Before the
DEPARTMENT OF HOMELAND SECURITY
Washington, D.C. 20528

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

TO: Cybersecurity and Infrastructure Security Agency

COMMENTS OF WTA – ADVOCATES FOR RURAL BROADBAND

WTA – Advocates for Rural Broadband ("WTA") submits its comments with respect to the Cybersecurity and Infrastructure Security Agency's ("CISA's") proposed regulations implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022's ("CIRCIA's") covered cyber incident and ransom payment reporting requirements for covered entities.

WTA is a national trade association that represents approximately 400 rural local exchange carriers ("RLECs") that provide voice and broadband communications services predominately by wire but also by radio to some of the most rural, remote, rugged, sparsely populated and expensive-to-serve areas of the United States. WTA members have long constructed and operated rural voice and broadband communications networks – very often as providers of last resort – in high-cost farming, ranching, mining, mountain, forest and desert areas, as well as on Native American reservations and other Tribal Lands. The typical WTA member company serves fewer than 5,000 customers per service area and has fewer than 50 employees.

It appears that many WTA members and other RLECs are likely to be "covered entities" under CISA's proposed definition that establishes cyber incident reporting requirements for entities that provide communications services by wire or radio communications to the public, business or

government [47 U.S.C. §§153(40) and 153(59)]. This means that the staffs or consultants of WTA members and other RLECs will be required to prepare and file cyber incident reports with CISA, the Federal Communications Commission ("FCC") portal [which shares information with the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI")], other federal agencies such as the Federal Trade Commission ("FTC"), and frequently one or more state, local and/or Tribal agencies. Such reports generally will be required at the very time that the relatively small staffs of these RLECs are busy assessing the extent of a cyber intrusion and the resulting damage, while restoring any interrupted service and repairing their networks and databases. In many instances, the required multiple incident reports will entail substantial and inefficient complexities because they will involve different formats and information, and will be required to be filed in different places according to different deadlines.

Harmonization of Incident Reporting Requirements

WTA applauds CISA's accurate recognition that covered entities are increasingly subject to multiple, potentially duplicative requirements to report cyber incidents at the Federal and state, local, tribal and territorial (SLTT) levels. 89 Fed. Reg. 23653 (April 4, 2024). It fully supports CISA's commitment to explore ways to harmonize its cyber incident reporting requirements with those of existing Federal reporting regimes.

WTA believes that CISA can and should negotiate and enter into an interagency agreement with the FCC as soon as practicable in order to harmonize and share the cyber incident reports submitted to the portal that the FCC currently operates and shares with the USSS and FBI. CISA should employ an interagency agreement as well as the substantially similar reporting exception to CIRCIA in order work with the FCC, USSS and FBI to establish a single common reporting requirement, a single reporting form and a single reporting deadline that would allow all four

agencies to access and share in an efficient, effective and economic manner the cyber incident reports submitted by WTA members and other covered communications service providers to the FCC portal.

WTA would further encourage the extension of a CISA-FCC-USSS-FBI interagency sharing arrangement for the FCC portal to include as many as feasible of the other federal, state, local, tribal and territorial agencies having cybersecurity jurisdiction over WTA members and other covered communications service providers. Whereas a single common portal and procedure for reporting all cyber incidents affecting the communications sector would be ideal, any significant reduction in the number of separate reports, procedures and deadlines affecting large, midsized and small communications service providers would minimize reporting complexities and reduce training and other reporting costs.

And whereas harmonization and consolidation of incident reporting requirements will benefit both regulators and communications service providers of all sizes, they will particularly help to address the growing burdens and costs imposed by cybersecurity requirements upon RLECs and similarly situated communications service providers. WTA urges CISA to recognize that the rural networks of RLECs are subject to cybersecurity risks and regulations, but are not lucrative, cash-rich businesses that can readily bear large cybersecurity costs. Most RLECs provide "last mile" voice and broadband distribution lines to their sparsely populated rural service areas, but lack the customer bases and economies of scale to develop profitable content, advertising and other complementary service lines. Most of WTA's RLEC members rely upon federal universal service support to cover their high per-customer capital and operating costs while keeping their broadband service rates at affordable levels.

WTA notes also that cybersecurity costs are not only substantial but also rapidly increasing for RLECs without any assurance that they can adequately and consistently protect against the constantly changing tactics and targets of cyber criminals and hackers. These growing cybersecurity costs include, but are not limited to:

1. Hardware and software needed to monitor networks and databases for cyber intrusions, and to protect against actual and potential intrusions;

2. Hiring and retention of cybersecurity professionals or consultants (with recognition that many RLECs have substantial difficulties in hiring and retaining competent and qualified cybersecurity personnel);

3. Training and updating their customer service and technical staffs to recognize the multiplicity of new and differing intrusion ploys and tactics, and periodic reviews and revisions of cybersecurity procedures and responsibilities;

4. Acquisition and update of cybersecurity insurance policies, and continuing review and compliance with the evolving terms and conditions of such policies; and

5. Discovering, assessing damage, notifying affected customers, and recovering from intrusions affecting billing contractors and other third-party vendors as well as their own RLEC networks and databases.

WTA's point is that cyber incident reporting is only one of the multiple responsibilities and costs inherent in cybersecurity, and is likely to occur at the very time that the staff of an RLEC is overwhelmed by "all-hands-on-deck" priorities to investigate, analyze and recover from potential cyber intrusion damage to its network, databases and customers. The most efficient and effective step that CISA can take with respect to CIRCIA reporting is to reduce the number of reports, report forms and reporting deadlines as much as possible – with a single portal and a single set of procedures, forms and deadlines as the ideal approach. This will prevent inundated covered entity staffs (and particularly the limited staffs of RLECs) from having to research, keep track of and respond to multiple agencies, filing deadlines and reporting forms and requirements at a time when they are deluged with pressing fact-finding and damage recovery obligations.

Definitions

WTA recognizes that it is extremely difficult to develop a practicable set of definitions to govern cyber incident reporting for a very diverse group of large, mid-sized and small entities operating in many different industries throughout the wide expanse of the United States and its territories. WTA will focus here on the term "covered cyber incident" and the term "substantial cyber incident" that is used to define it.

WTA understands that CISA wants to know about the occurrence and relevant details of certain types of cyber intrusions and incidents, while WTA members want to know whether they need to report a particular cyber incident to CISA. These different perspectives are very likely to result in ambiguity, uncertainty and differing concepts of what is and what is not a "covered cyber incident." This problem is particularly complicated by the terms "substantial cyber incident" and "substantial loss" and "serious impact" because what is "substantial" or of "serious impact" to CISA and to individual service providers of widely differing types and sizes will vary significantly.

The proposed definition of "covered cyber incident" as "a substantial cyber incident experienced by a covered entity" is not helpful to an RLEC or other service provider that needs to determine whether to report an incident to CISA. In turn, the definition of a "substantial cyber incident" is full of ambiguities and uncertainties that do little to help a service provider to determine whether a particular cyber incident needs to be reported.

The proposed definition of "substantial cyber incident" as one that leads to any of the following circumstances offers little guidance to an RLEC regarding whether a particular incident needs to be reported. Specifically:

1. A substantial loss of confidentiality, integrity or availability of a covered entity's information system or network. [How does an entity determine whether it has suffered a reportable "substantial loss"? Is "substantial" to be measured on a national basis or on an individual company basis? If the latter, is it to be measured in terms of percentage of affected records or network, the

time that system or subsystem is down, the number of affected customers, the estimated monetary loss, or something else? An attack that shuts down the entire network may be easy to class as "substantial," but what if the shutdown is only of short duration or only a portion of the network is affected? And what about the frequent case where an intrusion is not discovered for weeks or months after it has occurred?]

2. A serious impact on the safety and resiliency of a covered entity's operational systems and processes. [How does an entity determine whether it has suffered a reportable "serious impact"? Does some portion of its operational systems or processes have to be rendered inoperable? For how long? What percentage of the entity's operational systems or processes needs to be affected? What is the nature and extent of the serious impact?]

3. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services. [Is this any disruption, or one that lasts for more than a certain amount of time or that affects more than a certain portion of an entity's operations?]

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 compromise of certain third-party providers (cloud service, managed service, third-party data host or supply chain). [Is this any and every unauthorized access, or does an unauthorized access have to be for at least a certain amount of time and impact at least a certain minimum portion of the entity's network, data or customers?]

Perhaps these definitional problems can be more effectively addressed, or at least their ambiguities and uncertainties reduced, if and when CISA harmonizes and consolidates with the FCC portal its reporting requirements for communications service providers. If not, CISA will need to revisit the term "substantial" or employ alternative terms in order to determine and clearly designate what cyber incident information it wants from entities of differing sizes in various industries and to give such entities more clear and detailed guidance regarding whether and what they need to report to CISA.

Perhaps national reporting standards and definitions are too broad to provide useful guidance to the multiple covered entities of varying sizes in the diverse industry sectors involved. Perhaps CISA should develop different definitions of "covered cyber incident" and "substantial cyber incident" designed for specific industry sectors and then further refined for companies of varying sizes (large, mid-sized and small) within each sector. WTA would be willing to work with

CISA to develop such reporting definitions and standards for RLECs and other small companies in the communications industry sector.

Reporting Deadlines

A major advantage of a common cyber incident reporting portal is that there would be a single specific reporting deadline or period rather than a complicated and confusing variety of multiple reporting deadlines and periods for different federal, state, local and tribal agencies. However, WTA believes CISA's proposed 72-hour reporting deadline is unreasonably short for an RLEC or similarly situated company whose limited staff may still be trying to determine the extent of the intrusion and damage during the first 3-to-5 days after discovery of an intrusion, much less engaging in critical recovery, rebuild, notification, insurance and other essential matters.

One alternative would be to require RLECs and similarly situated companies to file a simple report within 72 hours stating that a cyber intrusion had taken place or been discovered, and providing in one or two sentences a general description of what was known about the incident at that time. The affected RLEC would then be required to file a more detailed report in the required format within a reasonable period – for example, seven (7)-to-ten (10) business days after the initial notice.

A second alternative would be to give RLECs and similarly situated companies an automatic seven (7)-to-ten (10) business day extension beyond the initial 72-hour reporting period, if requested.

These proposed extended reporting periods recognize the difficulties, complexities and special circumstances involved in continuing to operate critical communications networks while investigating and recovering from cyber intrusions. They ensure that CISA and other agencies will get the notices and information needed to perform their duties while allowing affected RLECs and

similarly situated companies to operate and restore their networks while conducting accurate investigations of cyber intrusions.

Record Retention

WTA does not oppose CISA's proposed two-year period for retention of covered cyber incident records. However, it is not clear exactly what records will be required to be retained. WTA believes that it is reasonable to retain both initial and follow-up covered cyber incident reports and any working papers and other documents related to their preparation. However, unless CISA or another agency with jurisdiction to investigate an incident requests additional information (for example, back-up system or database files) within twenty (20) days after the initial covered cyber incident report, such information should not be required to be retained. Many RLECs archive their backup network and database files in a manner that would become extremely cumbersome and expensive if they were required to be accessed at a later date to identify the corruption resulting from a cyber incident.

Confidentiality of Cyber Incident Reports

WTA believes that CISA should retain cyber incident reports for a similar limited period – for example, the same two-year period for which it required covered entities to retain their covered incident report records.

WTA further agrees that covered cyber incident reports should be deemed highly confidential and exempted from Freedom of Information Act ("FOIA") requests for public access. These reports are intended to improve national, service provider and customer security, and to discourage and minimize cybercrimes and hacking. They should not be publicly available for potential use by intruders to identify soft targets or by competitors to use for advertising or other commercial advantage.

Conclusion

WTA emphasizes that its RLEC members are willing to take the cybersecurity steps necessary to protect not only their networks and customers, but also the nation and general public. However, in light of the substantial and growing capital and operating costs of defending against evolving cybersecurity threats, WTA urges CISA to harmonize and consolidate its cyber incident reporting requirements as much as possible in order to minimize their complexities and costs. With respect to the communications sector in which its RLEC members operate, WTA asks CISA to employ interagency agreements as well as the substantially similar reporting exception to CIRCIA in order work with the FCC, USSS and FBI to use the existing FCC portal to establish a single common reporting requirement, single common reporting form and single common reporting deadline that would allow all four agencies to access and share the cyber incident reports submitted by covered communications service providers in an efficient, effective and economic manner.

WTA encourages the extension of a CISA-FCC-USSS-FBI interagency sharing arrangement for the FCC portal to include as many as feasible of the other federal, state, local, tribal and territorial agencies having cybersecurity jurisdiction over WTA members and other covered communications service providers.

WTA further proposes that CISA revisit its proposed definitions of "covered cyber incident" and "substantial cyber incident" to clearly designate what cyber incident information it wants from entities of differing sizes in various industries and to give such entities clear and detailed guidance regarding whether and what they need to report to CISA.

Finally, WTA recommends that CISA relax or extend the its proposed 72-hour deadline for over-burdened RLECs and similarly situated companies to file their initial cyber incident reports, or to make extensions readily available. WTA also asks CISA to clarify what cyber incident

records need to be retained by both CISA and covered entities for two years, and to make sure that all cyber incident reports are kept strictly confidential and exempt from FOIA disclosures.

Respectfully submitted,
WTA – ADVOCATES FOR RURAL BROADBAND
/s/ Derrick B. Owens
Senior Vice President of Government and Industry Affairs
/s/ Eric Keber
Vice President of Government Affairs
/s/ Gerard J. Duffy
Regulatory Counsel
400 Seventh Street NW, Suite 406
Washington, DC 20004
Phone: (202) 548-0202

Dated: June 14, 2024