ConnectedHealthInitiative

July 3, 2024

Cybersecurity and Infrastructure Security Agency
Department of Homeland Security.
245 Murray Lane
Washington, District of Columbia 20528-0380

RE: Comments of the Connected Health Initiative, *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements* (89 FR 23644)

The Connected Health Initiative (CHI) writes to provide input to the Cybersecurity and Infrastructure Security Agency (CISA) on its proposed rules implementing provisions of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) addressing covered cyber incident and ransom payment reporting requirements for covered entities.[1]

CHI is the leading effort by stakeholders across the connected health ecosystem to enable the responsible deployment and use of digital health tools throughout the continuum of care, supporting an environment in which patients and consumers can see improvements in their health. Across a range of touchpoints in the healthcare ecosystem, we seek essential policy changes that will enable all Americans to realize the benefits of an information and communications technology-enabled American healthcare system. For more information, see www.connectedhi.com.

We believe that CISA is well-positioned to serve as a leader and coordinator within the U.S. government with respect to realizing a more secure and productive healthcare sector (as well as in other critical infrastructure sectors), and that this request for information takes an important step in establishing this role. We applaud CISA's efforts and commitment to obtaining input from a diverse set of stakeholders, especially from the small business community, in the development of its approach to implementing the cyber incident and ransom payment reporting requirements of CIRCIA.

CIRCIA cyber incident notification requirements could impose serious obligations on the healthcare sector business community and on small businesses in particular. **In its implementation of CIRCIA, CHI urges CISA to prioritize the following:**

Establishing an appropriate reporting timeline. The regulation should reflect an appropriate, flexible standard for notifying government about significant cyber incidents.

[1] 89 FR 23644.

Covered entities may appropriately need to delay reporting if such reporting would disrupt an ongoing criminal or national security investigation, and CIRCIA reporting requirements should provide for such a delay when appropriate. Further, much may be discovered outside of the 72-hour timeframe after a cyber incident, and covered entities may need time to investigate an intrusion further, and to supplement an incident report. Covered entities should be given the ability to supplement a cyber incident, without penalty, after conducting initial mitigation and response efforts.

Appropriately scoping a reportable cyber incident and who must report cyber incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and confirmed cyber incidents. Some language being considered—such as "potential cyber intrusions" and incidents that could be "reasonably believed" to be reportable—is overly subjective. The definition of a covered cyber incident should be based on clear and objective criteria and should clearly differentiate between mere vulnerabilities and successful attacks that have caused harm. Building on Congress' intent in CIRCIA and CISA's remit, CISA's definition of a covered cyber incident that merits reporting should be limited to an incident that has a significant disruption to critical infrastructure operations. Reporting obligations should be extended only to companies that manage risks and disruptions to critical infrastructure, and size-based criteria that make CISA's coverage debilitatingly large should be avoided. Accordingly, we strongly recommend that CISA:

- Add "substantial" to the third prong of the "substantial cyber incident" definition;
- Add "substantial" to the fourth prong of the definition of a substantial cyber incident;
- Clarify the definition of "substantial cyber incidents" facilitated by a compromise of a cloud service provider (CSP) by confirming that such an in-scope incident relates to those within a CSP's or other third-party's area of responsibility; and
- Clarify in the fifth paragraph under the definition of "substantial cyber incident" that this text is not a separate impact prong.

Clarifying the key elements of an incident report. A cyber incident report should feature information such as how the attack was discovered; the vulnerability exploited and what metrics indicated the attack's success; what steps, if any, have been taken to mitigate the attack; and what the known impacts of the attack are. We encourage CISA to eliminate onerous reporting requirements and limit required detail of initial reports to facilitate faster reporting and reduce security risk. We also request that CISA clarify reporting requirements for covered entities subject to confidentiality obligations with Department of Defense (DoD) and Intelligence Community customers.

Providing needed liability protections. CISA should establish that the act of reporting a covered incident and the contents of any report, including supplemental reporting, do not unnecessarily subject a covered entity to discovery in any civil or criminal action, which would ultimately chill the public-private partnership construct needed for timely and appropriate cybersecurity incident reporting and collaborative efforts to mitigate harmful cyber incidents. Reporting entities, in essence, should not be penalized after

the fact for complying with a legal obligation. In addition, CISA is urged to tailor the amount of information that covered entities would be required to submit to the elements necessary to achieve CIRCIA's goals. There must be a compliance regime that treats cyberattack victims as victims, with a reporting program that encourages cooperation and strengthens trust between the public and private sectors. A regulatory-based approach that focuses on punitive actions, such as penalties like federal debarment, rather than mutual gains would run counter to the goal of creating a strong national partnership model to address the increasing cyber threats facing the United States.

Reporting to a victim entity or its designee, including an information sharing and analysis organization or center, should generally be limited. Cyber incident response service providers, such as cybersecurity firms, law firms, and insurers, should not be required to report incidents to government that have occurred on their customers' networks unless explicitly authorized by their customers to do so on their behalf. This approach would avoid unintended outcomes like compelling cybersecurity providers to disclose clients' sensitive business information in breach contractual obligations and/or dissuading businesses from employing outside experts to the detriment of businesses' cyber defenses.

Further, there needs to be a limit to the further use of information that is provided to the government under new CIRCIA incident reporting rules. Restrictions on government use of data should closely align with CISA 2015, which contains provisions to exempt reported information from federal and state disclosure laws and regulatory use; treat shared information as commercial, financial, and proprietary; waive governmental rules related to ex parte communications; and preserve trade secret protections and any related privileges or protections.

Harmonizing federal reporting requirements. Several critical infrastructure sectors, including the healthcare sector, have existing obligations to report significant cyber incidents to federal and/or state regulatory agencies. It is crucial that CISA's cyber incident reporting requirements are harmonized with such reporting requirements to the maximum extent possible to avoid the unnecessary burdens associated with monitoring and generating reports on the same incident for multiple agencies. In coordination with other federal agencies (such as the HHS Office of Civil Rights and the Federal Trade Commission), a single report leveraging existing reporting requirements should suffice to meet CIRCIA mandates. In addition, we request that CISA add a FedRAMP exception to avoid duplicative incident notification requirements under CIRCIA. CISA should also limit post-incident data preservation requirements to improve regulatory harmonization, reduce compliance burden, and improve security posture.

Providing certainty as to how CISA will share information and protect civil liberties. We request that CISA clarify when and how it will share information that may identify covered entities with other agencies and how CISA will safeguard that information. We further urge CISA to enhance protections for CIRCIA reports to protect security, privacy and civil liberties of victims, and to restrict the use of protected information against covered entities or their employees/executives.

Ensuring that CISA reporting requirements contribute to bidirectional sharing and collaboration. A true partnership between the private sector and government to mitigate cyber risks requires information to be bidirectional. Information reported to government needs to be promptly aggregated, anonymized, analyzed, and, when appropriate, shared more widely with affected stakeholders to mitigate and/or prevent further cyber incidents. To this end, we strongly encourage CISA to build on the existing public-private partnership with Information Sharing and Analysis Centers (ISACs), including the ISAC for the healthcare sector, as well as Information Sharing and Analysis Organizations, in shaping its CIRCIA reporting requirements. CHI is committed to working with CISA and other policymakers to strengthen U.S. national security and to protect critical infrastructure sectors that small businesses are key to. CISA needs to enhance agencies' situational awareness so that government can better inform and partner with businesses that become cyberattack targets or victims.

Clarifying CIRCIA enforcement. We urge CISA to limit debarment for noncompliance to the most egregious non-compliant entities, and for CISA to publicize these leading enforcements to raise awareness.

Educating and partnering with the digital health innovation community. Many in the CHI community face significant resource constraints as they operate in supply chains across the healthcare sector. CISA's partnership and resources will be critical to outreach, awareness, and education for these entities subject to new CIRCIA reporting requirements, particularly small businesses, and CISA's implementation of CIRCIA should include a robust education and support campaign focused on these entities.

CHI appreciates the opportunity to provide input to CISA on the importance of cyber incident and ransom payment reporting and looks forward to continued collaboration with CISA and other U.S. governmental partners.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005
p: +1 517-507-1446
e: bscarpelli@actonline.org