UnityPoint Health

Government & External Affairs
1776 West Lakes Parkway, Suite 400
West Des Moines, IA 50266
unitypoint.org

July 3, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, VA 20598-0630

Re: CISA-2022-0010; Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements published at Vol. 89, No. 66 Federal Register 23644-23776 on April 4, 2024.

Dear Director Easterly,

UnityPoint Health appreciates this opportunity to provide comments on the Cybersecurity and Infrastructure Security Agency's (CISA) proposed rule on cyber incident reporting, which implements requirements under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA).

UnityPoint Health is one of the nation's most integrated healthcare systems. Through more than 29,000 employees and our relationships with more than 375+ physician clinics, 36 hospitals in urban and rural communities and 13 home health agencies throughout our 8 regions, UnityPoint Health provides care throughout Iowa, central Illinois, and southern Wisconsin. On an annual basis, UnityPoint Health hospitals, clinics and home health provide a full range of coordinated care to patients and families through more than 8 million patient visits.

UnityPoint Health appreciates the time and effort of Cybersecurity and Infrastructure Security Agency (CISA) in developing this proposed rule. **UnityPoint Health is a member of the American Hospital Association and the Iowa Hospital Association and generally supports their formal comment letters. In addition, UnityPoint Health respectfully offer the following additional comments**.

COMMENTS

Cybersecurity impacts the healthcare industry uniquely. Health care organizations house an enormous amount of personal information, and we have an immediate need to access data to provide patient care and pursue an overall critical purpose to save/improve lives, making us top targets of cyberattacks.

UnityPoint Health urges CISA to simplify 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. Just as an emergency call to 911 reaches fire, ambulance, or police, CISA should set up an emergency call center that activates

incident response teams, forensics teams, system recovery teams, ransomware negotiation teams, and law enforcement resources such as the FBI. In essence, **CISA should be a one-stop shop for cyber incident reporting**. For industries like the healthcare sector with many state and federal regulatory and accreditation reporting requirements, using the call to CISA to activate immediate assistance and serve as our reporting requirement would lessen the burden to the victims of these attacks.

A 'Substantial Cyber Incident' is not a good term to use because it is subjective and does not have a well-defined or easily interpreted meaning. What is 'substantial' to one entity may not be 'substantial' to another. Impact is based on multiple facets such as financial, production or operations, services, reputation, safety, operations, personnel, or any other key area within the reporting organization. **CISA should tightly limit the definition of "covered cyber incident" to significant and substantial incidents that impact critical systems or services**. Critical infrastructure entities are the targets of malicious cyber actors millions of times a day. An overly broad definition of covered cyber incidents would present enormous compliance challenges for covered entities in addition to creating a deluge of reports that would make it difficult, if not impossible, for CISA to determine trends through the noise. An overly broad definition could result in covered entities diverting limited resources from strengthening information systems to regulatory reporting functions. It is a delicate balance. The criteria for what to report and when to report it should always be focused on our national security posture or capabilities and ensuring critical infrastructure entities are helped by the regulation and not further burdened or penalized.

UnityPoint Health requests that CISA consider enabling automated report mechanisms and treating covered entities participating in the Cyber Threat Indicators and Defensive Measures Automated Indicator Sharing initiative for Cybersecurity Purposes as meeting all reporting requirements for CIRCIA. CISA must ensure that processes are beneficial to national security while being workable for industry so that incident response activities are not slowed by non-essential compliance activities and reports remain anonymous. CISA should also be mindful that victims will be reporting to the FBI and consider how to harmonize that reporting channel with CIRCIA requirements.

While several federal agencies have an interest in cybersecurity and CISA must collaborate with them, **CISA must also consider existing data breach reporting requirements at the state level.** UnityPoint Health has a multistate footprint and reporting requirements vary by state. It will be critical for CISA to work with existing infrastructures wherever possible to allow single-point reporting with the government being responsible for sharing information internally in a need-to-know environment. A one-stop shop for reporting is preferrable, rather than imposing multiple reporting obligations on an impacted covered entity, which is simultaneously dealing with a live cybersecurity event.

CISA should clarify that filing an incident report under this rule does not automatically trigger any other reporting action or obligation. Covered entities should be able to determine whether to file reports with other oversight bodies or agencies based on those reporting requirements, not just because the incident qualified for a report under this statute. To minimize burden, the CISA incident reporting form should permit covered entities to indicate if CISA should make other agency notifications on their behalf.

UnityPoint Health is concerned with unintended consequences and reputational harm resulting from incident reporting. **CISA should take appropriate steps to secure the incident reporting system and**

associated data, including minimization, anonymization, and aggregation when appropriate. In addition, CISA should carry any financial and reputational costs through full recovery for covered entities if the cyber incident report is leaked. Costs for leaked information should include losses resulting from a bankruptcy filing/claim due to a lack of hardening of the cyber incident data stored by CISA. There is always some level of cost when it comes to compliance and reporting activities that can range from direct costs (e.g., legal) to indirect (e.g., staff time). Consideration of how much time pre, during, and post an incident might be taken for smaller entities that will have less staff to assist on their incident response should be considered.

While considering costs, **UnityPoint Health urges CISA to contemplate how to minimize costs, including funding for security controls**. In tandem with these resources, we urge CISA to continue efforts to stop, catch, and prosecute cyber criminals and prevent future attacks on a national scale. Individual covered entities have limited resources to combat the increasing threat from cyber-attacks and we should be able to rely upon CISA and the federal government to lead these efforts.

We are pleased to provide input and appreciate your consideration of our comments and endorsements for comment letters provided by the American Hospital Association and the Iowa Hospital Association. To discuss our comments or for additional information on any of the addressed topics, please contact Cathy Simmons, Government & External Affairs at Cathy.Simmons@unitypoint.org or 319-361-2336.

Sincerely,

Charity Sharpe
Chief Information Security Officer

Cathy Simmons, JD, MPP
Executive Director, Government & External Affairs