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

In the Matter of	)	
	)	Docket No. CISA-2022-0010
Cyber Incident Reporting for Critical	)	
Infrastructure Act of 2022	)	

COMMENTS
OF
NTCA–THE RURAL BROADBAND ASSOCIATION

By: /s/ *Michael R. Romano*
Michael R. Romano
Senior Vice President –
Industry Affairs & Business Development
mromano@ntca.org

By: /s/ *Tamber Ray*
Tamber Ray
Director of Policy
tray@ntca.org

By: /s/ *Meghan O'Brien*
Meghan O'Brien
Policy Coordinator
mobrien@ntca.org

July 3, 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CIRCIA offers an important avenue for CISA to identify modes of cyber incidents more rapidly and to share vital information about those incidents with other critical infrastructure providers. When carrying out this important directive, however, CISA must consider the burden of the proposed reporting and record retention requirements on small communications providers and identify methods of harmonizing CISA's rules with other incident reporting requirements in order to minimize the burden on these small entities. As described in these comments, CISA can do so while still obtaining pertinent information from these providers regarding cyber incidents that can be quickly evaluated and disseminated.

If CISA chooses to subject small communications providers to CIRCIA's reporting requirements, CISA should at a minimum: (1) limit the information required to be reported by these small entities to the information currently requested in CISA's voluntary cyber incident reporting form; and (2) require only one Supplemental Report to be filed within 30 days of filing a Covered Cyber Incident Report (that requires only the details in (1)) and only if the Covered Cyber Incident Report did not include all of the required information. These limitations will alleviate the impact of any reporting requirements on small communications providers, align the reporting requirements more closely with other federal reporting requirements, and allow small communications providers to focus their limited resources on responding to and recovering from a cyber incident.

Defining the scope of cyber incidents, including supply chain or other third-party cyber incidents, that must be reported in a manner consistent with prior federal directives and guidelines will reduce confusion, overreporting, and burdensome overlapping reporting requirements for the same incidents. This will also help fulfill CIRCIA's directive that CISA has

the ability to immediately review and rapidly disseminate cyber threat indicators and defensive measures to appropriate stakeholders. Accordingly, NTCA urges CISA to require covered entities to file a CIRCIA Report only after the entity has confirmed a cyber incident has occurred and the incident is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety. NTCA further recommends that information to be reported pertaining to supply chain or other third-party incidents be limited to entities whose core operations were compromised and that the information that must be reported include only information specific to the impact on, and method of entry applicable to, that entity's operations.

NTCA further recommends CISA limit the requirement that covered entities maintain data and records pertaining to a reported incident to one year and encourages CISA to focus the retention requirements on information critical to identifying threat indicators and defensive measures.

CISA can ensure CIRCIA's directive that entities be exempt from CIRCIA reporting requirements where they must file substantially similar information in a substantially similar timeframe with other federal agencies is not rendered meaningless by defining the timeline for reporting and the information that must be reported in a manner that reflects other federal incident reporting requirements for critical infrastructure providers.

Additionally, the highly sensitive and proprietary nature of the information to be collected necessitates that any information collected pursuant to CIRCIA will by default be treated as confidential, not subject to Freedom of Information Act ("FOIA") and protected against unauthorized access or disclosure.

Finally, NTCA encourages CISA to leverage more directly Information Sharing and Analysis Centers ("ISACs") as an effective method of quickly disseminating threat information to critical infrastructure providers.

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

In the Matter of	)	
	)	
Cyber Incident Reporting for Critical Infrastructure Act of 2022	)	Docket No. 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 Notice of Proposed Rulemaking ("NPRM")[2] released by the Cybersecurity and Infrastructure Security Agency ("CISA") in the above-captioned proceeding. CISA issued the NPRM 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] NTCA filed comments in response to the Request for Information in this proceeding and welcomes the opportunity to further participate in this rulemaking.[4]

[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] *Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements*, Cybersecurity and Infrastructure Security Agency, Dept. of Homeland Security, Docket No. CISA-2022-0010 (Apr. 4, 2024).

[3] 6 U.S.C. § 681, Pub. L. 117-103, as amended by Pub. L. 117-263 (Dec. 23, 2022).

[4] Comments of NTCA–The Rural Broadband Ass'n, *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Docket ID: CISA-2022-0010 (filed Nov. 14, 2022).

I. STATEMENT OF INTEREST

NTCA has been actively engaged in cybersecurity matters facing small and mid-sized broadband providers for years through public-private partnerships with federal agencies, Federal Communications Commission ("FCC") initiatives, and by providing valuable resources to members to help them increase their cyber posture. Over the past several years, on behalf of members, NTCA has been fortunate to participate in multiple working groups of the Information and Communications Technology Supply Chain Risk Management ("ICT SCRM") Task Force, the Communications Sector Coordinating Council Executive Committee, and the Communications Sector Reliability and Interoperability Council ("CSRIC"). In 2020, recognizing the importance of cyber information sharing especially among small broadband providers, NTCA established CyberShare: The Small Broadband Provider ISAC ("CyberShare"), a cyber and physical security information sharing platform for small broadband providers. Currently, more than 100 facilities-based small broadband providers participate in CyberShare, and most participants are involved in the day-to-day operation and protection of their company's network. CyberShare offers participants a daily report that identifies key security incidents, events, and vulnerabilities relevant to small broadband providers; a weekly technical report that describes active exploits and mitigation techniques; and bimonthly video conferences that allow members to discuss current threats, mitigation measures, and best practices. The video conferences also routinely feature a guest speaker from industry or government. For example, in February 2024, CyberShare participants received a briefing from CISA's Associate Director for China Operations on Volt Typhoon. NTCA also provides free

cyber resources for small broadband providers and consumers through Cyberwise,[5] which is available on NTCA's website. Furthermore, NTCA recognizes members who are demonstrating a commitment to securing their networks, assets, and sensitive customer information, along with a commitment to ongoing improvement in their cybersecurity measures, with a Cyber Champion Award.

NTCA members have also actively extended their cybersecurity practices by utilizing CISA's resources, offering cyber training for members of their community, and by participating in the ICT SCRM Task Force and CSRIC. For instance, Marne Elk Horn in Walnut, Iowa hosted CISA's Region 7 director for an employee tabletop exercise and utilizes CISA's free weekly vulnerability scan, in addition to participating in CyberShare and hiring outside experts to help defend its network against cyber threats. NineStar Connect in Greenfield, Indiana has teamed up with Telcom Insurance Group to offer free cyber training sessions to their community twice a year, while both Premier Communications in Sioux Center, Iowa and Blue Valley Technologies in Home, Kansas have been actively involved in the ICT SCRM Task Force for several years, and S&T Telephone Cooperative in Brewster, Kansas provided a valuable small broadband provider perspective as a member of the CSRIC VIII Working Group on Managing Software and Cloud Services Supply Chain Security for Communications Infrastructure. Additionally, NTCA member company Highline Services LLC was recently appointed to serve on CSRIC IX.

NTCA supports CIRCIA's objective of ensuring CISA receives timely information about cyber incidents that can be quickly digested and shared with other critical infrastructure entities to help guard against similar incidents; however, this objective can and must be balanced against

[5] *See* "Resources to Help You Be Cyberwise," https://www.ntca.org/member-services/be-cyberwise.

small broadband providers' ability to collect and report information about the incident (while also proactively responding to such incidents and doing so with the very same staff or outside experts doing the reporting) along with CISA's ability to collect and quickly interpret and disseminate information about threat actors and their tactics. As written, the breadth of incidents that must be reported, as well as the vast details that CISA proposes must be reported, would impede CIRCIA's goal of disseminating threat information quickly and will necessitate covered entities' focus on reporting in lieu of risk management and recovery. This is especially true for small communications providers, most of whom fall well below the Small Business Administration ("SBA") threshold for a small business, and who often rely upon outside experts to assist with incident response and recovery in the aftermath of a cyber incident.

II. CISA SHOULD MINIMIZE THE REPORTING BURDEN FOR SMALL COMMUNICATIONS PROVIDERS.

CIRCIA directs CISA to adopt rules requiring "covered entities" to report "covered cyber incidents" to CISA in a manner and with content that will allow CISA "upon receiving" a report to "immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures."[6] While CIRCIA also directs CISA to provide certain reports to Congress,[7] the basis of those reports and the information to be collected for such reports is not separate or different from the information to be collected for this purpose.

[6] CIRCIA sec. 2245(a)(2)(A).

[7] *Id.,* sec. 107.

To begin with, CIRCIA defines a covered entity only as "an entity in a critical infrastructure sector" and directs CISA to determine the scope of entities within those critical infrastructure sectors that will be subject to CIRCIA reporting requirements.[8] Accordingly, with respect to the communications sector, CISA proposes to define a "covered entity" as "*any entity* that provides communications services by wire or radio communications … to the public, business, or government" including "both one-way communications service providers (e.g., radio and television broadcasters, cable television and satellite operators) and two-way communications service providers (e.g., telecommunications carriers; submarine cable licensees; fixed and mobile wireless service providers, VoIP providers, internet service providers), regardless of size.[9]

With respect to a covered cyber incident, CIRCIA specifies only that the incident must be "substantial," and directs CISA to fully define and identify the criteria that must be met for a covered cyber incident.[10] Accordingly, CISA further proposes to define a covered cyber incident as a substantial cyber incident that results in any of the following: (1) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network; (2) a serious impact on the safety and resilience of a covered entity's operational systems and processes; (3) a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or (4) 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, managed service provider, other

[8] *Id*., sec. 2240(5).

[9] NPRM, 89 FR at 23686.

[10] CIRCIA sec. 2240(4).

third-party data hosting provider, or by a supply chain compromise ("Covered Cyber Incident").[11]

The proposed rules would require covered entities to report a Covered Cyber Incident within 72 hours after the entity reasonably believes a Covered Cyber Incident has occurred; a Ransom Payment Report within 24 hours after making a ransom payment; or a Joint Covered Cyber Incident and Ransom Payment Report within 72 hours following a Covered Cyber Incident that resulted in a ransom payment.[12] Finally, covered entities would be required to file a Supplemental Report "promptly," which CISA defines as within 24 hours, if "substantial new or different information becomes available," including information that was not included but was required to be provided in a Covered Cyber Incident Report.[13] (The "Covered Cyber Incident Report", "Ransom Payment Report", "Joint Covered Cyber Incident and Ransom Payment Report", and the "Supplemental Report" are hereinafter collectively referred to as "CIRCIA Reports.")

As described in Section III *infra*, the proposed reporting requirements are vast, time consuming, and costly even for large companies – for small companies the burden is compounded exponentially. This burden is directly contrary to Congress' imperative to avoid quantity over quality in the reporting and processing of data and to ensure small and medium-sized businesses are not burdened with unnecessary reporting requirements.[14]

---

[11] NPRM at 23662-23663.

[12] *Id*. at 23725.

[13] *Id*. at 23726.

[14] Remarks by Congressman Swalwell, "Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking," U.S. House of Representatives Committee on Homeland Security, May 1, 2024, https://homeland.house.gov/hearing/surveying-circia-sector-perspectives-on-the-notice-of-proposed-rulemaking/ ("Surveying CIRCIA Hearing").

The smallest NTCA member company, for instance, employs a staff of two, and the largest just over 400. Notably, even the largest member company has far fewer employees than the 1,500 employee level identified by the Small Business Administration ("SBA") as a small business for wired telecommunications carriers.[15] NTCA members also have an average of 5,494 residential and 551 business fixed broadband connections in service and an average of 10,231 serviceable locations within their service areas.[16] On average, NTCA member companies' customer density is approximately seven subscribers per square mile. By contrast, larger telecommunications companies, on average, serve 130 customers per square mile.

Notably, CIRCIA's requirements will affect not only small providers but their customers as well. The customers NTCA members serve are those in the most sparsely populated, highest-cost rural areas of the country and they depend upon these small broadband providers for critical connectivity to the rest of the world. If a small provider becomes a victim of a cyber and/or ransomware attack, lengthy and duplicative reporting requirements will direct the provider's focus away from addressing the needs of its network and customers, which could impact not only the provider's bottom line but customers' as well. With small businesses "already being three times more likely to be targeted by cybercriminals than larger companies" and the "total cost of cybercrimes to small businesses reach[ing] $2.24 billion in 2021,"[17] the impact of time-

[15] *See* Small Business Size Standards by NAICS Industry, sector 517, https://www.ecfr.gov/current/title-13/chapter-I/part-121#121.201.

[16] NTCA 2023 Broadband/Internet Survey Report, p. 1, https://www.ntca.org/sites/default/files/documents/2023-12/2023%20Broadband%20Survey%20Report%20FINAL.pdf.

[17] Goldstein, Eric, "Accelerating Our Economy Through Better Security: Helping America's Small Businesses Address Cyber Threats," CISA, May 2, 2023, https://www.cisa.gov/news-events/news/accelerating-our-economy-through-better-security-helping-americas-small-businesses-address-cyber.

consuming reporting requirements would not only be compounded for small communications providers but also for their customers who may be small businesses themselves.

A. CISA should minimize the information small communications providers must include in a Covered Cyber Incident Report.

Unlike other types of covered entities, CISA proposes not to provide an exception for communications providers that qualify as a small business under SBA standards, or any other standard for measuring a small business, based on the concern that disruption or compromise of communications systems "could significantly impact national security, economic security, and public health and safety"[18] and "will directly affect the security and resilience of critical infrastructure within and across numerous sectors."[19] By comparison, CISA does propose to exempt entities in the Emergency Services Sector who serve a population of less than 50,000 on the basis that "it makes sense to focus CIRCIA covered cyber incident and ransom payment reporting requirements on the larger, better-resourced entities."[20] Yet CISA describes the Emergency Services Sector as "the first line of support for nearly all critical infrastructure, and a failure or disruption in these services could result in significant harm or loss of life, major public health impacts, long term economic loss, and cascading disruptions to other critical infrastructure."[21] Notably, CISA also recognized that Emergency Service entities generally are not subject to any other federal cyber incident reporting requirements, while even small

[18] NPRM, 89 FR at 23686.

[19] *Id.*

[20] *Id*. at 23688.

[21] *Id*.

communications providers are subject to certain federal cyber reporting requirements as described in Attachment 1 of these comments.[22]

CISA further concluded that including Emergency Services Sector entities that serve a population of at least 50,000 in CIRCIA Reporting requirements is important because, without any other federal cyber incident reporting requirements for these entities, CIRCIA is the only method for CISA to gain information about Covered Incidents affecting these entities.[23] By contrast, communications providers of all sizes are required to report certain incidents to the FCC and the FCC shares the information reported with the FBI/Secret Service and with other federal and state agencies, depending upon the type of report.[24] CISA could work with the FCC to gain access to the same information and work directly with the provider impacted if additional information was needed to be able to alert other critical infrastructure providers to a cyber threat or vulnerability.

This discordance between the two sectors makes no practical sense; the same logic that warrants an exemption for smaller operators in the Emergency Services Sector applies with equal force to smaller communications providers, especially when these communications providers are already subject to federal reporting requirements. The only difference then for choosing to include all entities within the Communications Sector while exempting entities that serve smaller communities in the Emergency Communications sector is that a disruption or compromise of a

[22] *Id*.

[23] *Id*.

[24] *See Data Breach Reporting Requirements*, Report & Order, WC Docket No. 22-21 (rel. Dec. 20, 2023) at ¶ 28 ("We require telecommunications carriers to notify the Commission of a breach in addition to notification to the Secret Service and FBI.); *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Second Report & Order, PS Docket No. 15-80 (rel. March 18, 2021).

communications system "could significantly impact national security."[25] Therefore, if CISA nevertheless chooses to subject small communications providers to CIRCIA Reports, CISA's basis for doing so – that a disruption or compromise of any communications provider's system "could significantly impact national security" – necessitates that an "impact to national security" be a prerequisite to any Covered Cyber Incident. Additionally, CISA should at a minimum: (1) significantly reduce the information to be reported by these small entities; and (2) establish a clear ending for small communications providers' obligation to submit a Supplemental Report.[26]

With respect to the information to be provided in a Covered Cyber Incident Report, small communications providers should not be expected or required to submit the same extensive and detailed information proposed in the NPRM as other covered entities, nearly all of whom exceed the SBA small business standard. Instead, NTCA urges CISA to limit the information small communications providers must report to those elements currently requested by CISA for voluntary cyber incident reports:

1. Incident date and time
2. Incident location
3. Type of observed activity
4. Detailed narrative of the event
5. Number of people or systems affected
6. Company/Organization name
7. Point of Contact details

[25] NPRM, 89 FR at 23686.

[26] CISA could apply the SBA definition of small business as a method of identifying those that qualify as a small communications provider.

8. Severity of event

9. Critical Infrastructure Sector

10. Anyone else you informed

CISA describes these elements as "information … that could help mitigate current or emerging cybersecurity threats to critical infrastructure."[27] Significantly, this information is also quite similar to the details identified in CIRCIA as required to be included in Covered Cyber Incident Reports "to the extent applicable and available."[28] Additionally, CISA has identified the information above as necessary to allow CISA "to render assistance and provide a warning to prevent other organizations and entities from falling victim to a similar attack" and "critical to identifying trends that can help efforts to protect the homeland."[29] Accordingly, requiring small communications providers to submit this information in lieu of the vastly detailed information proposed in the NPRM will allow CISA to fulfill CIRCIA's objective without imposing an unnecessary burden on these small entities – whether through uncertainty regarding the types of incidents that must be reported or the details that must be included in reports. Moreover, this approach mitigates the likelihood of overreporting in the face of potential enforcement action if the provider concludes an incident is not "substantial" and as a result does not file a Covered Cyber Incident Report or if a small communications provider does file a Covered Cyber Incident Report but is unable to provide all of the details required, either within the 72-hour filing window or later.

---

[27] "Sharing Cyber Event Information: Observe, Act, Report," CISA, Apr. 2022, https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf

[28] CIRCIA sec. 2242(c)(4).

[29] "Sharing Cyber Event Information," n. 27, *supra.*

To further minimize the reporting burden on small communications providers while also providing much-needed clarity to CIRCIA's reporting requirements, NTCA recommends CISA modify the Supplemental Report filing obligation for small providers to require only one Supplemental Report within 30 days following submission of a Covered Cyber Incident Report and only if the provider was unable to provide all of the information required for a small provider Covered Cyber Incident Report (see above).

Allowing small communications providers to focus first on mitigating damage and restoring services following a cyber incident rather than ongoing, perhaps daily, reporting requirements will benefit both CISA and these small providers. A single Supplemental Report that contains any information not included in the Covered Cyber Incident Report will also contain more information that may be relevant to preventing similar attacks than scattered daily reports that contain few details. Furthermore, clarity regarding the content and timing for a Supplemental Report will eliminate the likelihood of overreporting due to the risk of enforcement action if the provider's interpretation of "substantial new or different information" happens to be different than CISA's.

NTCA further encourages CISA to continue making small communications providers aware of the free tools offered by CISA to help bolster companies' cybersecurity defenses, including the agency's CyberSentry Program, Cyber Hygiene Vulnerability Scanning service, and the Ransomware Vulnerability Warning Pilot established by CIRCIA. As CISA has noted, recovering from a ransomware attack costs a business an average of $1.85 million.[30] By

[30] Radesky, Sandra, "Cyber Hygiene Helps Organizations Mitigate Ransomware-Related Vulnerabilities," CISA, Apr. 25, 2024, https://www.cisa.gov/news-events/news/cyber-hygiene-helps-organizations-mitigate-ransomware-related-vulnerabilities.

contrast, CISA reports that organizations participating in CISA's free vulnerability scanning "typically reduce their risk and exposure by 40% within the first 12 months and most see improvements in the first 90 days."[31] Accordingly, small providers with minimal resources could benefit from additional support to reduce the risk of cyber incidents before they happen in lieu of time consuming reporting burdens in the aftermath of a cyber incident.

B. The requirement to file a Supplemental Report should be adjusted to provide clarity and not impede small providers' ongoing operations.

NTCA appreciates CISA's recognition that a covered entity might not have the ability to provide all of the information required for a Covered Cyber Incident Report within the 72-hour timeframe specified by CIRCIA[32] given the likelihood that the entity is still analyzing and recovering from the incident at the time the Covered Cyber Incident Report is due; however, the NPRM's proposal to require covered entities to submit ongoing Supplemental Reports "promptly" if "substantial new or different information becomes available"[33] would impose a significant burden on small providers' ability to focus upon incident recovery and analysis without commensurate benefit to CIRCIA's objective.

Notably, the Verizon Data Breach Investigations Report found "it takes around 55 days to remediate 50% of [ ] critical vulnerabilities once their patches are available."[34] The need to file multiple Supplemental Reports during this critical period would take small communications providers' limited resources away from: (1) identifying that a patch is available – due to the fact

---

[31] *Id*.

[32] CIRCIA, sec. 2242(a)(1)(A).

[33] NPRM, 89 FR at 23726.

[34] Verizon 2024 Data Breach Investigations Report, p. 21, http://verizon.com/dbir.

that these small providers are not always notified, or at least not the first to be notified, that a patch is available; (2) downloading the patch; and (3) ensuring the patch does not disrupt the provider's operations. By contrast, the details available while entities are downloading patches and conducting remediation are unlikely to contain time sensitive or critical information about an incident that, if shared, could reduce the likelihood of similar incidents. Furthermore, CIRCIA only requires "an update or supplement to a previously submitted covered cyber incident report if *substantial new or different information* becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report…."[35] To ensure small communications providers can focus on recovering from an incident rather than ongoing reporting requirements, NTCA encourages CISA to take several steps to reduce the burden of filing a Supplemental Report.

First, CISA should remove the request for information regarding "the current phase of incident response efforts at the time of reporting."[36] The incident response phase will inevitably change throughout an entity's restoration and recovery efforts. The specific phase of incident response is also irrelevant to alerting other entities on how to reduce their risk of a similar incident. Second, NTCA encourages CISA to specify that small communications providers need only file a single Supplemental Report (rather than ongoing reports) within 30 days of the date on which the provider submitted its initial Covered Cyber Incident Report and only if the provider was unable to include all of the information required in such an initial report (which once again should itself be limited to the information described above for small communications

[35] CIRCIA sec. 2242(a)(3) (emphasis added).

[36] *See* NPRM, 89 FR at 23720.

providers). This would allow covered entities to conduct a root cause analysis prior to submitting the Supplemental Report, which would in turn provide CISA with more useful information. This would also eliminate uncertainty regarding what constitutes "substantial new or different information," along with the need to report anything and everything out of fear of enforcement action should the provider interpret "substantial new or different" in a manner different from CISA.

This timing and the requirement to submit only a single Supplemental Report will further align these rules with the FCC's Network Outage and Reporting System ("NORS") requirements, which require communications providers to file a final report no later than thirty days after discovering the outage.[37] Providing consistency across different agencies not only benefits covered entities by eliminating different reporting requirements and deadlines across multiple federal agencies but is also consistent with the directive in the National Security Memorandum on Critical Infrastructure Security and Resilience that "[e]fforts to safeguard critical infrastructure will be fully integrated and coordinated with complementary Federal policies…."[38]

Providing a definitive filing date and requiring only clear, limited content will also eliminate the uncertainty, followed by likely overreporting, regarding whether circumstances such as identifying additional accounts accessed by the incident – which can take months or longer – constitutes "substantial new or different information" and at what point the provider's

[37] 47 C.F.R. § 4.9.

[38] National Security Memorandum on Critical Infrastructure Security and Resilience, Apr. 20, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ ("National Security Memorandum").

obligation to report this information concludes. Given the penalties for noncompliance, entities will once again necessarily err on the side of overreporting.

Uncertainty regarding the content that must be reported and when the reporting obligation concludes, combined with the threat of enforcement action for incomplete reporting, would necessarily dictate covered entities prioritize reporting over recovery, contrary to the National Institute of Standards and Technology Cybersecurity Framework 2.0 ("NIST CSF 2.0"). Notably, the NIST CSF 2.0 includes Recover as one of the six core functions based on NIST's recognition that recovering from an incident is equally important to an entity as protecting against, and responding to, cyber incidents.[39]

Specifying that small communications providers need only submit one Supplemental Report, along with a specific timeframe for doing so (i.e., 30 days as recommended above), will also clarify and reduce the data and records preservation requirements proposed in the NPRM. In particular, the NPRM proposes to require all covered entities to retain data and records related to a Covered Cyber Incident for "no less than two years from the submission of the latest required CIRCIA Report" including any Supplemental Reports.[40] Thus, as CISA noted in the NPRM, "the two-year retention period restarts at the time of submission of each Supplemental Report."[41] While NTCA appreciates the flexibility proposed in the NPRM for how the data and records are stored, as CISA also recognizes, "retaining data and records is not without cost" no matter what method is used.[42] While the exact cost will undoubtedly vary from one entity to

[39] The NIST Cybersecurity Framework 2.0, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[40] NPRM, 89 FR at 23731.

[41] *Id*. at 23732.

[42] *Id*. at 23731.

another, there is cost involved and that cost needs to be considered and calculated alongside all other CIRCIA requirements, especially for small businesses, to fully calculate the cost to covered entities versus the benefit. As described in Section IV *infra*, NTCA encourages CISA to limit to one year instead of two the requirement that covered entities retain data and records pertaining to a Covered Cyber Incident.

At a minimum, CISA can minimize the cost burden on small communications providers by requiring only one Supplemental Report be filed by these providers along with a 30-day timeline for filing a Supplemental Report that begins on the date the provider filed a Covered Cyber Incident Report (which requires only the information identified in Section II above as requested currently in CISA's voluntary cyber incident reports).[43] This will also ensure the record retention requirements proposed in the NPRM have a definite, and clear, end date.

III. THE PROPOSED REPORTING REQUIREMENTS EXCEED CONGRESSIONAL INTENT AND SHOULD BE CLEARLY DEFINED TO ELIMINATE UNCERTAINTY AND AN EMPHASIS ON REPORTING INSTEAD OF RECOVERY AND THREAT REDUCTION.

CIRCIA directs CISA to adopt rules requiring covered entities to report Covered Cyber Incidents to CISA in a manner and with content that will allow CISA to "immediately review the report to determine whether the cyber incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures."[44] Congress' intent is to ensure critical infrastructure

[43] If a small provider's Covered Cyber Incident Report contained all of the requisite information and thus a Supplemental Report was not required, the timeline would of course commence with the date the Covered Cyber Incident Report was filed.

[44] CIRCIA sec. 2245(a)(2)(A).

providers receive timely, actionable information from CISA that will allow these providers to take steps to reduce the risk of a similar attack perpetrating their system. To fulfill this directive, Congress has emphasized that CIRCIA's incident reporting rules must focus on risk reduction, not information gathering. Congressman Swalwell, for instance, commented during a recent hearing on the NPRM that overreporting is likely to occur given the current definitions.[45] Congressman Swalwell also commented that CIRCIA was adopted to allow CISA to detect and quickly disrupt tactics by adversaries and, to accomplish this objective, CISA must refine key definitions including covered entity and avoid focusing on quantity over quality.[46]

A. The criteria for a Covered Cyber Incident should be more clearly defined to eliminate uncertainty and overreporting.

CIRCIA as well as the National Security Memorandum call for sharing of "timely, actionable information."[47] As described previously, however, CISA's proposed definition of a Covered Cyber Incident extends far beyond "timely, actionable information" and provides significant room for interpretation from one company to another or from CISA to a covered entity, to the detriment of both critical infrastructure providers and Congress' goal in enacting CIRCIA. Notably, CISA proposes to define a covered cyber incident as a substantial cyber incident that results in any of the following: (1) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network; (2) a serious impact on the safety and resilience of a covered entity's operational systems and processes; (3) a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or

[45] Surveying CIRCIA Hearing, *supra*.

[46] *Id*.

[47] National Security Memorandum at 5, Information Exchange.

services; or (4) 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, managed service provider, other third-party data hosting provider, or by a supply chain compromise

As an initial matter, a "loss of integrity" is unclear. While CISA's examples of incidents that would or would not likely qualify as a Covered Cyber Incident are informative to some degree, small providers require clarity to ensure effective compliance in lieu of guesswork. Additionally, the examples are described as circumstances that are "likely" or "not likely" to qualify as substantial cyber incidents – which also offer no guarantees or even firm guidance. The definitions themselves need clarity to include only incidents that cause "demonstrable harm to the national security interests, foreign relations, or economy" of the U.S., consistent with CIRCIA.

To provide clarity regarding what constitutes a Covered Cyber Incident, NTCA recommends defining a "substantial" or "covered cyber incident" as a cyber incident that leads to any of the following:

> (1) A substantial loss of confidentiality, integrity or availability of a critical portion of a covered entity's information system or network required for the provision of critical products or services by that entity;
>
> (2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes required for the provision of critical products or services by that entity;
>
> (3) A disruption of a covered entity's ability to engage in a critical portion of business or industrial operations, or deliver critical goods or services.
>
> (4) Unauthorized access and interruption, disruption, or destruction of a covered entity's information system or network that results in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety that is facilitated through or caused by a:

(i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

(ii) Supply chain compromise.

(5) A "substantial cyber incident" resulting in the impacts listed in paragraphs (1) through (3) in this definition includes any cyber incident that results in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety regardless of cause, including, but not limited to, any of the above incidents caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

Importantly, this revised definition of a Covered Cyber Incident offers a risk-based approach to identifying incidents that must be reported, while also reducing uncertainty among covered entities that will by default lead to overreporting, impose unnecessary burdens, and impede CISA's ability to review and quickly disseminate important cyber threat information. This definition also furthers CIRCIA's directive to ensure regulatory harmonization by adhering to the definition of a substantial cyber incident contained in Presidential Policy Directive/PPD-41, United States Cyber Incident Coordination[48] as well as the imperative contained in the National Security Memorandum to apply a risk-based approach to advancing critical infrastructure security and resiliency.[49]

Similarly, what constitutes a "reasonable belief" can be open to multiple interpretations. For instance, CISA suggests that "where the covered entity has not yet been able to confirm the

[48] Presidential Policy Directive – United States Cyber Incident Coordination, The White House, July 26, 2016, II.B., https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident ("Significant cyber incident. A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.").

[49] National Security Memorandum, *supra*.

cause of the incident, the covered entity must report the incident if it has a "reasonable belief" that a covered incident occurred."[50] Under this standard, a broadband provider could conclude that discovery of an anomaly when conducting an internal check of logs constitutes a "reasonable belief," and thus the start of the 72-hour reporting clock. This alone could result in an overwhelming number of CIRCIA Reports.[51] To minimize uncertainty, NTCA recommends that the timeline for filing a Covered Cyber Incident begins when the covered entity *confirms* a Covered Cyber Incident has occurred rather than has a "reasonable belief" that a Covered Cyber Incident has occurred. This would be consistent with CIRCIA, which specifies that a cyber incident "does not include an occurrence that imminently, but not actually jeopardizes…."[52]

B. The criteria for a supply chain compromise sets a nearly impossible reporting threshold.

CISA seeks comment on "[a]nticipated challenges for covered entities related to understanding or reporting a covered cyber incident if such incident stemmed from a disruption of a third-party vendor or service provider that is itself not a covered entity."[53] As described above, CISA proposes to include as a substantial and thus, covered, cyber incident "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

[50] NPRM, 89 FR at 23665.

[51] By FCC estimates, there are approximately 2,159 small broadband service providers. *See Reporting on Border Gateway Protocol Risk Mitigation Progress*, Notice of Proposed Rulemaking, PS Docket Nos. 24-186 and 22-90 (rel. June 7, 2024) at ¶ 94.

[52] CIRCIA sec. 2240(6)(B).

[53] NPRM, 89 FR at 23675.

compromise."[54] Unlike other types of Covered Cyber Incidents, CISA proposes that these types of incidents need not be "substantial" or "serious" to be subject to the proposed reporting requirements.

While NTCA recognizes the importance of sharing information about supply chain incidents to allow critical infrastructure providers and others to shore up their defenses and mitigate the risk of a similar incident, the scope of supply chain (or cloud provider or managed service provider) incidents that CISA proposes to include as a Covered Cyber Incident should be expressly confined to incidents that result in demonstrable harm to national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety.

A supply chain incident should not qualify as a Covered Cyber Incident absent demonstrable harm. Absent such threshold criteria, the proposed definition would seem to include any vulnerability that an adversary could leverage, regardless of whether such vulnerability resulted in a compromise of the provider's operations or whether the incident impacted a critical portion of the provider's information system or network. Casting such a wide net would impose an inordinate burden on covered entities without a corresponding reduction in the ability to guard against similar cyber incidents.

CISA should also make clear that the details of a supply chain, cloud service provider, or managed service provider incident that must be reported are expressly limited to details specific to the covered entity itself and not that of any other entity in the supply chain, or of the cloud provider, managed service provider, or any other third-party data hosting provider. To require

[54] *Id.* at 23661.

otherwise would be a nearly impossible task, especially for small communications providers who rely almost entirely on "off the shelf" hardware and software and thus do not have the ability to obtain in depth details regarding the origin of the incident. Even if the provider happened to have a direct customer relationship with the entity where the supply chain or other incident was deemed to have initiated, any details beyond those already publicly disclosed would invariably be proprietary company information that cannot be disclosed to outside parties.

As a real-world example, the supply chain incident involving 3CXDesktopApp[55] originated with an employee of a multinational company downloading end of life software onto the employee's computer. Unbeknownst to the employee, the software contained malware that moved laterally and infected the company's installation software. The employee's company offers video conferencing and online communications platform to companies worldwide. As a result, the malware was able to infect the company's customers through the videoconferencing platform, and extended its reach to two energy providers.[56] If a small broadband provider happened to use this company's video conferencing and online communications platform, in circumstances such as the one described, the provider would be required to file a Covered Cyber Incident Report, at a minimum, due to the fact that the malware arguably "gained unauthorized access to" the provider's system or network due to a supply chain compromise – without regard for whether substantial harm resulted from the incident.

The definition that CISA applies to a supply chain, cloud service provider, or managed service provider incident also affects the amount of information covered entities must submit and

[55] *See, e.g.*, "Supply Chain Attack Against 3CSDesktop App," CISA, March 30, 2023, https://www.cisa.gov/news-events/alerts/2023/03/30/supply-chain-attack-against-3cxdesktopapp.

[56] "X_Trader Supply Chain Attack Affects Critical Infrastructure Organizations in U.S. and Europe," Apr. 21, 2023, https://symantec-enterprise-blogs.security.com/threat-intelligence/xtrader-3cx-supply-chain.

CISA must review in time to reduce the risk of a similar, cascading incident on other entities. Furthermore, requiring covered entities to include details in CIRCIA Reports regarding the impact of a compromise due to these types of incidents would be extremely difficult at best for small providers due to the time and resources necessary to trace the origination and path of these types of incidents. Furthermore, any information that covered entities impacted by the incident could provide apart from details specific to their own operations would at best be the same information already shared through news reports.

Approaching this step by step, a provider would first have to obtain the information from a third-party vendor where the incident took place - assuming the provider can even identify who that is and do so within 72 hours - all while responding to the impact of the incident on their own operations. Assuming that is possible, the third-party vendor is unlikely to disclose the level of detail proposed in the NPRM to be included in a Covered Cyber Incident Report to an outside entity, in part due to the proprietary nature of some of the information requested. The vendor would also be in the midst of addressing the impact of the incident on its own operations, and determining the parties affected, at the time the Covered Cyber Incident Report must be filed, further increasing the challenges confronting covered entities' ability to report detailed information regarding the incident. Finally, in the likely event that not all of the information was available to be included in the Covered Cyber Incident Report, the provider would be responsible for filing Supplemental Reports for weeks or even months while attempting to collect all of the information required. These efforts would detract heavily from a small communications provider's ability to focus on ongoing operations, with little information to be gained by CISA from the reporting, and little likelihood that the additional information would be useful to

helping other covered entities avoid similar attacks, especially given the length of time between the initial incident and when the reporting obligation is deemed complete.

CISA must balance imposing burdensome and ongoing reporting requirements against the value of information to be gained and the time required by CISA to review and disseminate critical information. At a minimum, CISA should therefore require a covered entity to report an incident involving a supply chain, cloud service provider, managed service provider, or other third-party data hosting provider only when the incident caused an interruption, disruption, or destruction of a covered entity's information system or network, or any nonpublic information contained therein, that results in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety. This is 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[57] and aligns a supply chain incident with the same definition proposed in section III above for other Covered Cyber Incidents, thereby eliminating a separate, lower, threshold for supply chain or third-party provider incidents that unnecessarily risks confusion and enforcement action on the part of, and against, covered entities.

Carefully defining the scope of information that must be reported following a third-party or supply chain compromise will further allow CISA to focus on circumstances and information

[57] CIRCIA sec. 2240(17).

that would prevent cascading events. NTCA therefore 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 rather than providers of intermediary transport or contractors. In those instances, affected entities are merely the consumers of the product or service and have no control over, or meaningful insights into, what may have led to the incident, or any internal actions taken in response to the incident. Requiring reports from covered entities in such cases would yield little to nothing in the way of useful information to help prevent a similar incident from occurring or from harming critical infrastructure, as intended by CIRCIA. Furthermore, due to the fact that many small providers often use the same managed service provider, CISA would find itself having to wade through many CIRCIA Reports that contain virtually identical information, taking valuable time and resources away from the small providers affected by the incident as well as from CISA's ability to quickly assess the source of the incident and method of access and in turn share that information quickly with other critical infrastructure providers.

C. The breadth of information proposed to be required in a Covered Cyber Incident Report will force providers to prioritize reporting over recovery and impede CISA's ability to expeditiously share information about cyber incidents.

CISA's ability to collect, analyze and quickly share information about Covered Cyber Incidents is essential to reducing the risk of ongoing, similar incidents, and is the basis for CIRCIA. The broad scope of covered entities combined with the wide array of mandatory information proposed to be provided in CIRCIA Reports would render CISA unable to act on the

information provided within the short timeframe necessary to help others guard against similar incidents.

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 incident to mitigating damage and restoring operations, CIRCIA Reports should include only core information necessary to allow CISA or other federal agencies to offer assistance to the Covered Entity and to help others avoid or mitigate a similar incident. Limiting the scope of information that must be reported, and correspondingly, the time necessary to complete one or more CIRCIA Reports, is especially important for small broadband providers, many of whom do not have a dedicated security professional on staff to respond to an incident and must instead call in outside professionals to assist with scoping the incident and obtaining details that must be reported.

IV. THE RECORD RETENTION REQUIREMENTS SHOULD BE LIMITED TO THOSE THAT CISA CAN EVALUATE QUICKLY AND USE TO ALERT OTHER ENTITIES TO METHODS OF GUARDING AGAINST SIMILAR INCIDENTS.

CIRCIA requires covered entities who experience a Covered Cyber Incident to preserve "data and information" related to the event and directs CISA to establish a "clear description of the types of data and information that covered entities must preserve."[58] In response, the NPRM proposes to require data and "records" (in place of "information") to be preserved, which CISA identifies as "log entries, memory captures, or forensic images that the covered entity believes in good faith are relevant to the incident."[59] CISA describes these items as necessary to support "the ability of analysts and investigators to understand how a cyber incident was perpetrated and

[58] NPRM, 89 FR at 23730, citing 6 U.S.C. § 781(b)(c)(6).

[59] NPRM at 23731.

by whom."[60] Without further clarification, and limitation, of exactly what is included within these terms, however, covered entities are going to be left with uncertainty, unnecessary costs, and potential liability.

To begin with, CISA's proposal to use the terms data and "records" in lieu of the statutory language of data and "information" could be construed more broadly than intended by Congress.[61] For instance, the NPRM's inclusion of "log entries" among the records to be collected leaves room for interpretation. Additionally, if a customer's database was breached, covered entities need to know whether they must store the entire compromised database, only the server involved in the breach, or all servers along the chain to the database and in the state they were in when the breach occurred. Furthermore, to comply with CISA's determination that the preservation of records and data is necessary to support "the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom"[62] covered entities would have to preserve much more than CIRCIA's requirement of "data and records," and instead require the covered entity to retain the entire server. For many small broadband providers, this would require investing in an entirely new hard drives – at significant cost – because the amount of hard drive space necessary to preserve forensic images on a server impacted by the cyber incident would leave insufficient space on that server for the provider to maintain its normal operations. Clearly, this cost is well beyond that estimated by CISA and expected by CIRCIA. Accordingly,

[60] *Id.*

[61] CIRCIA sec. 2242(a)(4) and 2242(b)(6).

[62] NPRM, 89 FR at 23731.

NTCA encourages CISA to clarify and limit the data and information covered entities must preserve.

NTCA also urges CISA to consider the cost to covered entities of retaining data and records as compared to the ability of such data and information to help critical infrastructure providers protect against similar incidents. Specifically, the NPRM proposes to require covered entities to retain data and records for two years from the date on which they filed a CIRCIA Report. Further CIRCIA Reports made by the covered entity, according to the NPRM, would restart the two-year timeline.[63] CIRCIA, however, does not specify the length of time these records must be retained and CISA recognizes that "the costs for preserving data increase the longer the data must be maintained."[64] NTCA therefore recommends limiting covered entities obligation to retain any data or information related to a Covered Cyber Incident to one year from the date of filing the initial CIRCIA Report.

As CISA is well aware, the cybersecurity landscape changes quickly and as malicious actors have repeatedly demonstrated, these actors have developed adaptable models – as soon as the indicators of compromise are made known publicly, the malicious actors must adopt different methods of attack, sometimes changing their tactics entirely. Accordingly, within one year, the tactics used in any given cyber incident will likely change, rendering forensic data and similar information extending beyond that period of little value to defending against similar tactics. Therefore, retaining forensic data any longer than that is simply adding a burden to covered entities without any corresponding benefit.

---

[63] *Id*.

[64] *Id*. at 23732.

Finally, NTCA urges CISA to codify in the final rules a good faith exception consistent with the language in the NPRM limiting the data and records collected to those that the covered entity "believes in good faith are relevant to the incident."[65] This is essential as interpretations can vary widely from one entity to another, as CISA recognized in the NPRM,[66] and small providers in particular should not risk liability if they interpret the scope of data and records to be retained different from CISA, or even from another agency or private company, if they acted in good faith to meet the requirements.

V. CISA MUST USE AUTHORITY GRANTED UNDER CIRCIA TO AVOID REDUNDANT AND CONFLICTING FEDERAL INCIDENT REPORTING MANDATES.

CIRCIA provides an exception to the incident reporting requirements where the covered entity 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.[67] This exception would be especially beneficial to small communications providers both to allow these entities to focus their small staff on addressing and recovering from the incident while also avoiding confusing and perhaps conflicting reporting requirements.

Specifically, focusing solely on small broadband providers – all of whom are well below the SBA small business threshold – and only on federal reporting requirements, Attachment 1 to these comments shows the core overlapping reporting requirements that small communications providers must adhere to in the minutes, hours and days immediately following a cyber incident

[65] *Id*. at 23731.

[66] *See Id*. at n. 369 ("numerous definitions … have been proffered … from a wide variety of cyber-related resources….").

[67] CIRCIA sec. 2242(a)(5)(B).

that causes a service outage and/or unauthorized access to customers' personal information. As an initial matter, in the event of a service outage, small providers must file a NORS report with the FCC. If customers' personal information was accessed without authorization, the provider must file a separate data breach report with the FCC (in addition to notifying customers and any State reporting requirements).[68] If the incident caused a system outage *and* customers' information was accessed without authorization as part of the same incident, the provider would be required to file both a NORS and a data breach report. Finally, if the incident qualified as a Covered Cyber Incident, the provider would be required to also file one or more CIRCIA Reports. If these small providers deliver service pursuant to a government contract, they would likely be subject to even more reporting requirements,[69] and if the outage impeded the delivery of 911 services, yet more reporting would be required.[70]

Redundant and burdensome cyber incident reporting requirements are inconsistent with both the Congressional directive under CIRCIA and the White House's focus on the need for regulatory harmonization.[71] Congressman Garbarino, for instance, recently commented that there are more than three dozen federal cyber reporting requirements; these are confusing and

---

[68] *Data Breach Reporting Requirements*, WC Docket No. 22-21, FCC 23-111. Report & Order (rel. Dec. 21, 2023). Note the section of the FCC's data breach reporting requirements pertaining to the collection of data breach reports is pending approval by the Office of Management and Budget ("OMB"); however, the rules defining a breach have become final and communications carriers remain subject to the same 7-day timeline for reporting access to customers' proprietary network information pursuant to existing FCC rules. *See* 89 FR 9968 (Feb. 12. 2024) ("This rule is effective March 13, 2024, except for the amendments codified at 47 C.F.R. 64.2011 and 64.5111, instructions 3 and 4, which are delayed indefinitely.").

.

[69] *See Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing*, 88 FR 68055 (Oct. 3, 2023).

[70] *See* 47 CFR § 4.9.

[71] *See* "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information," Office of the National Cyber Director, June 2024, https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.

reactive and need harmonization. He also commented that a fragmented approach to incident reporting is cumbersome and oftentimes redundant, creating a compliance burden on private sector partners who could be spending their resources on security rather than fulfilling multiple reporting requirements, and that CIRCIA was adopted to provide a better and more coordinated reporting mechanism.[72] Congressman Swalwell similarly emphasized the importance of avoiding redundant and duplicative cyber incident reporting requirements.[73]

Looking only at the FCC's NORS and data breach reporting requirements and how they fit into CIRCIA's "substantially similar" exception, Attachment 1 demonstrates that at a minimum, these small providers must know the deadline for reporting an incident; the agency and the portal where the incident must be reported; and the details that must be reported – all while in the midst of responding to and recovering from an incident that impacts their operations and/or accesses customers' personal information, and all with the risk of enforcement action for missing a report or failing to report all of the details required by the respective federal agency.

Accordingly, for CIRCIA's mandated exception to have any practicality, CISA must carefully define what it means for covered entities to report "substantially similar information" in a "substantially similar timeframe."[74] The NPRM's proposed method of defining these terms would render the exception nonexistent for small broadband providers. To begin with, the FCC's data breach rules require communications providers to file a notice with the FCC no later than seven business days after reasonable determination of a breach.[75] Without further

[72] Surveying CIRCIA Hearing, *supra*.

[73] *Id.*

[74] NPRM, 89 FR at 23708.

[75] 47 C.F.R. § 64.2011(b). (as noted *supra*, the FCC's data breach rules are pending OMB approval).

clarification, CIRCIA's 72-hour timeframe for submitting a Covered Cyber Incident Report presumably would not be considered a "substantially similar timeframe," thereby eliminating communications providers' ability to avail themselves of this important exception when filing an FCC data breach report. As a result, in these circumstances, small providers would be faced with ongoing substantially duplicative reporting requirements at both the FCC and CISA at the very time their focus is needed for identifying the source and extent of the incident and restoring service. CISA at a minimum could reduce this burden by limiting the information required to be reported to the ten items described in section II *supra*.

Looking at NORS, the other type of incident reporting facing communications providers, if a cyber incident causes a network outage as defined by the FCC's rules for the type of service impacted, within 120 minutes of discovering the outage providers must file: (1) a NORS notification with the FCC that contains preliminary information about the outage; (2) an initial outage report within three calendar days; and (3) a final report within 30 days after the preliminary report.[76] At best then, the time for filing an initial outage report in NORS could be considered within the same timeframe as required for a Covered Cyber Incident Report. The next test then would be whether a NORS report includes "substantially similar information" as that proposed for a Covered Cyber Incident Report. Initial outage reports required to be filed in NORS must include:

1. Name of the reporting entity;

[76] "Network Outage Reporting System (NORS)," FCC, https://www.fcc.gov/network-outage-reporting-system-nors. The FCC has proposed rules that would require broadband providers to report network outages through NORS as well. *See Resilient Networks, Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, Second Report and Order and Second Further Notice of Proposed Rulemaking, PS Docket No. 21-346 et al, FCC 24-5 (rel. Jan. 26, 2024).

2. Date and time of onset of the outage;

3. Brief description of the problem;

4. Service effects;

5. Geographic area affected by the outage; and

6. A contact name and contact telephone number

The initial report must contain all pertinent information then available regarding the outage while the final report must also contain not only pertinent information regarding the outage but also any information that was not contained in, or that has changed from that provided in, the initial report.[77] These details are significantly different from, and importantly, significantly less burdensome than, the incident reporting requirements proposed in the NPRM. Notably, however, these details are not significantly different than those requested in CISA's voluntary cyber incident reporting form (see section II *supra*) and recommended herein as the information to be collected from small communications providers pursuant to CIRCIA absent an exemption for these providers. Therefore, if CISA were to adopt NTCA's recommendation herein to limit the information that small communications providers must report to that currently requested in CISA's voluntary cyber incident reporting form, complying with both NORS and CIRCIA reporting requirements would not pose an undue burden even if the reports were required to be filed separately.

[77] 47 C.F.R. § 4.11.

VI. THE SENSITIVE NATURE OF INFORMATION TO BE COLLECTED PURSUANT TO CIRCIA NECESSITATES CONFIDENTIALITY AND PROTECTION FROM DISCLOSURE OR UNAUTHORIZED ACCESS.

Due to the highly sensitive and proprietary nature of the information proposed to be collected pursuant to CIRCIA, whether through CIRCIA Reports, Requests for Information, subpoenas, or information sharing with other federal agencies, CISA must adopt rules that specify safeguards for protecting the information collected against unauthorized disclosure or access. Accordingly, NTCA makes the following recommendations.

First, all information provided by covered entities pursuant to CIRCIA must be treated as presumptively confidential and not subject to FOIA requests, without the need for covered entities to check a box requesting such classification when they submit a CIRCIA Report.[78] This is also consistent with CIRCIA, which provides that CIRCIA Reports "shall be exempt from disclosure under FOIA."[79]

Second, CISA must adopt rules to ensure the information collected is securely stored and protected against unauthorized disclosure or access, including as part of any information sharing agreement CISA enters into with other federal agencies with respect to CIRCIA Reports or cyber incident reports submitted to other federal agencies and shared with CISA.

Third, CISA should adopt rules specifying who has access to the information, what they will do with the information, and how they will protect the information from unauthorized access or disclosure.

---

[78] *See* NPRM, 89 FR at 23737 (CISA will provide covered entities and third parties with an option to make such a designation throughout the web-based form for all CIRCIA reports).

[79] CIRCIA sec. 2245(b)(2).

Finally, CISA should adopt rules requiring the destruction of reporting entities' identifiable information annually unless such information is the subject of an ongoing investigation.[80]

VII. CISA CAN QUICKLY EXPAND AWARENESS OF CYBER INCIDENTS BY SHARING NONPROPRIETARY INFORMATION WITH ISACs.

To further minimize the impact that widespread cyber incident and ransomware attacks can have on the public, NTCA encourages CISA to share anonymized information provided in CIRCIA Reports with software, hardware, and cloud providers and with member Information Sharing and Analysis Centers ("ISACs") as soon as reasonably possible after receiving CIRCIA Reports. ISACs were established by a 1998 Presidential Directive to enable critical infrastructure owners and operators to share cyber threat information and best practices. ISACs are best able to fulfill that mission when information is readily exchanged between the government and private sector.

For instance, in an internal survey of CyberShare members, 100% of respondents stated they are receiving information through their participation in the ISAC that makes them more aware of and/or helps them manage threats to their enterprise. Sharing key information regarding the method and scope of the compromise with ISACs will allow this important information to be disseminated rapidly to a large swath of critical infrastructure providers and in turn allow these providers to quickly identify whether their operations contain the same vulnerability and to make targeted modifications to their systems as needed to address the identified vulnerabilities. Given the ISACs' established communication mechanisms and

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

information sharing protocols, they are well positioned to receive CISA's reports and relay the information throughout the private sector, including to small businesses that typically do not have as ready access to cyber threat information as large businesses.

In addition to rapidly sharing information about threats and vulnerabilities, a quarterly trends report that does not include confidential or proprietary data would help critical infrastructure providers adapt to an ever-changing threat landscape. Sharing aggregated or anonymized summaries of reports, trending analysis, or analysis of a specific threat, vulnerability, or risk that do not identify any incident at a specific covered entity with the ISACs will help further CIRCIA's objective by disseminating the information quickly instead of relying solely on an expectation that companies, especially small ones, will receive alerts relevant to their operations.

VIII. CONCLUSION

CIRCIA offers an important avenue for CISA to identify modes of cyber incidents more rapidly and to share vital information about those incidents with other critical infrastructure providers. When carrying out this important directive, however, NTCA urges CISA to consider the impact on small communications providers of both the definition of a Covered Cyber Incident and the information that must be reported in the immediate aftermath of an incident and to limit both the definition and scope of the information to be reported and retained to only those

incidents and information that would help prevent similar incidents affecting other critical infrastructure providers.

Respectfully submitted,

By: */s/ Michael Romano*
Michael Romano
Tamber Ray
Meghan O'Brien

4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
(703) 351-200

Attachment 1
Core Incident Reporting Requirements for Small Communications Providers

	FCC Data Breach Reporting[1]	**NORS (Network Outage Reporting System)**[2]	**CISA CIRCIA NPRM**
Events that start the reporting requirement	When a carrier has made a reasonable determination that a breach occurred. When 500 or more customers are affected or when a carrier can't determine number affected.	An outage lasts at least 30 minutes and satisfies other specific thresholds (see timing below).	A covered entity must submit a report to CISA when it reasonably believes a covered cyber incident occurred, makes a ransom payment, or experiences circumstances that require an update or supplement to a Covered Cyber Incident Report submitted by the covered entity.
Who it applies to	Providers of telecommunications, interconnected VoIP, and telecommunications relay services.	Communications providers that provide for a fee to one or more unaffiliated entities by radio, wire, cable, satellite, and/or lightguide: two-way voice and/or data communications, paging service, and/or Signaling System 7 communications. The FCC's Resilient Networks NPRM proposes to extend the rules to broadband providers.	Focusing solely on the Communications Sector, any entity that provides communications services by wire or radio communications to the public, business, or government.

[1] *Data Breach Reporting Requirements*, Report & Order, WC Docket No. 22-21 (rel. Dec. 20, 2023).

[2] 47 C.F.R. §§ 4.1 – 4.11. *See also Resilient Networks*, Second Report and Order and Second Further Notice of Proposed Rulemaking, PS Docket No. 21-346 *et. Al.* (rel. Jan. 26, 2024) ("Resilient Networks NPRM"). Please refer to the rules for more detailed outage reporting requirements based on the type of communications service affected.

Attachment 1
Core Incident Reporting Requirements for Small Communications Providers

	FCC Data Breach Reporting	NORS (Network Outage Reporting System)	CISA CIRCIA NPRM
Timing for reporting	No later than seven business days after reasonable determination of a breach if at least 500 customers are affected or the carrier cannot determine the number affected. If fewer than 500 customers are affected and the carrier can reasonably determine the breach is not reasonably likely to **harm**[i] those customers, the carrier need only file an annual report on or before February 1 of each year.	**Cable, Wireless, Wireline, Satellite, and Signaling System 7** Notification: within 120 minutes of discovering they have experienced an outage of at least 30 minutes duration Initial Outage Report: within 72 hours of discovering the outage Final Report: within 30 days of discovering the outage **IXC or LEC tandem facilities** Notification: outages of at least 30 minutes duration **Interconnected VoIP providers** Notification: within 240 minutes of discovering an outage of at least 30 minutes that potentially affects a 911 facility or within 24 hours of discovering an outage of at	Covered Cyber Incident Report must be filed within 72 hours of reasonable belief that a covered cyber incident has occurred. A Ransomware Payment Report must be filed within 24 hours of making a ransom payment as a result of a ransomware attack. A Joint Covered Cyber Incident and Ransom Payment Report can be used by covered entities that make a ransom payment associated with a Covered Cyber Incident prior to the 72-hour deadline for submitting a Covered Cyber Incident Report. A Supplemental Report must be filed "promptly" (within 24 hours) if substantial new or different information becomes available or the covered entity makes a ransom payment after submitting a Covered Cyber Incident Report. Reporting obligation continues until all information required for a Covered Cyber Incident Report has been submitted.

		least 30 minutes that potentially affects 900,000 user minutes Final Report: within 30 days of discovering the outage.	
	FCC Data Breach Reporting	**NORS (Network Outage Reporting System)**	**CISA CIRCIA NPRM**
Criteria	What constitutes a breach? Any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed covered data. Covered data includes both a customer's **Customer Proprietary Network Information (CPNI)**[ii] and **personally identifiable information.**[iii] This includes inadvertent access, use, or disclosure of customer information. Excludes good faith acquisition of customer data by an employee or agent where such information is not used improperly or further disclosed.	What constitutes an outage? A significant degradation in the ability of an end user to establish and maintain a channel of communications as a result of failure or degradation in the performance of a communications provider's network.	What constitutes a Covered Cyber Incident? A substantial cyber incident that leads to: (a) substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network; (b) 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.
	FCC Data Breach Reporting	**NORS (Network Outage Reporting System)**	**CISA CIRCIA NPRM**
Information required to be reported	Carrier address and contact information, description of the breach incident, method of compromise, date range of the incident, approximate number of customers affected, estimate of financial loss to carrier and customers, if any, and the types of data breached.	Notification: Name of the reporting entity; date and time of onset of the outage; brief description of the problem; service effects; geographic area affected; and contact name and telephone number Initial Report: All pertinent information then available on the outage Final Report: All pertinent information about the outage specific to the type of service affected (details in 47 C.F.R. part 4) and any information that was not contained in, or that has changed from that provided in, the Initial Report	All CIRCIA Reports: 1. Report Type 2. Identity of the Covered Entity 3. Contact Information for Covered Entity 4. Third party authorization to submit, if applicable Covered Cyber Incident Report: 1. Description of the Covered Incident 2. Vulnerabilities, Security Defenses, and TTPs 3. Information related to identity of perpetrator of the incident 4. Mitigation/Response 5. Additional data or information Ransom Payment Report: 1. Description of ransomware attack 2. Vulnerabilities, Security Defenses, and TTPs 3. Information related to identity of perpetrator of the attack 4. Information on the ransom payment 5. Results of the ransom payment 6. Additional data or information

Attachment 1
Core Incident Reporting Requirements for Small Communications Providers

			Supplemental Report: A subset of required and optional content from a Covered Cyber Incident Report and/or Ransom Payment Report.
	FCC Data Breach Reporting	**NORS (Network Outage Reporting System)**	**CISA CIRCIA NPRM**
Reporting location	Electronically notify the FCC, United States Secret Service and FBI through a central reporting facility. The FCC will maintain a link to the reporting facility on its website.	Electronically notify the FCC using the NORS filing portal.	Covered entities must submit CIRCIA Reports through the web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner approved by the Director.

Attachment 1
Core Incident Reporting Requirements for Small Communications Providers

Definitions

[i] Harm:
1) Financial harm
2) Physical harm
3) Identity theft
4) Theft of services
5) Potential for blackmail
6) Disclosure of private facts
7) Disclosure of contact information for victims of abuse
8) Other similar types of dangers

[ii] Customer Proprietary Network Information (CPNI):
1) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
2) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

[iii] Personally Identifiable Information (PII):
1) First name or first initial and last name in combination with any government issued identification numbers or government issued document used to verify the customer's identity or other unique identification number used for authentication purposes;
2) Customer name or email address in combination with a password or security question and answer or any other authentication method or information necessary to permit access to an account;
3) Unique biometric, genetic, or medical data;
4) "Disassociated data" that if linked would constitute PII if the means to link the data were accessed and the data obtained would enable a person to commit identity theft or fraud against the individual to whom the data pertains;
5) Does not include publicly available information that is lawfully made available to the public from federal, state, or local government records or widely distributed media.