Charles N. Kahn III
President and CEO

July 3, 2024

Via electronic submission at *http://www.regulations.gov*

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, DC 20528

Re: Notice of Proposed Rulemaking, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS); Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements (Docket No. CISA–2022–0010; 89 *Federal Register*, April 4, 2024)

Dear Director Easterly:

The Federation of American Hospitals (FAH) is the national representative of more than 1,000 leading tax-paying public and privately held hospitals and health systems throughout the United States. FAH members provide patients and communities with access to high-quality, affordable care in both urban and rural areas across 46 states, plus Washington, DC, and Puerto Rico. Our members include teaching, acute, inpatient rehabilitation, behavioral health, and long-term care hospitals and provide a wide range of inpatient, ambulatory, post-acute, emergency, children's and cancer services.

We appreciate the opportunity to provide the Cybersecurity and Infrastructure Security Agency (CISA) with our views in response to the *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule*, 89 *Fed. Reg.* 23,644 (April 4, 2024) (Proposed Rule). The FAH strongly supports the goals of CIRCIA, as proposed by CISA, to provide a comprehensive and coordinated approach to understanding and reducing cyber incidents across critical infrastructure sectors to strengthen national cybersecurity.

In achieving CIRCIA goals, it is critical that there be consistency and integrity in reporting so that CISA receives data for only the types of incidents that need to be reported, along with a common understanding by covered entities of the types of incidents they are required to report. In addition, given the sensitivity of the data to be reported, it is imperative that covered entities are

provided sufficient assurance that the data they report will be used and protected appropriately, and shared only as minimally necessary to achieve the purpose of the reporting. Finally, we urge CISA to ensure harmonization of cyber incident reporting obligations. This is important so that government agencies and covered entities can properly focus their resources and quickly address and mitigate the cyber incident.

The FAH's comments below are based on our members' experience serving patients and maintaining critical healthcare infrastructure. Hospitals and health systems have considerable experience in navigating the cybersecurity of such information systems, requiring both expedient and thoughtful assessment and response to cyber threats, as well as strategic allocation of limited resources. Thus, discretion, consistency with existing regulatory frameworks, and minimizing the risk of unintended negative consequences are key elements to be considered within the Proposed Rule.

In considering our comments, the FAH has weighed the desire of our members to contribute to the resiliency of the healthcare industry with the flexibility needed to focus resources on patient care. The FAH urges CISA to further collaborate with critical infrastructure participants and other federal agencies regarding the continued rulemaking process.

Definitions

The Definition of "Covered Entity" and "Substantial Cyber Incident" Is Too Broad and May Undermine CISA's Ability to Analyze and Respond to Material Incidents

Covered Entity

Under CIRCIA, any "covered entity" must report a "covered cyber incident" to CISA within 72 hours after the entity reasonably believes that the covered cyber incident occurred. In the Proposed Rule, CISA states that a broad interpretation of "covered entity" is essential to ensure that CISA receives a sufficient number of reports to achieve its regulatory goals.[1] The FAH believes that such a broad interpretation of "covered entity" would be to the detriment of CISA's regulatory goals as this likely would lead to CISA receiving thousands of reports regarding minor incidents which detract from CISA's ability to quickly review and analyze the data and act when necessary, while at the same time undermining a covered entity's response and recovery efforts.

For example, if a physician practice within a hospital system experiences a cyber incident, this raises a question under the proposed rule of whether the incident is reportable. Under the proposed rule, for the sector-specific criteria, the entire entity (e.g., corporation), not the individual facility or function, is the covered entity. And if that entity experiences a substantial cyber incident, the entity would be required to report that incident to CISA regardless of whether the underlying incident impacted any of the critical infrastructure sector (CIS) facilities. If in this instance the cyber incident does not affect the rest of the hospital system, e.g., does not divert or disrupt patient care and CIS operations, and is contained within that physician practice, reporting the incident to CISA would simply create noise for CISA and would take away from the entity's response efforts. We also note that this incident, even if substantial for the physician practice, may

[1] 89 *Fed. Reg.* 23,677 (Apr. 4, 2024).

not be "substantial" for the overall entity. Thus, whether it would be reportable remains unclear under the Proposed Rule.

Covered Cybersecurity Incident

Cybersecurity disclosures are of a conceptually different nature than many other types of reporting obligations. Incidents may vary in nature, scope, and magnitude of individuals impacted, particularly if an incident is ongoing. Based on CISA's focus on preserving critical infrastructure, it would be prudent to establish a narrower definition of "substantial cyber incident" limited to those incidents that materially affect the ongoing viability and operations of an entity, including a loss of control and loss of capability or an infiltration of an entity's systems. For hospital systems, certain factors suggesting a "substantial" incident could include those requiring diversion of patients, operational downtime (e.g., inaccessibility of building, security, or medical systems), or other effect on hospital systems preventing clinicians from effectively treating patients.

Yet, the Proposed Rule broadly defines a substantial cyber incident as one that leads to any of the four following impacts: (1) a substantial loss of confidentiality, integrity or availability of a covered entity's information system or network; (2) a serious impact on the safety and resiliency of a covered entity's operational systems and processes; (3) a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; (4) unauthorized access to a covered entity's information system or network, or any nonpublic information contained in it, that is facilitated through or caused by a: (i) compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (ii) supply chain compromise.[2]

The FAH appreciates CISA's focus on the operational impacts in defining a substantial cyber incident. Yet, defining this term so broadly would result in CISA receiving too many reports, affecting both its ability to manage quantity and sort through what information is material to other healthcare covered entities and those in other sectors, while detracting from the entity's response efforts. For example, as defined above, a "substantial cyber incident" would occur due to "unauthorized access to a covered entity's information system or network …". It is unclear what type of "unauthorized access" would trigger a "covered cybersecurity incident." An attempt to secure "unauthorized access" to an entity's information system or network may occur often, though such attempts may be thwarted by the entity and thus are not successful in disrupting operations or meeting any of the other criteria of a "covered cybersecurity incident." Requiring reports for all incidents related to "unauthorized access," including unauthorized access from within an entity, would inundate CISA and undermine its ability to focus on key information being reported for which immediate action is needed.

Reporting Requirements

Hospitals and healthcare systems need flexibility with regard to the timing and contents of a covered entity's report. To provide any meaningful report, a covered entity must know an incident has occurred and have initial opportunity to assess if it rises to the level of a "substantial cyber incident," which should include consideration of the factors described above.

[2] Id. at 23,661.

The Time Frame for Developing a "Reasonable Belief" Should Be Expanded

The FAH acknowledges the underlying statutory requirement that a covered entity submit an incident report "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred." However, we urge CISA to reconsider its position that a preliminary analysis before a "reasonable belief" can be obtained "should be relatively short in duration (i.e., hours, not days) … and generally would occur at the subject matter expert level and not the executive officer level."[3] This time frame is much too short. A "reasonable belief" can take days to obtain, even over the course of expedient assessment. It takes time for a hospital or healthcare system to determine whether a given incident at a specific facility rises to one of the four substantial impacts set forth above for the covered entity as a whole. In addition, a subject matter expert within one facility of an entire healthcare system typically would need to collaborate with others across the entity, including at the executive officer level, to conduct this preliminary analysis to obtain a reasonable belief. Without greater flexibility in "obtaining a reasonable belief," CISA risks receiving information that amounts simply to noise or that otherwise could be material, yet not properly analyzed at the entity level so that CISA and the covered entity can respond appropriately.

Specifically, the FAH is concerned that preliminary reporting may lead to: (i) submission of reports for circumstances that are not ultimately covered cyber incidents; and (ii) submission of reports that are inconsistent with, or harmful to an entity's coordinated investigation and response with respect to its legal, regulatory, and insurance obligations. Although the FAH supports the overall intent of this proposal, including the benefits of enhanced knowledge to the resiliency of the healthcare industry, it is critical to allow more time to form a "reasonable belief" that an incident has occurred.

Flexibility and Harmonization is Needed in Submitting Reports to CISA and Other Federal Agencies

Covered entities need flexibility in submitting cyber reports, whether a supplemental report or a "substantially similar" report to another federal agency. For supplemental reports, covered entities need time and the ability to analyze the data and develop a response, while also coordinating with law enforcement, as premature disclosure has the potential to harm investigation of an active perpetrator.

Flexibility also is needed for submitting "substantially similar reports to another federal agency." Cyber incidents, including breach notification requirements, are already the focus of both extensive federal regulatory schemes and state law. For example, in addition to other federal laws, the *Health Insurance Portability and Accountability Act* (HIPAA) has its own incident reporting requirements and definitions, including materiality thresholds for disclosures to government authorities, individuals, and media agencies. In addition, other federal agencies, as well as state law enforcement, have certain authority to investigate cybersecurity incidents and pursue the bad actors involved. As such, HIPAA and certain other state and federal laws allow a covered entity to delay reporting an incident if the entity is working with law enforcement to investigate the cyber incident. Requiring entities to report a cyber incident while an active law enforcement investigation is underway would conflict with the intent of HIPAA's reporting delay

[3] Id. at 23,725.

and may adversely affect law enforcement's investigation of a cyber incident and apprehension of the responsible bad actors. The FAH understands CISA's "substantially similar reporting" exemption, as proposed, may exclude HIPAA reporting based on its general reporting timeline. However, CIRCIA reporting should be harmonized as much as possible with other laws and should allow entities to delay reporting a cyber incident in line with any delayed reporting exemptions of HIPAA and other applicable state and federal law, or where requested by the Attorney General, in order to balance the need for timely disclosure with the pursuit and prosecution of malicious actors.

The FAH is concerned that the Proposed Rule's high bar for the harmonization of cyber incident reporting may not achieve sufficient harmonization, which would result in over-reporting to multiple federal and state agencies. To help mitigate this result, we urge CISA to establish a CIRCIA Agreement between CISA and other federal and state agencies that reduces the burden on a covered entity – entity reporting should be streamlined so that it reports an incident to CISA – and all other federal and state entities interested in that incident would receive a notification. We urge this more flexible approach that would streamline reporting for covered entities so that they would not be required to report the same incident multiple times.

Further, at a minimum, if an incident is required to be reported as a data "breach" under another federal law, such as HIPAA, HITECH, or the FTC Act, entities should not have to again report the incident to CISA. This is consistent with CISA's reason for excluding health information technology entities from the sector-specific reporting requirements, noting that data breaches are not the primary focus of CIRCIA, and those entities already are required to report data breaches under HIPAA and HITECH.

Finally, covered entities need flexibility to determine when an incident has been "fully mitigated and resolved." The FAH agrees with CISA's statement that the damage caused by an incident does not have to have been fully addressed and remediated in order for the incident to be considered fully mitigated and resolved for the purpose of completing the supplemental report cycle.

Contents of Reports Should be Confidential Except as Appropriate to Contain a Cyberattack

It is likewise important that the reported contents end up in the right hands at the right time. Reports received by CISA should be leveraged for the collective benefit of similarly situated entities. For example, if a hospital system makes an early-stage disclosure of an active vulnerability as described above, it is important that such information be relayed to similarly situated hospital systems that may be most at risk of the same attack.

Nevertheless, it is equally important that the confidentiality of such information should be appropriately maintained. While there should not be attribution to the entity experiencing the cyberattack, in many cases it may be critical that certain Indicators of Compromise are shared with similarly situated entities so that they can quickly defend themselves and update their internal defenses to stop any spread of an attack against the sector.

However, much of this information should not be shared with the general public, as knowledge of an ongoing vulnerability may make an entity more at-risk of additional attacks. And to the extent that CISA receives company-specific proprietary information, it should not be shared

with other federal agencies and entity reports submitted to CISA should not be used by other federal agencies to penalize the entity.

Data and Records Preservation Requirements

CISA proposes requiring covered entities to 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.

Although CISA states that only data the covered entity believes in good faith are relevant to the incident must be preserved, the FAH is concerned about the cost to retain certain of the forensic information specifically listed by CISA (e.g., memory captures). The requirement to maintain this forensic data may significantly increase hospital and health system costs by increasing required capacity or otherwise taking certain systems offline, thereby diverting resources away from patient care. Accordingly, we urge CISA to allow flexibility in data preservation such that a covered entity would be required to preserve data that the entity believes in good faith are relevant to the incident – and refrain from specifically listing examples of such data. These overly prescriptive examples have varying meanings, and thus entities may end up over-reporting too much data, again burdening CISA with certain immaterial information and undermining its ability to focus on material data.

Enforcement

CISA proposes multiple enforcement tools, including issuing a Request for Information (RFI) if CISA believes a covered entity experienced a covered cyber incident or made a ransom payment but failed to report it. In addition, CISA will issue a subpoena if it does not receive an adequate response to the RFI within 72 hours. We urge CISA to provide a more reasonable timeframe to respond to an RFI as this 72-hour timeframe may be too aggressive, depending on the information requested in the RFI. Entities typically have 10 days to respond to a subpoena and a similar timeframe should apply to the RFI. Alternatively, at a minimum, CISA should allow the covered entity to request additional time, if needed.

****

The FAH appreciates CISA's dedication toward protecting critical infrastructure as well as consideration of our comments. We look forward to continued collaboration with CISA to implement effective policies that assist the healthcare industry in meeting the challenges of the evolving cyber landscape. If you have any questions, please contact me or any member of my staff at 202-624-1500.

Sincerely,