TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

July 3, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, D.C. 20528

Re: Docket No. CISA-2022-0010

Dear Director Easterly:

TechNet appreciates the opportunity to submit written comments in response to the Department of Homeland Security's (DHS) and the Cybersecurity and Infrastructure Security Agency's (CISA) Notice of Proposed Rulemaking (NPRM) regarding implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. Our membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.4 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

We agree that in order to meet the cybersecurity needs of today's increasingly interconnected digital world, policymakers and industry leaders must focus efforts on building long-lasting public-private partnerships. TechNet is committed to promoting the adoption and use of voluntary, adaptable, risk management-based approaches to meet this changing environment and effectively manage cybersecurity risk.

As CISA works to finalize a rule setting forth regulatory requirements for the implementation of CIRCIA, we urge CISA to properly account for the scope of "covered entities" that are required to report a significant cyber incident, to accurately calibrate the required timing for reporting of a cyber incident, and to appropriately define which instances meet the definition of "covered cyber incident" under CIRCIA. Doing so will best achieve the goal of improving America's

cybersecurity posture and limiting risks to America's economic and national security interests in the years to come.

Scope of "Covered Entity" Under CIRCIA

Under CIRCIA, the term "covered entity" means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21 (PPD-21), that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b).[1] PPD-21 further defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[2]

Furthermore, CIRCIA requires CISA to base its definition of "covered entity" on: (1) the consequences disruption to or the compromise of such an entity would have for national security, economic security, or public health and safety; (2) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and (3) 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.

We urge CISA to appropriately tailor the scope of the definition "covered entity" to ensure it does not encompass broad sectors of the economy at outsized cost with minimal benefits for cybersecurity resilience. Specifically, we believe entities should only be subject to mandatory reporting for their critical functions.

CISA's NPRM suggests that an entire entity, not just an individual facility or function performed by an entity, is covered under CIRCIA's reporting mandate. However, the approach in this proposed rule runs counter to CISA's own work in identifying National Critical Functions, which identified these functions as follows: "the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." This important work confirms that entities may have some operations that are critical, as well as others that do not rise to this threshold. We respectfully urge CISA to refine the proposed rule so that entities are only subject to mandatory reporting for their critical functions.

---

[1] Presidential Policy Directive 21 (PPD-21) identifies 16 critical infrastructure sectors, including Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater Systems.

[2] Id.

We are concerned that an expansive definition of "covered entity," based on the three factors listed in section 2242(b), could envelop nearly all entities that operate in the critical infrastructure sectors of PPD-21.

We support setting an appropriate threshold for these factors consistent with PPD-21 that tailors the scope of "covered entity" to organizations that, if subject to a cyberattack, would have a "debilitating" impact on security, national economic security, or national public health or safety. Doing so will ensure that CISA and the private sector are effectively utilizing their respective resources to address the highest-priority cyber incidents that undermine America's security interests.

Reasonable Belief Required for Reporting of a Covered Cyber Incident

Section 2242(a) requires covered entities that experience a covered cyber incident to report such incident not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.[3] By their very nature, cyber incident responses are based on rapidly-developing fact patterns. We urge CISA to recognize that covered entities may not be able to come to a reasonable belief immediately upon becoming aware of a cyber incident. In crafting such a definition, CISA should also factor in the need of a covered entity to balance its obligations under these reporting requirements as well as conduct internal cyber incident response and investigations to properly assess the magnitude and risk of a cyber incident.

In addition, we urge CISA to interpret the timeframe for reporting cyber incidents and ransom payments to mean "business days," excluding weekends or federal holidays. This will provide additional flexibility for smaller entities that may not have the requisite personnel or ability to generate and file reports over a weekend or a federal holiday. While the proposed timeframe is included in statute, requiring reporting entities to quickly submit reports may result in the submission of unreliable or incomplete reports. CISA should, to the greatest extent possible, identify additional flexibilities in its proposed reporting structure, including allowing entities to file supplemental reports once an incident has been fully resolved or mitigated.

Definition of "Covered Cyber Incident" Under CIRCIA

As defined in CIRCIA, a "covered cyber incident" is a "substantial cyber incident experienced by a covered entity" that meets the criteria listed in Section 2242(c)(2)(A)-(C). These criteria include "substantial loss of confidentiality, integrity, or availability" in information systems or "serious impact on the safety and resiliency" of operations; "disruption of business or industrial operations;" or "unauthorized access or disruption" of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service

[3] P.L. 117-103 (Mar. 15, 2022)

provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise."

In addition, these criteria require consideration of additional factors, including the sophistication or novelty of the tactics used to perpetrate the cyber incident and potential impacts on industrial control systems, and should 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, as well as threats of disruptions that do not result in the actual disruption of a system. We urge CISA to ensure its proposed definition of "covered cyber incident" excludes routine events that lead to services not being available, such as updates to a covered entity's computer systems and incidents not related to the functioning of critical infrastructure. More broadly, the proposed definition should be tailored to avoid the over-reporting of cyber incidents that avoid imposing outsized time and resource burdens on CISA as well as covered entities. We recommend limiting the definition of "covered cyber incident" to "substantial cyber incidents" that directly impact the portion of the covered entity that provides the service or function that makes the entity a covered entity.

In addition, we urge CISA to exclude from the definition of "covered cyber incident" any incidents that do not directly involve U.S. critical infrastructure, even in cases where a company may be considered a covered entity under CIRCIA in other contexts. Without such an exclusion, the proposed rules could encourage reciprocal rules from foreign governments that jeopardize U.S. sensitive data or conflict with foreign data protections and privacy laws. In these scenarios, companies could be at risk of violating provisions of the Data Privacy Framework or other national frameworks such as the General Data Protection Regulation. We urge CISA to utilize existing processes, including but not limited to Cloud Act agreements or the Mutual Legal Assistance Treaty (MLAT) process, to seek information on extraterritorial incidents.

Finally, we urge CISA to provide further clarity regarding the impact thresholds for the definition of "substantial cyber incident." While the current definition of "substantial cyber incident" includes clarification for "substantial loss of confidentiality" and "a serious impact on the safety and resiliency" of a covered entity's operational systems and processes, there is no similar qualifier regarding the impacts of the third and fourth prongs of this definition. To provide greater clarity on these prongs, we urge CISA to incorporate a limiting threshold regarding impact level or, through guidance, provide a more exhaustive list of examples of the types of incidents it views as likely to be reportable in order to aid covered entities in understanding their reporting obligations.

Conclusion

We appreciate the opportunity to submit comments to CISA's Proposed Rule regarding the implementation of CIRCIA. We stand ready to serve as a resource to

you in your continued examination of this important issue and your continued efforts to improve America's cybersecurity posture.

Sincerely,

Linda Moore
President and CEO