Charles N. Kahn III
President and CEO

November 14, 2022

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

Ms. Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, DC 20528

Re: CISA-2022-0010: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022; 87 Fed. Reg. 55,833 (September 21, 2022)

Dear Director Easterly:

The Federation of American Hospitals (FAH) is the national representative of more than 1,000 leading tax-paying community 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 *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022* (CIRCIA), 87 Fed. Reg. 55,833 (September 21, 2022) (RFI). Hospitals and health systems have significant experience in navigating the cybersecurity of information systems, requiring both expedient and thoughtful assessment and response to cyber threats, as well as strategic allocation of limited resources. Hospitals well understand the ongoing and significant challenges presented by cybersecurity threats and incidences and strongly support and appreciate CISA's efforts to improve cyber resilience and share information and tools with the healthcare industry to help mitigate and prevent cyber threats to the healthcare infrastructure. As CISA continues in these efforts and engages in rulemaking to implement CIRCIA, we urge that the regulations maximize flexibility, consistency, and

harmonization across existing regulatory frameworks, while minimizing the administrative burden and risk of unintended negative consequences, as discussed further below.

Definitions

The FAH urges that CISA regulations -- requiring covered entities to submit reports detailing covered cyber incident and ransom payments, as directed by CIRCIA -- ensure that definitions of key terms are clear, consistent across other federal and state laws, and allow flexibility for hospitals to report covered incidents in a timely manner that does not undermine a hospitals' ability to quickly remedy the cyber incident, while restoring critical systems that impact patient care and maintaining the confidentiality to sensitive patient health information.

Covered Entity

While the definition of a "covered entity" that is subject to cyber reporting requirements should include those entities that provide critical infrastructure, it should not be defined too broadly. Specifically, the definition of "covered entity" should not be so broad as to obligate critical infrastructure entities to report cyber incidents of downstream vendors and other entities outside of their control. For example, hospital systems utilize multiple third-party vendors, such as electronic medical record and other similar service providers, relevant to their daily operations. Hospitals do not have access and real-time visibility into the security status of these third-party vendors' internal systems, which are operated independently by these vendors. Therefore, hospitals cannot necessarily discern when an incident may have occurred or is still in process regarding information systems used, but not owned, by the hospital. Any ability to make a determination regarding a cyber incident on information systems owned by a third-party will depend on the discretion of that vendor. While hospital systems may have agreements with third-party system owners requiring upstream reporting of cyber incidents, these third parties may have varying views of what constitutes a cyber incident. In addition, a hospital system may find it particularly difficult to obtain information from a privately held information systems provider, whose resources may be stretched thin as it responds to an incident, potentially resulting in misinformation to the hospital system. Thus, CISA reporting requirements should apply separately to these vendors and should not be reported through the hospital system.

Covered and Substantial Cyber Incident

Under CIRCIA, a "covered cyber incident" turns on whether an incident is "substantial." The term "substantial" presents significant ambiguity. There are many factors to consider before determining whether an incident is "substantial," yet the definition of this term should not turn solely on one factor, and hospitals need flexibility in assessing whether these factors rise to the threshold of "substantial."

Cybersecurity disclosures are of a conceptually different nature than many other types of reporting obligations. Incidents may vary greatly in nature, scope, and magnitude of individuals impacted, particularly if an incident is ongoing. Thus, the definition of a "substantial cyber incident" in the context of hospital systems, should take into account whether an incident significantly affects the ongoing viability of a hospital's operations to the extent that the incident triggers the diversion of patients, significant operational downtime (e.g., inaccessibility of building, fire systems, security, or electronic medical systems), or other effect on hospital systems

preventing clinicians from effectively treating patients. On the other hand, the definition of "substantial cyber incident" must be balanced and flexible to ensure that it is not overly broad and does not require the reporting of incidents that do not significantly impact business operations or patient safety. For example, if a cyber incident were to temporarily compromise the operation of a hospitals' imaging machine, but the hospital is able to quickly detect and remedy the cyber interruption with little impact on hospital operations and no threat to patient safety, this type of incident (and other similar incidents) should not be considered "substantial." If so, this would result in CISA receiving too may reports with unusable information, which would undermine its ability to properly analyze and respond to truly substantial and significant cyber incidents, while hindering the goal of information sharing to prevent other similar attacks. It also would undermine a hospitals' ability to monitor and quickly remedy ongoing cyber threats.

Ransom Payments

Based on the layered involvement of parties that may coordinate with a covered entity in investigating or remediating an incident, "ransom payments" should consider the moment an individual entity has made a transaction with a criminal or state-sponsored actor, whether such transaction includes payment by the covered entity or a third party.

Incident Report Contents and Timing

With regard to the timing and contents of a covered entity's reporting of a covered cyber incident, the FAH urges that any related requirements allow flexibility for hospitals. In order to provide any meaningful report, a covered entity must have a "reasonable belief" that an incident has occurred as well as ample opportunity to assess if the incident rises to the level of a "substantial cyber incident," which should include consideration of the factors described above.

Reasonable Belief

In determining what constitutes a "reasonable belief" that a covered cyber incident has occurred, which would trigger the 72-hour reporting deadline, again flexibility and reliance on multiple factors to make this determination is critical. For example, a covered entity may know that a cyber incident has occurred but does not yet know if it is "substantial." Both of these factors -- the entity's knowledge of the occurrence of a cyber incident and its assessment that the incident is significant and "substantial" -- must be present before forming a "reasonable belief" and the entity will need time to properly make this assessment. Other considerations affecting whether a "reasonable belief" exists could include whether an entity has engaged an internal or third-party incident response team and that team has confirmed the incident.

Incident Report Timing

Covered entities need the latitude to coordinate with law enforcement in determining the timing of a covered incident report, as premature disclosure has the potential to harm investigation of an active perpetrator. Cyber incidents, including breach of protected health information (PHI) notification requirements, are already the focus of both extensive federal regulatory schemes and state law. For example, the *Health Insurance Portability and Accountability Act of 1996* (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 and may adversely affect law enforcement's investigation of a cyber incident and apprehension of the responsible bad actors. Therefore, we urge that any rulemaking by CISA allow entities to delay reporting a cyber incident, when working with and requested by law enforcement, similar to what is permitted under HIPAA and other applicable state and federal laws, or when requested by the Attorney General. This is necessary to balance the need for timely disclosure with the pursuit and prosecution of malicious actors.

Supplemental Information

The submission of supplemental reports must consider several factors. As discussed above, entities working in partnership with law enforcement may be constricted in what they report per the request of law enforcement, and thus they need the flexibility to report consistent with such requests in terms of timing and content. Yet, FAH members understand and support the need for information sharing so that CISA and other covered entities can work to better assess, mitigate, or prevent future cyberattacks. While these goals of information sharing and delayed reporting due to law enforcement activity may present a paradox, an appropriate balance of these goals may be achieved through a multi-phased reporting structure. This could focus on (1) early reporting of initial information identifying the particular vulnerability (with sensitive or under-developed information redacted) that can be shared with similarly situated critical infrastructure entities to help prevent attacks; and (2) supplemental information reported later on after the covered entity and law enforcement are able to engage in additional fact-finding and establish a more comprehensive assessment of the incident, and this information could potentially identify a course of action necessary to address the attack. This would provide the necessary and immediate opportunity to protect other critical infrastructure entities, while later allowing assessment of trends and opportunities to enhance investigation of perpetrators.

We also note that it is 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. However, it is equally important that such information not be shared with the general public, as knowledge of an ongoing vulnerability may make an entity more at-risk of additional attacks.

Other Incident Reporting Requirements

Harmonization with Other Federal and State Laws

The FAH urges CISA to coordinate with other federal agencies, such as the Department of Health and Human Services (HHS), to harmonize cyber reporting requirements to avoid duplicate incident reporting as much as possible. Hospitals already are required to comply with extensive health data breach reporting requirements under HIPAA (as well as to the Federal Trade Commission (FTC)). Consistent with the CIRCIA directive that CISA not require reporting to a

covered entity where a covered entity is required by law, regulation, or contract to report substantially similar information to another federal agency within a substantially similar timeframe, we urge CISA to harmonize its requirements as much as possible with HHS and the FTC, while also ensuring that CISA is able to timely receive the cyber reports discussed above to engage in the necessary information sharing that can help other covered entities mitigate and prevent cyberattacks. We also urge CISA to leverage existing state cybersecurity breach reporting laws and state data breach reporting laws to minimize the reporting burden for covered entities.

Reporting Costs

As CISA develops reporting requirements, we urge that it seek to minimize the reporting burden, especially through harmonizing requirements with federal and state laws, as discussed above. This will assist in mitigating the costs of meeting reporting requirements that will be in addition to the existing substantial costs that entities already incur to daily assess and remedy potential risks, threats, and incidences of cyberattacks. This effort should include (1) ensuring that the information collected is core to the key end goals of CIRCIA and does not include extraneous details not needed to promote the CIRCIA's end goals; and (2) optional disclosure of certain information if CISA purely plans to use it to track trends.

****

The FAH appreciates CISA's leadership and dedication toward protecting critical infrastructure and consideration of our comments in that regard. We look forward to continued collaboration with CISA to implement effective policies that assist hospital systems 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,