

**Before the
Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Washington, D.C. 20032**

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

**COMMENTS OF
THE NATIONAL ASSOCIATION OF BROADCASTERS**

I. INTRODUCTION

The National Association of Broadcasters (NAB)¹ submits these comments in response to the Cybersecurity and Infrastructure Security Agency’s (CISA) Notice of Proposed Rulemaking (NPRM) soliciting comments on proposed rules implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA requires certain “covered entities” that operate in a critical-infrastructure sector to report cyber incidents to CISA within 72 hours for “substantial cyber incidents” and 24 hours for ransomware attacks.² The CISA rule defines covered entities to include entities that provide wire or radio communications services to the public, business, or government, including one-way communications services

¹ The National Association of Broadcasters (NAB) is the nonprofit trade association that advocates on behalf of free local radio and television stations and broadcast networks before Congress, the Federal Communications Commission and other federal agencies, and the courts.

² *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*, Notice of Proposed Rulemaking, Docket No. CISA-2022-0010, at 21 (Apr. 4, 2024) (NPRM).

providers (e.g., radio, television, satellite).³ The proposed rule defines a substantial cyber incident as a cyber incident that meets at least one of four impact-based criteria.⁴

NAB supports CIRCIA's goal of preserving national security, economic security, and public health and safety,⁵ and we welcome the opportunity to assist CISA in securing our nation's critical infrastructure. But we believe that CISA's proposed rule, as written, would subject broadcast stations to significant reporting obligations that do not necessarily relate to a station's core critical-infrastructure activity – namely, emergency alerts. We also note that, in general, the reporting requirements are quite onerous and would require significant resources that would disproportionately fall on local stations. Finally, we request that the SBA's small-business criteria be applied to small broadcast stations, as the reporting burden likely will be acutely felt by these entities, which typically have few employees and minimal financial resources.

II. CISA's Proposed Rule is Overbroad and Requires Tailoring to Capture the Cyber Incidents that Have a Significant Impact on Emergency Alert Systems

According to CISA, CIRCIA's primary purpose is to “help preserve national security, economic security, and public health and safety.”⁶ CIRCIA further calls on CISA to identify covered entities that, if attacked, would cause “damage, disruption, or unauthorized access . . . [that] will likely enable the disruption of the reliable operation of critical infrastructure.”⁷ In

³ NPRM at 147-49 (identifying the communications sector as meeting sector-based criteria, and in particular, noting that “radio and television broadcasters” fit within the criteria).

⁴ *Id.* at 73-77 (explaining whether a cyber incident meets one of the four impact-based criteria).

⁵ *Id.* at 31.

⁶ *Id.*

⁷ *Id.* at 32 (quoting CIRCIA).

addition, the NPRM states that the statute also authorizes CISA to perform trend and threat analysis, engage in vulnerability and mitigation assessment, provide early warning signs, engage in incident response and mitigation, support federal efforts to disrupt threat actors, and advance cyber resiliency.⁸ While likely true, each of those purposes are in service of protecting critical infrastructure, which for broadcasting means EAS. As the NPRM notes, CISA's primary purpose for including one-way communication services like radio and television broadcasting services is because a cyber incident "has the potential to significantly jeopardize public health and national security by crippling *the government's* ability to distribute important information quickly."⁹

The proposed rule, however, goes far beyond the EAS system and would require broadcast stations to report cyber incidents that have no impact on a station's ability to deliver emergency alerts. A few hypothetical scenarios bring this into focus:

- If a denial-of-service attack leads to an outage of streamed content from a radio or television broadcaster's website, a station may have a degraded or lost ability to stream content, but its ability to transmit emergency alerts would remain intact.
- If a ransomware attack locked up a music vault for a radio station, the radio station may not be able to play music, but it very well could provide emergency alerts.
- If a cyber-incident resulted in a data breach that affected advertiser information, such a breach would not necessarily affect a station's ability to deliver emergency alerts.¹⁰

⁸ *Id.* at 33-34.

⁹ *Id.* at 148 (emphasis added).

¹⁰ See *id.* at 121 (recognizing advertising firms as an illustrative example of an entity that is not considered critical infrastructure).

Thus, a cyber incident might meet the qualifications of CISA's definition for a reportable event, but those incidents would not necessarily have impacted a broadcast station's emergency alert systems. Under CISA's rule, broadcast stations also may have ongoing "supplemental" reporting obligations to update CISA on the outcome of the incident.¹¹ And stations would face these reporting obligations all while they are trying to respond to the cyber incident in the first instance. We therefore urge CISA to narrow its definition of a covered cyber incident to only target those substantial incidents that impair a station's critical portion of the station's critical-infrastructure service, emergency alerts.

If CISA, however, declines to modify the definition of a cyber incident, we suggest that CISA consider narrowing the scope of the information requested.

III. CISA's Proposed Rule Should Be Streamlined to Minimize Reporting Requirements

CISA's proposed rules identify an extraordinary amount of information that broadcasters would be required to report in the event of a cyber incident. For all CIRCIA reports, broadcasters would have to identify the type of report, provide details about the broadcaster's identity (e.g., name, state of incorporation, affiliated trade names, organizational type, physical address, website, any internal incident tracking number, applicable business numerical identifiers, name of the parent company or organization), details about the individual submitting the report (e.g., name, email address, phone number, title, point of contact if the covered entity uses a third party, the registered agent for the covered entity), and an attestation from the covered entity if it uses a third party to submit the report.¹²

¹¹ *Id.* at 219-21.

¹² *Id.* at 423-24 (listing the requirements under proposed 6 C.F.R. § 226.7).

In addition to that baseline information, for covered cyber-incident reports, the broadcast station will have to describe within 72 hours:

- the incident with precise details about the devices and information systems affected;
- the technical details and physical locations of those items of those devices or networks;
- information about whether any of those devices support the intelligence community or has been determined by the federal government to require protection against unauthorized disclosure for reasons of national defense or foreign relations;
- a description of any unauthorized access, regardless of whether the covered cyber incident involved an attributed or unattributed cyber intrusion; identification of the impact;
- a list of dates and timelines relating to the incident; the impact of the incident on the covered entity's operations; a description of information that may have been accessed;
- a description of any vulnerabilities that might have been exploited;
- a description of any security defenses in place;
- a description of the type of incident and the tactics, techniques, and procedures used to perpetrate the covered cyber incident; any indicators of compromise;
- a description and copy of any malicious software; any information about the individuals who perpetrated the cyber incident; a description and details of any mitigation actions; and

- any other data required by the CIRCIA Incident Reporting Form.¹³

For ransomware, the broadcaster will have to describe within 24 hours much of the same information as is required by the covered cyber incident except they will have to provide additional details about the ransomware payments and any instructions arising out of the ransomware incident.¹⁴ The proposed rule also incorporates an ongoing supplemental reporting requirement that would compel a broadcast station to provide supplement updates to CISA if any substantial new or different information became available.¹⁵ For both categories of information, CISA would require the entity to preserve such information for two years.¹⁶

Make no mistake: This is an extraordinary amount of information to collect and submit in a short period. Moreover, the information-preservation requirements would compel stations to hold a large volume of information for a significant amount of time. While large entities may appear to have more resources to respond to these requirements, for broadcast stations, these reporting requirements will create significant information gathering and preservation responsibilities on the affected individual stations and even among those that are a part of a broader ownership group. As a result, individuals at each local broadcast station very likely will have to shoulder the burden of gathering and submitting this information within the requisite time. Of course, as we discuss further in the next section, the burden on small-sized broadcasters will be even more acutely felt given the resource constraints of those stations.

¹³ *Id.* at 424-37 (listing the requirements under proposed 6 C.F.R. § 226.8).

¹⁴ *Id.* at 427-30 (listing the requirements under proposed 6 C.F.R. § 226.9).

¹⁵ *Id.* at 419 (listing the supplementing reporting requirement under proposed 6 C.F.R. §226.3(d)).

¹⁶ *Id.* at 434 (identifying a preservation period under proposed 6 C.F.R. § 226.13(c)).

There is, however, an alternative. CISA has in place today an interim mechanism for voluntarily reporting cyber incidents that is far more streamlined. In contrast to the massive multi-part form that asks broadcasters to sleuth out every forensic detail of the cyber incident, CISA's current framework requests the ten most important pieces of critical information that shed light on the most salient information regarding the cyber incident.¹⁷ We believe that this current variation of the framework or some modest variation of this framework would enable CISA to collect the key, timely information about the cyber incident without overburdening broadcast stations. We also recommend shortening the information-preservation period to minimize the burden on stations to maintain cyber-incident records.

If CISA declines to make such an adjustment for all broadcast stations, we at least ask CISA to consider providing some reprieve to small broadcast stations given their personnel and resource constraints.

IV. CISA's Proposed Rule Should Exempt Broadcasters that Meet the SBA Size-Based Criteria from Having to Comply with CISA's Proposed Reporting Requirements

CISA's proposed rule exempts certain entities from cyber-incident reporting requirements based on size-based criteria. In particular, the rule exempts an entity operating in a critical-infrastructure sector that falls below the small-business-size standards specified in the North American Industry Classification System Code (NAICS) in the U.S. Small Business

¹⁷ Cybersecurity & Infrastructure Security Agency, Sharing Cyber Event Information: Observe, Act, Report (Apr. 2022), https://www.cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf.

Administration's small-business-size regulations. In proposing to exempt certain smaller entities, CISA made three findings following criteria outlined by CIRCIA:

- Exempting smaller entities would not deprive CISA of crucial information relating to the disruption of national security, economic security, or public health and safety;
- Smaller entities are less likely to be the targets of cyber incidents; and
- Smaller entities are less likely to own critical infrastructure.

For some reason, CISA proposed excepting television and radio broadcasters from these size-based exemptions. This decision is misplaced for a few important reasons, and moreover, we note that failing to exempt small broadcasters in particular would impose an acute reporting burden on those resource-constrained stations.

First, CISA considered the consequences of a disruption on national security, economic security, or public health and safety when it applies to a smaller entity and found that the effect would be muted for certain small businesses. The NPRM illustrates this point when it notes that not applying the rule to mom-and-pop drugstores, a small independent farm, a bed and breakfast, or a doctor's office are less likely to have an adverse effect than it would to a large retail drugstore chain, an industrial food conglomerate, a multinational hotel chain, or a large health system (respectively). Indeed, the same can be said for a small television or radio station, particularly as it relates to non-critical services that do not affect emergency alerts.

Second, CISA considered the likelihood that an entity would be targeted by a cyberattack. The NPRM provides ample evidence that larger entities are at a higher risk of being targeted but makes no findings that small broadcast stations are more likely to be the targets of debilitating cyber incidents.

Third, CISA contemplated the likelihood that a cyber incident may damage, disrupt, or result in unauthorized access to an entity's infrastructure in such a way that would impair the

reliable operation of critical infrastructure. But as discussed in Section II, the rule as written does not just target a broadcast station's critical infrastructure; rather, it targets all broadcast-station operations.

For small broadcasters, all three of these considerations weigh in favor of granting an exemption or, at a minimum, relaxing the rules for these stations. Many small broadcast stations only have a handful of employees, and their time is often divided serving many different capacities at these stations. These employees also must comply with FCC regulations that come with the FCC's own paperwork requirements and reporting certain incidents to the Federal Bureau of Investigation and local emergency officials. And, to the extent there is a substantial cyber incident, these multi-functional employees may be occupied responding to the cyber incident. This additional reporting requirement will only further stretch resource-constrained broadcasters.

To address this resource concern, we exhort CISA to consider extending the small-business exemption to broadcasters. We otherwise request that CISA consider narrowing for small broadcasters the definition for a covered incident to target only those elements of the business that relate to providing critical-infrastructure services. As discussed in Section III, we also ask that CISA consider applying narrower reporting requirements for broadcasters that meet SBA's size-based criteria to reporting the ten key pieces of information that CISA currently requests as a part of its voluntary reporting regime. We also suggest shortening the record preservation requirement for small broadcast stations. Finally, we ask that the FCC consider extending the reporting timeline for broadcasters that meet SBA's sized-based


criteria to allow for more than 72 hours for cyber incidents and more than 24 hours for ransomware incidents.

V. Conclusion

Although NAB supports CIRCIA's broader goal of safeguarding our nation's critical infrastructure against cyber-attacks and does not object to the CISA's proposal to implement CIRCIA's mandate to create cyber-incident reporting requirements for critical infrastructure sectors, we believe the rules, as written, are overbroad, request information about cyber- incidents that are unrelated to critical-infrastructure operations and are burdensome to broadcasters – particularly, small broadcasters. We therefore request that CISA consider narrowing its definition of a cyber incident and relax the extent of its reporting requirements.

Respectfully submitted,

**NATIONAL ASSOCIATION OF
BROADCASTERS**
1 M Street, SE
Washington, DC 20003
(202) 429-5430



Rick Kaplan
Nandu Machiraju
Larry Walke

July 3, 2024