February 14, 2025

**VIA ELECTRONIC FILING:**
Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security
Attn: Jeffrey E. Greene, Executive Assistant Director for Cybersecurity
1110 N. Glebe Road
Arlington, VA 20598-0630

**National Cyber Incident Response Plan Update: Public Comment Draft**
**Docket No. CISA-2024-0037**

Dear Mr. Greene,

NTCA—The Rural Broadband Association ("NTCA") welcomes the opportunity to comment on the National Cyber Incident Response Plan Update: Public Comment Draft ("NCIRP") released by CISA on December 16, 2024. [1] NTCA supports efforts to establish a coordinated approach to addressing cyber incidents before they happen as well as defined steps to take if/when they do. NTCA, however, encourages CISA to include in the updated NCIRP certain measures to ensure small broadband providers are not overlooked in federal agencies' planning, awareness, and response to cyber incidents.

NTCA represents hundreds of community-based telecommunications providers across 44 states who deliver critical broadband and voice services to rural communities.[2] To facilitate awareness of cyber vulnerabilities as well as information sharing among small broadband providers, NTCA began offering CyberShare: The Small Broadband Provider ISAC in 2020. Presently, 134 companies participate in CyberShare.[3] NTCA also actively participates in CISA's

[1] Request for Comment on the National Cyber Incident Response Plan Update, Docket No. CISA–2024–0037, 89 Fed. Reg. 241, 10164 (Dec. 16, 2024). Comment deadline extended by Fed. Reg. Notice dated Jan. 3, 2025.

[2] *See* NTCA 2024 Broadband Internet Availability Report (Dec. 2024), available at https://www.ntca.org/sites/default/files/documents/2025-01/2024-broadband-internet-availability-report.pdf.

[3] CyberShare helps small broadband providers strengthen their cybersecurity through bi-monthly educational sessions featuring speakers from CISA, FBI, and private cybersecurity experts, daily

ICT-SCRM Task Force as well as the Communications Sector Coordinating Council and was recently a member of the FCC's Communications Security, Reliability and Interoperability Council VIII.

Based on these experiences, NTCA recommends CISA use this opportunity to identify methods that the agency and its federal partners will use to communicate and coordinate with broadband providers of all sizes before, during, and after a significant cyber incident.

**1. The NCIRP should provide a pathway for clear, consistent and timely information sharing with all broadband providers.**

The NCIRP correctly observes that "[c]omprehensive national preparedness requires additional planning … and stakeholder communities…."[4] Consistent with this observation, NTCA encourages CISA to provide for small broadband providers' active participation in nationwide training events such as CyberStorm and to provide broadband providers of all sizes with timely awareness of cyber incidents. While CISA provides valuable resources to assist companies large and small bolster their cyber defenses, time is of the essence when cyber incidents do occur. As a result, all broadband providers need early and frequent information regarding incidents that involve not only their networks but also those that rely on broadband providers' connectivity.

As an example, Salt Typhoon reportedly was indiscriminate in its targets - manifesting not only in communications providers' networks but also in government networks and even individuals' computers in part through equipment commonly used by businesses of all sizes, the government, and consumers. Given the far-reaching nature of this intrusion, CISA needs to include small broadband providers in the "stakeholder community" as they engage in "exercise coordination" and "conduct additional planning" in preparation for future cyber incidents.[5]

NTCA also encourages the NCIRP to more clearly identify how CISA and federal partners will support critical infrastructure entities, and small broadband providers in particular, during cyber incidents that "cause consequences outside the cyber domain."[6] In doing so, CISA and partners need to balance providers' need to receive timely, actionable information in a manner that accounts for the fact that these providers might simultaneously be in the midst of responding to the incident. One method CISA could use is to make critical infrastructure

---

threat intelligence, peer networking and information sharing. More information on CyberShare is available at https://www.cyber-share.org/.

[4] NCIRP, p. 3.

[5] *Id*. at p. 20.

[6] *Id*. at p. 4.

providers aware of their ability to register for access to information contained in the Homeland Security Information Network ("HSIN"). This could be performed through outreach with Information Sharing and Analysis Centers ("ISACs") and Sector Risk Management Agencies ("SRMAs") at a minimum and would allow more entities to benefit from the information contained in HSIN, while requiring little additional effort from CISA. Additionally, HSIN offers a single, consistent location where critical infrastructure providers can obtain important information and guidance whenever needed.

The NCIRP references ISACs as a tool throughout but lacks clarity on how and when ISACs are to be utilized. NTCA recommends including a more precise delineation of how CISA envisions working with ISACs during cyber incidents. In particular, the current draft appears to position ISACs primarily as information-sharing conduits; however, CISA should use this opportunity to also leverage ISACs' expertise and established relationships more effectively as strategic partners in incident response. One method of doing so is to loosen the information sharing restrictions on reports shared with ISACs wherever possible (*e.g.*, label documents shared using Traffic Light Protocol ("TLP") green instead of red) so that entities can freely share the information with peers.

Further, Table 2 of the NCIRP, "Coordinating Structures Involved in Cyber Incident Response," correctly places ISACs as a coordinating structure, but then vaguely directs ISACs to "work with. . . SRMAs to support incident response activities."[7] To expedite and more readily target support during incidents, the NCIRP should clearly identify which agency and department within the agency(ies) will serve as the primary point of contact for ISACs during incident response. Furthermore, given the multiple agencies referenced throughout the NCIRP, the plan should outline how these various agencies will coordinate their communications with critical infrastructure providers, both through ISACs and to the public directly, to ensure clear and consistent information flow. The NCIRP would also benefit from a more detailed explanation of the specific expectations and parameters for ISAC support of SRMA response activities.

NTCA also notes that CyberShare: The Small Broadband Provider ISAC represents an established and effective channel for helping to reach many small broadband providers. With direct access to 134 providers, most of which are not members of the COMM-ISAC, CyberShare is uniquely positioned to help facilitate bi-directional communication between CISA and hard-to-reach providers with limited resources. While this should not be the sole method of communication – not all small broadband providers participate in CyberShare – CyberShare's existing infrastructure can complement CISA's direct outreach by expanding the reach of communications to additional broadband providers.

**2. The NCIRP should provide more detailed information regarding how the government "remains cognizant" of private sector activities.**

Ensuring all broadband providers have timely access to information regarding techniques used in a significant cyber incident, regardless of whether such incident was directly focused on

[7] *Id*. at p. 10.

broadband providers, is essential for all providers and especially small providers as they work to identify how best to prioritize their limited funds and staff based on impact, cost and complexity, consistent with CISA's Cross Sector Cybersecurity Performance Goals.

**3. The NCIRP should provide a clear pathway for public-private coordination.**

NTCA agrees with the NCIRP's recognition that public-private partnerships are an essential component of detecting and responding to cyber incidents; however, to achieve the intended objective, these partnerships must extend beyond the Unified Coordination Group and the Joint Cyber Defense Collaborative to include an established and ongoing method of ensuring broadband providers of all sizes are included in these public-private partnerships, given the essential role all providers play in connecting their communities.

CISA and other federal agencies have a history of successful public-private coordination that benefits both the agencies and the private sector and that includes participation by, and information sharing with, small communications providers. For instance, the ICT-SCRM Task Force has provided the foundation for officials from CISA and other federal agencies to work side by side with private sector entities to create expert guidance directed at assisting private sector entities in the communications and Information Technology sectors defend against cyber supply chain risks. CISA has also provided the communications sector with a number of webinars focused on guidance for increasing network security, such as through CISA's secure by demand initiatives, as well as briefings on Volt Typhoon and Salt Typhoon that provide concrete information regarding methods used to compromise networks and actions communications providers can take to detect and guard against future cyber incidents. Such actionable and concrete guidance remains a necessary and useful tool in helping all broadband providers defend their networks.

**4. The NCIRP should avoid future revisions that can be or are already included in other federal cyber guidance.**

The NCIRP, while intended "at the highest level" to be used by the federal government, also expressly "encourages" private sector entities to incorporate the NCIRP "into their own planning efforts."[8] Accordingly, while the NCIRP offers important methods of preparing for and responding to cyber events, the document is one more federal cyber guideline that private sector entities will be expected to incorporate into their own cyber initiatives. The NCIRP further provides that "CISA plans to implement a regular cycle of revisions to … update, maintain, and exercise the NCIRP."[9]

[8] NCIRP at p. 3.

[9] *Id.*

NTCA understands that methods used to conduct cyber incidents change and the techniques used to defend against such incidents must also be fluid and able to adapt to such changes. At the same time, however, requiring communications providers – whether by actual rule or by "recommended guidelines" – to adhere to federal guidance that changes frequently places a particular burden on small communications providers.

Entities participating in the Federal Communications Commission's ("FCC") Enhanced A-CAM program, for example, were required to "implement operational cybersecurity and supply chain risk management plans [C-SCRM Plans]" that "reflect the latest version of the NIST Framework for Improving Critical Infrastructure Cybersecurity" and an "established set of cybersecurity best practices, such as … [CISA's] Cybersecurity Performance Goals and Objectives or the Center for Internet Security Critical Security Controls" as well as "NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, and … NIST 800-161."[10] Additionally, Enhanced A-CAM participants must modify their C-SCRM Plans "to comply with new cybersecurity regulations, standards, or laws."[11] The FCC has proposed similar cybersecurity risk management requirements for other communications services, including International Section 214 Authorizations,[12] Emergency Alert System,[13] and 5G funding.[14] Accordingly, small communications providers already must remain cognizant of updates to multiple federal "guidelines" and must modify their own C-SCRM Plans each time one of those guidelines is updated.

Frequent updates to the NCIRP would require yet more updates to these providers' C-SCRM Plans because even if not "required" by rules, "best practices" will necessitate adherence to the NCRIP and thus take time and resources away from active cyber defenses to rewriting, or paying an outside entity to rewrite, C-SCRM Plans. Accordingly, NTCA encourages CISA to work with the agency's federal partners to consolidate cybersecurity guidelines where possible

---

[10] *See Connect America Fund: A National Broadband Plan for Our Future High-Cost Universal Service Support*, Report and Order, Notice of Proposed Rulemaking, and Notice of Inquiry, FCC 23-60 (rel. July 23, 2023) ("*Enhanced A-CAM Order*"), at ¶ 111.

[11] *Id*. at ¶ 112.

[12] *See Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks*, Order and Notice of Proposed Rulemaking, FCC 23-28 (rel. Apr. 25, 2023).

[13] *See Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, Notice of Proposed Rulemaking, FCC 22-82 (rel. Oct. 27, 2022).

[14] *See Establishing a 5G Fund for Rural America*, Further Notice of Proposed Rulemaking, FCC 23-74 (rel. Sep. 22, 2023).

and to make updates only when recommended guidance changes and is not already addressed in other federal guidelines.

**5. The NCIRP's reliance on Title 47 of the Communications Act and Section 706 of the Telecommunications Act is inconsistent with Congress' and courts' action.**

The NCIRP's reference to Title 47 of the Communications Act and Section 706 of the Telecommunications Act extends those authorities beyond their intended scope.[15] Notably, Section 706's scope is limited to the deployment of advanced telecommunications capability and infrastructure and has not historically been interpreted to specifically address cybersecurity incident response. Further, these long-established provisions have traditionally been interpreted as applicable to regulating telecommunications services and restoration of telecommunications services following emergencies, not cybersecurity. By extending these provisions beyond their intended scope, the NCIRP risks federal overreach into areas where Congress has not granted explicit authorization.

This expansive interpretation of legal authorities may damage the crucial trust relationship between the federal government and private sector partners and frustrate implementation and achievement of important cyber objectives by resting them on questionable legal authority. To address these issues, NTCA recommends CISA conduct a thorough review of the legal authorities cited in the NCIRP. Authorities that require broad interpretation or stretch beyond their statutory limits should be removed or replaced with more appropriate references.

**6. Conclusion**

The NCIRP provides an important opportunity to establish clear and consistent methods of rapidly conveying critical information to communications providers regarding incidents impacting not only their own networks but also those of other critical infrastructure providers. NTCA encourages CISA to use this opportunity to work with the private sector and federal partners to identify methods of conveying actionable information building upon existing methods and resources.

Respectfully submitted,

*/s/ Tamber Ray*
Tamber Ray, Director of Policy
Lorna Gilmore, Policy Analyst

NTCA—The Rural Broadband Association

[15] 47 U.S.C. § 1302.