted by a third party. For an incident to be covered, it must be "facilitated through or caused by a compromise of a cloud service provider, managed service provider, other third-party data hosting provider . . . [*when the incident compromises a control within the third party's area of responsibility*]."

Additionally with respect to the inclusion of cloud service providers in point D, we note that the NPRM acknowledges the important role of FedRAMP, and its requirement that a CSP with an Authorization to Operate (ATO) or a provisional ATO must report suspected and confirmed information security incidents to the FedRAMP Program Management Office within the General Services Administration (GSA), CISA, and the affected agency. Given this already high standard that CSPs are held to, we believe it would be appropriate for CISA to carve out FedRAMP-authorized CSP service covered incidents—this can avoid inefficient duplication of efforts that distract resources from focusing on core security functions. Additionally, if an exemption is not granted, then at a minimum a CIRCIA agreement should be established with GSA to grant reciprocity to FedRAMP incident reporting before the rule is finalized.

Additional items for consideration

The CSP-AB would appreciate further clarity on how collected information will be reported to other government agencies, and the safeguards that CISA has in place to protect this sensitive information. We note that CISA has not described the steps that would be taken to ensure the safeguarding of any personal victim information that is included in a CIRCIA report before it is shared with another government agency. The CSP-AB recommends that CISA provide more

detail on how it would protect this information and further, we encourage CISA to allow covered entities to redact personal information in reports they submit.

We further encourage CISA to consider reducing the requirement to preserve forensic evidence from two years to one-year active storage. This would improve harmonization with M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, which is the required FedRAMP assignment for AU-11 Audit Record Retention. We believe one year to be sufficient to complete forensic analysis of an incident, determine whether an incident is connected to other incidents, and to allow the government time to determine whether it has further interest in the incident report.

We additionally note that disbarment may be a mechanism deployed in cases of non-compliance. While the CSP-AB supports the overarching policy rationale of ensuring the Federal Government does not engage with irresponsible contractors, disbarment is a punitive measure and therefore should only be deployed in cases where a contractor has been proven to repeatedly and intentionally violated reporting requirements. A broad disbarment standard may result in less transparency from federal contractors reporting incidents to CISA if there is no clear standard as to what reports may be referred for federal procurement review.

Finally, The CSP-AB would also welcome explicit clarity from CISA that the requirement in §226.18(c)(3)(v), which prohibits regulators from using information against a covered entity, also extends to employees of the covered entity.

* * *

We thank you for your consideration of our comments on this important topic and would welcome serving as a resource in consideration of this Proposal.

Sincerely,

Laura Navaratnam

Executive Director

The Cloud Service Providers - Advisory Board

lnavaratnam@csp-ab.com

http://csp-ab.com