American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

July 2, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
1110 N. Glebe Road
Arlington, VA 20598

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

Dear Director Easterly,

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) appreciates the opportunity to provide comment to the Cybersecurity and Infrastructure Security Agency (CISA) on their proposed rule to establish reporting requirements for cybersecurity incidents under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).

America's hospitals are keenly aware of the escalating frequency and severity of cyberattacks against hospitals and health systems and recognize the need for incident reporting as part of a broader effort to understand the nature of these attacks. Analyzing cyber incidents and tracking ransomware payments is important to enable real-time pattern identification and information sharing. The information CISA gathers in these reports will improve the agency's ability to assist victims, analyze trends, and, crucially, disseminate preventive measures as cyber threats evolve. However, we have several concerns about this proposal and urge the agency to modify the reporting process such that in the immediate aftermath of a cyberattack, hospitals can provide vital information to the government without diverting crucial staff and resources away from containing the attack and addressing the aftermath.

Specifically, the reporting proposed by CISA is redundant to what is required by other federal agencies, adding unnecessary burden to what the hospital must do at the same

time that it is working to ensure patients are getting the care they need despite the crippling of vital electronic systems. Moreover:

- CISA and other agencies should guarantee data anonymity across all federal agencies.
- The applicability of the reporting rules is confusing — the rules should apply to the whole health sector given the operating interconnectedness of relationships among the health sector entities.
- The reporting requirements should be simplified as they present significant compliance and operational burdens and privacy risks to hospitals and health systems.
- Affected entities should have a clearer explanation of the potential penalties and when they would apply.
- The penalties are too harsh, especially when imposed on an organization that did not do anything wrong but instead was the victim of an attack by a group or nation-state with malintent.

Our detailed comments follow.

HARMONIZATION

Hospitals and health systems' handling of patient information is primarily regulated by the Office of Civil Rights (OCR) through enforcement of the Health Insurance Portability and Accountability Act (HIPAA). Patient information is also regulated by the Federal Trade Commission, specifically concerning data exchanges with non-HIPAA-covered entities. All 50 states and all U.S. territories have additional breach notification requirements, and 17 states now have distinct privacy rules that require incident reporting. CISA is aware of the lack of harmonization in cyber incident reporting; in the proposed regulation it notes that "Given the number of existing cyber incident reporting requirements at the Federal and SLTT [state, local, tribal and territorial] levels, CISA recognizes that covered entities may be subject to multiple, potentially duplicative requirements to report cyber incidents." This proposed rule offers no remedies to this problem and only states that CISA is "committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable and seeks comment from the public on how it can further achieve this goal." CISA's commitment to harmonization is notable, and we urge it to demonstrate that commitment by putting a unified solution in place with other federal agencies before adding another reporting requirement. **The AHA recommends that CISA immediately convene the appropriate federal and state agencies to agree on a single, uniform reporting process before introducing any new reporting requirements. A single web-based report based on the Information Sharing and Analysis Center (ISAC) model already used by CISA would be a great starting place for this discussion.**

Anonymity

As CISA continues to grapple with how to effectively share cyber incident data among various agencies, the AHA commends CISA for proposing that "CIRCIA Reports submitted pursuant to this part and responses provided to requests for information issued under § 226.14(c) are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3), and under any State, Local, or Tribal government freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records." **It is crucial that CISA ensure anonymity for entities reporting incidents under this proposed rule. CISA should add language that specifically guarantees that information contained in these reports will not be shared between federal agencies. This will ensure that criminal liability or civil monetary penalties will not be imposed on any entities complying with the reporting requirements of this proposed rule.** Without this guarantee, a federal agency could use a CIRCIA-defined incident report to start an investigation into a potential breach which, per one agency's current process, includes publishing information about the event before cause or responsibility is established.

Applicability

CISA's definition of "substantial cyber incident" is ambiguous, confusing and does not adequately consider the operational realities or complex interconnectedness of the field. CISA is proposing to define a cyber incident as "an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system." Unfortunately, none of the examples given by CISA are specific or quantifiable. Instead CISA relies on vague language such as "a 'substantial' loss will likely depend on a variety of factors, such as the type, volume, impact, and duration of the loss" and overly broad scenarios like "One example of a cyber incident that typically would meet the 'substantial' threshold for this impact type is a distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time." This is problematic because even with mission-critical systems the length of an outage may be irrelevant: a one-minute outage to one system could be devastating and, conversely, an outage that lasts weeks or months to another could be more of a manageable annoyance depending on system redundancies, failover protocols and downtime procedures.

Further confusing this definition is that the proposed rule also includes the impact of the entity's incident response actions as contributing to the incident's impact. The proposed rule states that "if a covered entity, in response to a ransomware attack or other malicious incident, decides to take an action itself resulting in reportable level impacts, such as shutting down a portion of its system or operations, to prevent possibly more significant impacts, this would still be considered a reportable substantial cyber incident." Quickly shutting down or taking systems offline to mitigate potential impacts is a common and widely recognized best practice for responding to visible and potential threats. Based on this logic, a hospital with a cyber incident response plan that errs on the side of caution when dealing with potential threats is effectively being punished for

having a proactive and laudable approach to dealing with cyber incidents. Because context matters here, **AHA recommends that CISA work with representatives of each sector to quantify the impact of events in unambiguous terms that do not disincentivize organizations to act swiftly and effectively to minimize the impact of an attack.**

For hospitals and health systems, this would mean things like the number of patients whose care was adversely impacted or whose privacy was compromised (the latter aligning with OCR breach notification requirements), the number of procedures disrupted or canceled, the necessity of diverting ambulances, the financial loss amounts that reach the level of operation disruption, etc. If CISA intends to collect data on cybersecurity events that are significantly disruptive and dangerous, the proposed rule should include additional qualifying language to better define those instances in which reporting will be required. **The AHA urges CISA to revise the definition of "substantial cyber incident" for clarity as the current language in the proposed rule will result in both excessive disclosures of cybersecurity incidents and the under-reporting of potentially significant events.**

Defining Entities

CISA seems to have made a concerted effort to lessen the reporting burden for smaller hospitals, going as far as to state that they are "not generally proposing to require reporting from smaller hospitals." We appreciate this recognition of the particular challenges such reporting could pose for these hospitals. However, when considering both the proposed rule's general and health sector-specific applicability criteria, very few, if any, hospitals would be exempt. Indeed, to be exempt from CISA's reporting requirements a hospital would need to meet all the following criteria:

- Have less than approximately $47 million in receipts.
- Not offer emergency services to a population equal to or greater than 50,000 individuals.
- Have fewer than 100 beds.
- Not be a critical access hospital (CAH).

Given that CAHs are some of the most under-resourced hospitals, it is unclear if there is any tangible benefit from offering these exemptions. In fact, the AHA estimates that less than 60 hospitals would benefit from this exemption. **A better way to reduce reporting burdens on overstressed hospitals is to simplify the reporting criteria such that all health sector entities can easily report incidents. If the reporting requirements cannot be sufficiently simplified so as not to burden any entity in the sector, then CISA should broaden the exemption criteria so that any hospitals below 100 beds, including all CAHs, would be exempt from these incident reporting requirements.**

The way the health sector is defined, and the fact that some health sector entities are excluded from reporting regardless of their size — including three types of entities critical to the underlying stability of the entire sector — demonstrates a flawed understanding of the interconnectedness of the health care ecosystem. CISA states, "In establishing these proposed criteria, CISA also considered including criteria related to health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities. Ultimately, CISA determined it was not necessary to include specific sector-based criteria for any of those three industry segments. In the case of health insurance companies and entities operating laboratories or other medical diagnostics facilities, CISA believes a sufficient number of entities already will be captured under the size-based criterion that applies across all critical infrastructure sectors ...."

Putting aside for a moment the considerable number of smaller specialty insurers, laboratories and others that provide services and exchange data with hospitals and health systems, it does not make sense to think of any health insurers and clinical laboratories as disconnected outliers. **In fact, they are health care entities, and all health care entities regardless of size are integral parts of the patient care continuum with shared risks and responsibilities regarding patient outcomes** as we saw during the COVID-19 pandemic. They are directly integrated with codependent technology such that the cascading impact of a single entity's system disruption can cripple the entire sector which was the case in the Change Healthcare ransomware attack.

Furthermore, CISA's consideration of health information technology (IT) providers reporting responsibilities in the proposed rule, they state that they believe that the "most common type of cyber incident such entities will face are data breaches. As data breaches are not the primary focus of CIRCIA, and those entities already are required to report data breaches of unsecured protected health information under the HIPAA Breach Notification Rule and personal health records under the HITECH Act Health Breach Notification Rule, CISA does not believe it is necessary to include a specific criterion focused on entities in the health IT industry." **The AHA strongly disagrees with this assessment. Attacks on hospitals and health systems are "threat to life" crimes. There are hundreds of devices and third-party technology systems operating in the health sector that are critical to patient care and hospital operations that do not handle or otherwise touch patient data. Additionally, in a ransomware attack, the breach may be only one of many issues, which was the case in the Change Healthcare attack, where the breach of data, though severe, was only one of many catastrophic operational financial disruptions to hospitals and health systems.**

Burdens and Risks

The proposed rule's reporting requirements present hospitals and health systems with significant compliance and operational burdens and privacy risks. First, as noted in the

"Applicability" section of this letter, the lack of clarity around the definition of a "substantial incident" coupled with the extensive amount of information that CISA is requesting in sections 226.6 through 226.8 and ransomware payments in sections 226.9 and 226.10 will require a lot of work to accomplish. The proposed timeline will distract the hospital or health system's cyber security, IT, legal, compliance and leadership teams at a time when their effort and attention need to be laser-focused on ensuring clinical and operational continuance. All this makes the 72-hour incident reporting requirements unreasonable. Additionally, given that the impact of an event can evolve and change significantly from the time that an attack is first discovered, and the effects of the event can remain hidden for months or years, the Required Information for Supplemental Reports would make complying with this reporting even more burdensome and disruptive to operations.

Beyond the reporting burdens of the incident's details, the data retention requirements of the proposed rule are excessive. The proposed rule would "require covered entities preserve data and records relating to communications between the covered entity and the threat actor; indicators of compromise; relevant log entries, memory captures, and forensic images; network information or traffic related to the cyber incident; the attack vector; system information that may help identify vulnerabilities that were exploited to perpetrate the incident; information on any exfiltrated data; data and records related to any ransom payment made; and any forensic or other reports about the cyber incident produced or procured by the covered entity." This is a shockingly large amount of data, and this requirement is compounded by the fact that CISA is requiring these data be retained for two years after the incident — which can linger for months or years with no clear end date. Log files can be very data-dense; as such, the victimized hospital would now be burdened with unplanned and unbudgeted data management expenses to retain a huge amount of non-clinical, non-financial and non-operational data. This would require significant data storage capacity and necessitate hiring additional staff.

The AHA strongly recommends that CISA simplify and shorten the reporting requirements of covered cyber incidents during the incident; cap file and data retention requirements for a duration of no longer than one year; cap the size of the data files stored; and offer government funding or a no-cost storage option once that limit is exceeded.

The risks associated with this proposed rule cannot be understated. Complying with the reporting requirements of this rule would require a hospital or health system to turn over sensitive information regarding their systems and network architecture and overall information security posture. If this information fell into the hands of a cybercriminal or a nation-state-directed, supported or shielded adversary it could be catastrophic. Unfortunately, no one has a magic shield impenetrable to hackers, not even federal agencies. According to a White House report, in 2023 there were 11 major incidents reported across federal agencies, including HHS, classified as data breaches. These breaches met the Office of Management and Budget's December 2022 Federal Information Security and Privacy Management Requirements memorandum definition of

"incidents likely to result in harm to national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people." Further, in March 2024 it was reported that CISA had its systems breached by hackers. In effect, the proposed rule creates a potential treasure trove of information that hackers can use in case of another breach. **The AHA is concerned about the risk posed by such a broad intelligence collection on the critical infrastructure of hospitals and health systems. We all know that any organization — even CISA, as recent events show — can be a victim of hackers. We recommend that the reporting requirements of this proposed rule be modified to eliminate sensitive information regarding hospital and health systems technical architecture and cybersecurity defenses.**

Penalties

The proposed rule's penalties are vague and potentially severe. The AHA is concerned that this proposed rule recommends the victims of a crime be referred "to the Attorney General to bring a civil action to enforce the subpoena and/or pursue a potential contempt of court (6 U.S.C. 681d(c)(2)), and other enforcement mechanisms to include potential acquisition penalties, suspension, and debarment" of those victims for failure to comply with the reporting requirements of that crime. The AHA acknowledges that the spread and impact of cybercrime require the federal government to take strong actions to protect American citizens. However, punishing victims is counterintuitive and counterproductive. Additionally, the language of the proposed rule is too vague; CISA should include real-world scenarios so, for example, stakeholders have a better understanding of what is meant by "progressive penalization". **As such, the AHA recommends that CISA revise the proposed rule to incentivize collaboration rather than threaten further punishment on hospitals and health systems responding to a criminal attack.**

We appreciate your consideration of these issues. Please contact me if you have questions or feel free to have a member of your team contact Stephen Hughes, AHA's director for health information technology policy, at stephen.hughes@aha.org.

Sincerely,

/s/

Ashley Thompson
Senior Vice President, Public Policy