Before the
Cybersecurity and Infrastructure Security Agency
Washington, D.C. 20528

In the Matter of	)	
	)	
Cyber Incident Reporting for Critical Infrastructure Act of 2022	)	Docket ID: CISA-2022-0010
	)	

COMMENTS OF NTCA–THE RURAL BROADBAND ASSOCIATION

NTCA–The Rural Broadband Association ("NTCA")[1] hereby submits these comments in response to the Request for Information ("RFI")[2] released by the Cybersecurity and Infrastructure Security Agency ("CISA") in the above-captioned proceeding. CISA issued the RFI in response to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), which directs CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransom payments to CISA.[3] CISA noted that these reports are intended to allow CISA to rapidly deploy resources and render assistance to victims of cyber incidents while also identifying methods used to perpetrate those incidents and share that information with the public to allow entities to take steps to mitigate against similar incidents.[4] NTCA appreciates the steps CISA is taking to obtain public feedback regarding the

[1] NTCA–The Rural Broadband Association represents approximately 850 independent, community-based companies and cooperatives that provide advanced communications services in rural America and more than 400 other firms that support or are themselves engaged in the provision of such services.

[2] Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, Docket ID: CISA-2022-0010 (Sep. 12, 2022).

[3] 87 Fed. Reg. No. 175 at 55834 (Sep. 12, 2022).

[4] *Id.*

reporting requirements and welcomes the opportunity to provide the following recommendations in response to questions raised in the RFI.

I. "Covered Cyber Incident" Should Be Defined As a Confirmed Incident That Significantly Disrupts a Provider's Core Functions.

As an initial matter, consistent with CISA's intended uses of reports filed pursuant to CIRCIA, NTCA encourages CISA to define "covered cyber incident" to include only confirmed incidents that significantly disrupt a provider's ability to operate core functions. CISA should specifically exclude attempts to disrupt that service. By way of example, a cyber incident that significantly endangers public safety by disrupting the provider's core, transport, and/or access networks would be considered a covered incident.[5] An incident of this type would severely impair the provider's customer services as well as negatively impair the provider's business operations if those operations utilize some of the same network elements for access to the Internet.

Alternatively, if an incident results in access to customers' or employees' personal information, without disrupting the provider's core, transport, and/or access networks, the provider must already report the unlawful access to multiple other agencies, including the Federal Communications Commission ("FCC") and state regulators.[6] Accordingly, reporting the same incident to CISA would be contrary to CIRCIA's intention of avoiding duplicative reports

[5] Network outages caused by an incident unrelated to cybersecurity, such as a fiber cut caused by construction crews, should not by subject to cyber incident reporting requirements as they are already subject to FCC Network Outage Reporting System requirements. *See* https://www.fcc.gov/network-outage-reporting-system-nors.

[6] *See* 47 U.S.C. § 222(h)(1) and 47 C.F.R. § 64.2011. Notably, the FCC's rules require telecommunications providers to disclose any breach of customers' proprietary information to the U.S. Secret Service and the FBI. Furthermore, the FCC's rules prohibit telecommunications providers from disclosing the breach to the public until seven business days have passed following notification to the U.S. Secret Service and FBI. Accordingly, the Commission's rules would likely need to be amended to allow telecommunications providers to report such breaches to CISA any earlier than seven business days following notification to the U.S. Secret Service and FBI.

and take away valuable time from both CISA and the reporting entity without resulting in more secure critical infrastructure or providing any other benefit.

Including attempted cyber incidents that do not disrupt a provider's core, transport, and/or access networks would also result in far too many incident reports for CISA to be able to act on immediately. Neither inundating CISA with voluminous reports of incidents that are unsuccessful nor requiring providers to devote time away from maintaining their operations to prepare reports that would not benefit others would fulfill CIRCIA's purpose of deploying resources effectively and rendering assistance to victims of cyber-attacks. Accordingly, both the provider's and CISA's resources would be better invested in addressing and responding to attacks that *do* impact providers' operations.

Cyber incident reports also should not be required until a minimum of 72 hours after a covered entity has confirmed a cyber-attack disrupting the provider's core, transport, and/or access networks has occurred. Covered entities need time to investigate and mitigate an intrusion before reporting to the government. This will also result in more effective incident reports as the reporting entities will have a clearer picture of the incident, which will make CISA better aware of the tactics used to carry out the cyber-attack.

II. Covered Entities Should Only be Required to Report a Supply Chain Compromise that Results in a Covered Cyber Incident.

CISA also seeks comment on the meaning of supply chain compromise, consistent with section 2240(7) of CIRCIA, which directs CISA to define "supply chain compromise" in the context of an incident that takes place within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can

occur at any point during the life cycle.[7] NTCA recommends CISA define supply chain compromise as a covered cyber incident where the covered entity determines the attack was against goods, services, hardware, software, or cloud-based services provided by one or more suppliers instead of the covered entity's core, transport, and/or access networks. By way of example, these incidents may include, but are not limited to, credential compromise due to a vulnerability in a Software-as-a-Service ("SaaS") provider; hard-coded administrative credentials; loss of availability due to a provider outage; and lateral movement into the business systems from a connection to a vendor network.

NTCA further encourages CISA not to require covered entities to report supply chain incidents that take place on third party providers' systems or products. Instead, incident reporting responsibilities should lie solely with the entities whose core operations were compromised by malicious actors, not providers of intermediary transport or contractors. In those cases, affected entities are merely the consumer of the product or service and do not have any control over what may have led to the incident or responses to the incident. Furthermore, such entities likely know very little, if anything, regarding the incident and therefore would be unable to provide information in an incident report that could help prevent a similar incident from occurring or from harming critical infrastructure, as intended by CIRCIA. Moreover, such reports could be duplicative and confusing to the extent that multiple providers report with respect to the same incident occurring on only one of their networks. Instead, such intermediaries should only be subject to reporting requirements when their own core, transport, and/or access networks are disrupted due to a covered cyber incident.

[7] CIRCIA sec. 2240(17).

To help minimize the impact that widespread supply chain attacks can have on the public, NTCA encourages CISA to share anonymized information provided in cyber incident reports with software, hardware, and cloud providers and with member Information Sharing and Analysis Centers ("ISACs") as appropriate as soon after receiving the reports as CISA can provide an informed awareness to these entities. Sharing key information regarding the method and scope of the compromise with equipment, software and cloud providers and ISACs will allow providers whose products were compromised to quickly make targeted modifications to their products to address the identified vulnerabilities and thereby reduce the number of entities affected by the same vulnerability. Additionally, a publicly released quarterly trends report that does not include confidential or proprietary data about the covered entities affected would help others adapt to an ever-changing threat landscape.

III. Cyber Incident Reports Should Contain Only the Core Information Needed to Mitigate the Cyber Incident and Have the Ability to be Completed Without the Need to Create an Account or Install Software or Hardware.

In response to CISA's request for comment on how covered entities should submit cyber incident reports, including the information that should be included in the reports, NTCA recommends reports be electronically submitted using an online form that requests only the information needed to receive assistance investigating the incident from government agencies and to mitigate against future incidents.[8] Utilizing an online form such as the one currently in place for voluntary reporting of cyber incidents to CISA[9] would result in consistent data that would better allow CISA to identify and share "information about indicators of compromise,

[8] 87 Fed. Reg. No. 175 at 55834, Sec. II.

[9] *See* CISA Incident Reporting System, available at https://us-cert.cisa.gov/forms/report.

tactics, techniques, [and] procedures" critical to mitigating future cyber-attacks while also better informing the reports required to be made by CISA pursuant to CIRCIA.[10]

To ensure CISA can act quickly and responsively upon the information reported, and covered entities can dedicate the critical hours and days immediately following a cyber-attack to mitigating damage and restoring operations, incident reports should only include core information necessary to allow CISA or other federal agencies to offer assistance to the reporting entity and to help other entities avoid or mitigate a similar attack.[11] Limiting the scope of information that must be reported, and correspondingly, the time necessary to complete the incident report, is especially important for small entities, many of which do not have a dedicated security professional to respond to an incident. Instead, the task of identifying the source of the cyber-attack and restoring network operations would rest on a single employee.[12] This employee would also be the only one with knowledge of the information necessary to be included in a cyber incident report. Accordingly, any time that employee devotes to completing the incident report is time away from assessing and mitigating the damage to the provider's network and restoring services.

To balance small entities' competing needs and capabilities, NTCA encourages CISA to develop rules that would allow small entities additional time to submit an incident report. Specifically, CISA should allow sufficient time for small entities to recover from the incident

[10] 87 Fed. Reg. No. 175 at 55833, Summary.

[11] In the case of a ransomware attack, for instance, valuable information would be initial entry method, ransomware variant, and ransom demand.

[12] Some small entities do not have any security professionals on staff capable of responding to a cyber incident and must rely on a third party to assist with a forensic analysis to identify the cause and depth of the attack. Depending on the distance between the entity and the third party, two or three days might pass before the third party arrives on site to begin this analysis.

and complete their forensic analysis of the event prior to submitting a cyber incident report. This would allow small entities the time needed to focus first on mitigating the damage and restoring services and result in a more informative and useful cyber incident report.

NTCA further recommends that access to the cyber incident reporting form not require any software to be installed or a password. Additionally, instead of requiring samples of malicious code to be included in any report, NTCA recommends CISA request either a screen shot of the source code or a text file containing the source code. This would provide CISA with the information necessary to respond to the incident without putting the impacted provider at risk of providing information proprietary and confidential to its operations as would be the case if the source code was embedded into the affected provider's system. Due to the highly sensitive nature of the information to be reported, NTCA also recommends that the information submitted be anonymized upon transmission and treated confidentially.

Finally, NTCA encourages CISA to allow Information Sharing and Analysis Centers ("ISACs") to have the option of submitting any reports required by CIRCIA and adopted pursuant to this proceeding to CISA. Thus, while CIRCIA allows covered entities to submit required reports using a third party such as an ISAC,[13] and CyberShare: The Small Broadband Provider ISAC, for example, could provide a valuable and timely method of two-way information sharing between small broadband providers experiencing a covered incident and CISA, each ISAC should have the ability to determine whether and under what terms the ISAC can fulfill this role.

[13] *See* CIRCIA sec. 2242(d).

IV. A "Reasonable Belief" That a Covered Incident Has Occurred Must Not Depend Upon the Installation or Use of Additional Hardware or Software.

CIRCIA specifies that the timeline for covered entities to report a cyber incident is triggered when the entity "reasonably believes" that a covered cyber incident has occurred.[14] CISA seeks comment on what constitutes a reasonable belief that a covered cyber incident has occurred.[15] NTCA suggests this could be defined as confirmation by the covered entity that a credible, verifiable, and actionable compromise of the entity's core, transport and/or access networks has occurred. Perhaps just as importantly, CISA should not require any entities to purchase or install additional systems to monitor the defined criteria.

V. Information Reported Pursuant to CIRCIA Must be Protected.

Due to the highly sensitive nature of the information reported, ensuring that information reported is not shared with or accessible to anyone else, except when anonymized of all information that could identify the reporting entity, will be essential. To fulfill this critical objective, NTCA urges CISA to adopt rules requiring the destruction of reporting entities' identifiable information annually unless such information is the subject of an ongoing investigation.[16]

Any rules adopted in this proceeding should also prohibit the sharing of reporting entities' names with other agencies. Sharing reporting entities' names is not necessary to fulfill CIRCIA's goal of reducing the risk of similar cyber incidents occurring across sectors. Reporting entities also should not be required to report customer information or other personally

[14] CIRCIA sec. 2242(a)(1)(B).

[15] 87 Fed. Reg. No. 175 at 55835.

[16] *See, e.g.*, CIRCIA sec. 2245(a)(2) (aggregated reports that do not contain identifiable company information would not be subject to disposal).

identifiable information. Finally, CISA must ensure that information provided pursuant to CIRCIA cannot be used for punitive measures, including punishment toward the reporting entity. Sharing reported information with other agencies must be used solely for the purpose of helping to better secure those agencies' own networks and to assist the reporting entity in recovering from the identified cyber-attack.

VI. Conclusion

CIRCIA offers an important avenue for CISA to identify modes of cyber-attacks more rapidly and to share critical information about those attacks with other agencies and the public to better secure critical infrastructure. To effectively carry out this important directive, however, CISA must clearly identify and collect only the core information necessary to achieve CIRCIA's objective, ensure the timing and content of cyber incident reports do not delay covered entities' ability to assess and respond to cyber-attacks, and provide strong protections to safeguard the information contained in cyber incident reports.

Respectfully submitted,

By: */s/ Michael Romano*
Michael Romano
Tamber Ray

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203

(703) 351-2000