OCHIN

A driving force for health equity

Submitted via www.regulations.gov

July 3, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

Re: *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements*

Dear Director Easterly,

On behalf of OCHIN, I appreciate the opportunity to provide comments on the Cybersecurity and Infrastructure Agency's (CISA) proposed rule to implement the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) requirements. OCHIN is a **national nonprofit health information technology and research network** comprised of over 2,000 community health care sites and 33,000 providers serving more than 6.1 million patients and includes Critical Access Hospitals (CAHs), rural and frontier health clinics as well as federally qualified health centers (FQHCs) and local public health agencies in 43 states. Following the February Change Healthcare cyberattack, which required rebuilding hundreds of cyber interfaces in our network, it is important more than ever that we secure our nation's critical infrastructure from criminal elements and adversarial nation-states and support sharing of information on cyber incidents to support patient care and safety. **We share CISA's goal to protect our country's critical infrastructure. To that end, we recommend several clarifications and modifications to the provisions of the proposed rule. The current proposal would have unintended results that would undermine the cyber readiness of CAHs and other under-resourced providers and impose requirements they cannot meet without funding and essential resources. We urge CISA to provide additional hardship exemptions for smaller organizations, among other recommendations.**

OCHIN CYBERSECURITY AND IMPACT

Since its inception in 2000, the OCHIN collaborative of community providers has focused on expanding access in underserved and rural communities to quality health care services through technology solutions, technical assistance, operational support, informatics, evidence-based research, workforce development and training, and policy.

OCHIN is committed to protecting the privacy and security of the health information of our members' patients and securing their operations and has represented their voices in the Health Sector Coordination Council (HSCC) Cybersecurity Working Group to ensure recommendations and policies leveraged reflect their needs, concerns, and input. The ramifications of the February Change Healthcare cyberattack impacted operations and resulted in the re-allocation of resources to re-build and reconnect to interfaces to as well as reroute claims for 510 payers used by OCHIN members, many of whom are already facing significant sustainability challenges. These interfaces were disconnected to address the

breach, which needed to be rebuilt and reconnected. Four months later, we are still working with our members on the aftermath of the incident resulting in increased costs and the need to redirect OCHIN staff who normally support members in care delivery and innovation to aid in dealing with the effects of the cyberattack. Even prior to the cyberattack, safety-net providers have been experiencing financial stress as the Medicaid unwinding has directly impacted their financial sustainability as more of their patients are under- or uninsured and a fewer are covered under Medicaid. Our members do not have the financial margins nor the capital reserves of large health systems or large private practices.

RECOMMENDATIONS

OCHIN offers the following global recommendations to ensure providers in rural and underserved communities can report cyber incidents in a manner that optimizes cybersecurity without exacerbating a crisis in the event of a breach. We include more detail in the **Appendix**.

- **Invest in modernized health IT for CAHs and other providers in underserved and under-resourced communities that include essential 21st cybersecurity features.** There is an urgent need for investments to upgrade health IT systems of rural providers, including CAHs, to strengthen the cybersecurity ecosystem which is interconnected. While CISA does not have funding for this purpose, the Agency should communicate the urgent need for these types of investments to Administration officials and Congress as CAHs are at a disadvantage where both technology and workforce challenges disparately impact their ability to strengthen their cyber defenses and provide care for their communities.
- **Immediate funding is needed to increase the number of cybersecurity staff among underserved providers and rebuild the community health clinic operational and support staff with health IT training that includes cybersecurity.** Significant and immediate investments by the Biden Administration is needed to address the ongoing cybersecurity workforce shortage. Personnel are needed to maintain cyber defenses and, in the event of a reportable incident, provide accurate cybersecurity incident reporting. Without additional funding and trained staff, the reporting obligations increase financial pressure and divert resources from patient care for CAHs and other under resourced organizations. In rural communities this will exert more financial pressure that is leading to an alarming rate of closures and reduced access to healthcare. **Again, CISA is uniquely positioned to deliver this information to Administration leadership and sister agencies where funding is available to fund health IT infrastructure upgrades and cybersecurity resiliency (such as the USDA community connect grant program and the FCC's Rural Health Care Program's Healthcare Connect Fund program).**
- **Include specific Healthcare and Public Health (HPH) Sector-based criteria rather than allowing certain entities to determine for themselves if they meet the proposed criteria.** Specifically, HPH Sector-based criteria should include health insurance companies, third-party administrators of health plans, and healthcare clearinghouses. Unless CISA explicitly includes these third parties into the HPH Sector-based criteria, they will not be subject to CIRCIA if they self-assess that they do not meet the proposed criteria. Mandating their inclusion will ensure organizations such as Change Healthcare are implementing essential cybersecurity hygiene and reporting.
- **Align federal and state reporting timeline requirements and standards so they're not duplicative, burdensome, overwhelming, nor divert critical resources.** We strongly recommend CISA coordinate with other federal agencies, such as the Department of Health and Human Services (HHS), including HHS' Office of Civil Rights (OCR), and the Federal Trade Commission (FTC) to reduce any duplicative cyber incident reporting requirements. **CISA should also work closely with the Health Sector Coordination Council (HSCC) Cybersecurity Working Group,**

specifically the Under-resourced Provider Cybersecurity Advisory Group, and incorporate and prioritize the recommendations they offer. CISA should extend coordination efforts to state entities to harmonize reporting requirements given many states have existing data breach notification laws that could further complicate reporting for health care providers, especially those service rural, underserved, and under-resourced communities.

- **Include additional clarifications and modification to the proposed rule as it relates to the definition of "substantial cyber incident" as well as to the manner, form, and content of reports.** The existing definitions for mentioned sections of the proposed rule are vague and could potentially cause confusion and additional burdens to cover entities who need to report under CIRCIA. CISA needs to provide clear acknowledgement of resources required of CAH as a component of this reporting. Given the manner CISA will be collecting cyber incident reports, CISA should ensure any submitted confidential information is secure and continue bolstering their cybersecurity infrastructure.
- **Build flexibility around the timeframes for initial and supplemental reporting to accommodate quality reporting and allow cybersecurity professionals to address cybersecurity incidents.** The 72-hour initial reporting timeline required by CISA, and 24-hours required for supplemental reports is highly likely to place undue burden on cybersecurity professionals who are simultaneously trying to respond to a cyber incident. CISA should allow flexibility and require reporting entities to, in good faith, submit the least amount of information statutorily permitted within the 72-hour timeline to ensure quality reporting and allow cybersecurity professionals to respond to cybersecurity incidents. Similarly, CISA should also consider extending the 24-hour window to submit supplemental reports related substantial, newly discovered information or if the covered entity has made a ransom payment.

Please contact me at **stollj@ochin.org** to discuss how we can support the Agency's implementation of the proposed rule to strengthen cybersecurity—particularly for rural and other providers in underserved and underinvested communities.

Sincerely,

Jennifer Stoll
Chief External Affairs Officer

APPENDIX

Investments in Modernized Health IT

- **Too many providers in rural and underserved communities are using dated, fragmented technologies that lack essential cybersecurity features that hinder consistent and secure access, exchange, and use of standardized, uniform electronic health information.** They have not received the necessary funding to modernize their health IT systems which is essential to not only strengthening cybersecurity but achieving interoperability and electronic health information exchange, expanding access to care through telehealth and other virtual services; optimizing operations and financial sustainability through informatics and analytics that support transitions to new payment and delivery models; and leveraging the benefits of rapidly developing artificial intelligence (AI) systems. **We urge CISA to work with the Administration and Congress to drive investments in modernized health IT systems with essential cybersecurity features. We also urge CISA to reach out to sister agencies that do have funding to support such efforts including the USDA community connect grant program and the FCC's Rural Health Care Program's Healthcare Connect Fund program.** Working with these other federal departments and agencies is essential to ensuring that existing programs that directly work to redress the digital divide in health care are easily accessible to providers of rural, underserved, and under-resourced communities. Modernized health IT is key to maintaining a strong cyber infrastructure and cybersecurity defense practices.

Funding to Address the Ongoing and Critical Hospital Cybersecurity Workforce Shortage

- Essential and basic security measures require operational, support, and clinical staff with health IT training including foundational cybersecurity upskilling. Accessible cybersecurity workforce development and ongoing upskilling training for all health care staff is an urgent priority. Technical assistance and targeted funding for health IT training for staff of community health centers, CAHs, and local public health agencies is part of the equation to achieve enhanced cybersecurity readiness and reporting. **While we acknowledge CISA does not have jurisdiction under CIRCIA to allocate funding to address cybersecurity workforce shortage and training, CISA is in a unique position to communicate the urgent need for investments in cybersecurity workforce, especially for providers in rural, underserved, and under-resourced communities facing structural challenges.**

Sector-Based Criteria: Healthcare and Public Health Sector

- As part of CISA's proposal to include additional, sector-based criteria, we urge CISA to include health plans, health insurance companies, third-party administrators of health plans, and healthcare clearing houses under the HPH sector. As OCHIN members can sometimes rely on third-party services, any disruptions to these services can directly impact their operations – as exemplified by the Change Healthcare cyberattack, which caused massive disruption to, not only OCHIN member operations, but to other providers nationwide given its role in providing revenue cycle and payment management solution. **Given the vast amounts of patient data held by these third parties and the crucial role they play in keeping health care provider operations running smoothly, we strongly encourage CISA to include the third-party entities listed above in the final rule.**

- Additionally, the proposed definition acknowledges that substantial cyber incidents could occur through compromises of third-party services providers or supply chains. From an operational standpoint, it is intuitive that the entity that experiences the cyber-attack would have the information needed to complete the proposed required CIRCIA reporting requirements. **We request CISA make it clear that if a substantial cyber incident occurs at a third-party entity, they must be the covered entity to fulfill all CIRICIA reporting obligations if they serve, contract, or are legally engaged with any entities in an outlined critical infrastructure sector.**

Alignment of Reporting Timeline Requirements and Standards

- A key aspect of provider burnout is the complex array of reporting requirements necessary to adhere to the many facets of health care rules and regulations. Under-resourced providers in rural and underserved areas currently are reporting record high levels of burn out post COVID-19. This is further compounded by complicated and layered reporting that providers in underserved communities shoulder disproportionately and the short staffing due to limited resources. OCHIN members are already subject to substantial reporting requirements and enforcement under several federal reporting requirements under HIPAA and FTC, for example. Covered entities under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 should not be subject to multiple enforcement mechanisms for failure to provide similar information. **OCHIN strongly encourages CISA to coordinate with other federal agencies, including HHS, HHS' OCR, and FTC to reduce duplication of cyber reporting requirements.** Aside from the duplicative nature of requiring additional reporting, the added work will only serve to slow a provider's ability to deliver care following the incident. We recommend CISA align with and leverage existing federal cyber incident and data breach reporting requirements for consistency to lessen the burden on health care providers in rural, underserved, and under-resourced communities.
- We appreciate CISA's efforts to harmonize Federal cyber incident reporting requirement and encourage the agency to ensure active recruitment of stakeholders from rural, underserved and under-resourced areas be included in outreach to gain a whole understanding of the existing cyber incident reporting regulatory landscape and contribute their perspective on how best to harmonize existing cyber incident reporting requirements. CISA can do so by **engaging with the HSCC Cybersecurity Working Group's Under-Resourced Provider Cybersecurity Group**, which meets with providers to hear their perspectives about cybersecurity, financial and operational challenges, and what they need to meet cybersecurity obligations (e.g., key investments, other assistance). **The Cybersecurity Security Working Group also develops cybersecurity best practices and policy recommendations, which we encourage CISA to use to help inform its development of the final rule.**
- Existing state data breach notification laws could also potentially further complicate reporting requirements and could saddle health care providers with added challenges. As CIRCIA does not preempt any state data breach notification laws, **we ask CISA to clarify whether it will engage with state entities to align CIRCIA reporting requirements existing state laws and, if not, strongly urge CISA to proactively work with state entities to align CIRCIA reporting requirements with existing state laws on an ongoing basis, similar to its Federal harmonization efforts.**

Definition of "Substantial Cyber Incident"

- CISA's current definition of "substantial cyber incident" requiring submission of a Covered Cyber Incident Report is vague and could result in reports of cyber incidents that outside of CISA's intent. The definition in the proposed regulation includes the following qualifying threshold "(3) [a] disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services…" CISA asks whether they should "specifically add the term "significant," "substantial," or any other appropriate word at the beginning of subparagraph 3 of the definition of substantial cyber incident to clarify the impact level required." **OCHIN agrees that it would be appropriate to further clarify the impact level required by modifying subparagraph (3) to reflect "(3) A "*significant*" disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services."** Adding "significant'" further distinguishes the definition of "substantial cyber incident" from the definition of a "cyber incident" and aligns the definition with that of subparagraph (1) and (2), which outline the required impact level by using qualify phrases "a substantial loss of confidentiality" and "a serious impact on the safety and resiliency" to specify the required impact level.

Manner, Content, and Form of Reports

- *Confidentiality of Submitted Reports*
    - Under §226.8, covered entities have to submit CIRCIA Reports to CISA via a web-based CIRCIA Incident Reporting Form available on CISA's website (or in another form approved by the Director). **CISA should commit to ensuring the confidentiality of the web-based form and the database where records submitted will be stored.** CISA should provide covered entities with assurance that any confidential information submitted in a report will remain protected. CISA should also clarify who will be able to view submitted data. **We also urge CISA to continue strengthening its cybersecurity infrastructure before the implementation of reporting requirements.** Otherwise, the manner in which reports are collected could potentially serve as a central location containing covered entities' information systems, networks, or devices to be breached or compromised.
    - CISA should allow covered entities to identify a notification contact if they choose to optionally register in advance with CISA so when CISA receives reports via the web-based form, the contact can receive a notification from CSIA to create awareness if unauthorized reports are submitted.

- *Evolving Reporting Requirements*
    - According to § 226.9(4)(n), covered entities will be required to submit "…[a]ny other data or information as required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6." Given the rapidly changing nature of cybersecurity incidents, OCHIN understands there may changes to reporting needed. The ambiguity of the requirements in this section may be intentional meaning CISA would have the opportunity to change reporting requirements without public input or notice leaving cybersecurity professionals with the challenges of searching for new or different information for each cybersecurity incident, which could further exacerbate the impact of cybersecurity incident by calling their attention to something new or novel for each incident. **OCHIN acknowledges the need for flexible reporting but asks CISA to ensure any additional reporting contained on the website**

be voluntary and that any additional reporting requirements be subject to stakeholder input and review with a minimum of 30 days' notice.

Report Timing and Deadline Submissions

- As CISA considers what should be included in CIRCIA reports, **OCHIN would like to note that the amount of information available at the 72-hour mark of a significant cyber incident will be limited and may not be of quality** – cybersecurity professionals may not yet know the exact details of the cyber incident occurred. The 72-hour reporting requirement could also hinder a covered entity's response to cybersecurity incidents, as such, CISA should require covered entities to instead make a good faith effort to submit the least amount of information statutorily permitted within the 72-hour timeline to ensure quality reporting and acknowledge that some details will only be included in supplemental reports.
- Moreover, CISA includes extensive initial reporting requirements that do not necessarily constitute quality reporting of incidents. **An initial report should instead be a clear, concise report that meets the statutorily permitted minimum reporting requirements that an incident has occurred and will be followed by more substantial supplemental reports.** This notifies CISA that an incident has occurred and ensures they received quality data about the incident.
- **We also encourage CISA to extend the reporting deadlines for supplemental reports from 24 hours (as outlined in § 226.5) to at least 48 hours.** Supplemental reports are important for facilitating the communication of substantial, newly discovered information or if the covered entity "makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf". However, CISA's proposal that covered entities "must promptly submit supplemental reports to CISA" until the incident is fully addressed poses a challenge to health care providers, especially given CISA's interpretation of "promptly" as "within 24 hours of the triggering event." The frequency of report submission could place undue burden on covered entities and the cybersecurity professionals who are simultaneously trying to quell the ensuing crisis of a cyber incident. Extending the reporting deadlines for supplemental reports allows CISA to still achieve its goal of receiving additional information through supplemental reports and for those responding to cyber incident to focus their efforts while meeting the reporting requirements.