

November 14, 2022

Director Jennie M. Easterly
Cybersecurity and Infrastructure Security Agency, Stop 0380
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

RE: CISA–2022–0010 - Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022; published at Vol. 87, No. 175 Federal Register 55833-55836 on September 12, 2022.

Submitted electronically via <http://www.regulations.gov>

Dear Director Easterly,

UnityPoint Health appreciates this opportunity to provide comments on this request for information related to the Cyber Incident Reporting for Critical Infrastructure Act of 2022. UnityPoint Health is one of the nation's most integrated health care systems. Through more than 32,000 employees and our relationships with more than 480 physician clinics, 40 hospitals in urban and rural communities and 14 home health agencies throughout our 9 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 8.4 million patient visits.

UnityPoint Health appreciates the interest of Cybersecurity and Infrastructure Security Agency (CISA) in seeking stakeholder input on this legislation. UnityPoint Health respectfully offers the following comments to the CMS inquiries below:

GENERAL COMMENTS

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA) directs CISA to develop and oversee implementation of regulations requiring covered entities to submit to CISA reports detailing covered cyber incidents and ransom payments. CISA is interested in receiving public input on potential aspects of the proposed regulation and welcomes input on all aspects of CIRCA's regulatory requirements.

Comment: Cybersecurity impacts the health care industry uniquely. Health care organizations house an enormous amount of personal information, and we have an immediate need for to access data to provide patient care and pursue an overall critical purpose to save/improve lives, and thus health care

organizations are a top target for cyber criminals. As a result, health care breach costs are the most expensive of all industries for 12 years running, setting a record of \$10.1 million average in 2022.¹ As an industry leader, UnityPoint Health's information protection goal is to align our information security strategy by implementing appropriate security measures to mitigate risks and reduce the impact of negative events. The commitment to our information protection program is evidenced through both strong financial investments, which exceed ten percent of our information technology operational budget, as well as governance oversight by a subcommittee of our management board.

In terms of purpose and overall expectations for cybersecurity reporting, **UnityPoint Health encourages CISA to set clear expectations on what is to be reported, why reports are being collected (trend identification, proactive indication and warning, response assistance, national security), what happens after reporting an incident, how information will be distributed and handled, and what other Federal entities could receive the reported data under what conditions.**

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 health care 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.

DEFINITIONS, CRITERIA, AND SCOPE OF REGULATORY COVERAGE

CISA seeks input on several specific questions related to the topic of regulatory coverage, although these questions are not intended to be exhaustive.

Covered Entity:

- a. The meaning of "covered entity," consistent with the definition provided in section 2240(5) of the Homeland Security Act of 2002 (as amended), taking into consideration the factors listed in section 2242(c)(1).*
- b. The number of entities, either overall or in a specific industry or sector, likely to be "covered entities" under the definition provided in section 2240(5) of the Homeland Security Act of 2002 (as amended), taking into consideration the factors listed in section 2242(c)(1).*

Comment: As the definition of "covered entity" is considered, **UnityPoint Health urges CISA to leverage the pre-existing list of entities within the 16 critical infrastructures identified under Section 9 of Executive Order 13636 "Improving Critical Infrastructure Cybersecurity."**

Covered Cyber Incidents:

- c. The meaning of "covered cyber incident," consistent with the definition provided in section 2240(4), taking into account the requirements, considerations, and exclusions in section 2242(c)(2)(A), (B), and (C), respectively. Additionally, the extent to which the definition of "covered cyber incident" under CIRCIA is similar to or different from the definition used to describe cyber incidents that must be reported under other existing federal regulatory programs.*

¹ IBM Security's 2022 Cost of a Data Breach Report

e. The meaning of “substantial cyber incident.”

Comment: The statute restricts the rule to entities and incidents with national-level impact and not every cybersecurity incident within the country. **UnityPoint Health urges CISA to define “covered cyber incidents” in a way that captures actual incidents of national-level impact without imposing unnecessary additional burdens on entities reporting and responding to incidents in real-time.** Focus needs to remain on cyber incidents with the potential to cause significant negative impacts to national security, economic security, or public health and safety. 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 or industry sector is not ‘substantial’ to another.

A consistent or better methodology that has a clear meaning for the covered entity and is commonly used in incident response analyses is to incorporate the term ‘Impact’. ‘Impact’ is relevant to each specific covered entity based on multiple facets such as financial, production or operations, services, reputation, safety, operations, personnel, or any other key area within the reporting organization. **UnityPoint Health recommends the reporting of cyber incidents based on the category of Impact.** For example, mandatory reporting to CISA within 72 hours of determination of cyber incident can be required for those incidents with Severe or Significant Impact, while voluntary reporting of cyber incidents of lesser Impacts can be encouraged for information sharing purposes (Sample Impact Chart):

Impact Scale	Magnitude of Impact
5 Severe	<ul style="list-style-type: none"> • Safety concerns due to disruption of information systems. • Loss of major tangible assets or resources or business operations. • Loss of or disruption to mission critical information systems. • Potential reputational harm to organization or customers.
4 Significant	<ul style="list-style-type: none"> • Loss of major tangible assets or resources or business operations. • Loss of or disruption to mission critical information systems. • Potential reputational harm to organization or customers.
3 Moderate	<ul style="list-style-type: none"> • Loss or disruption to some tangible assets or resources or business operations. • Loss of or disruption to non-critical information systems.
2 Slight	<ul style="list-style-type: none"> • Minimal loss or disruption to some tangible assets or resources. • Momentary disruption to operations or non-critical information systems.
1 Minimal	<ul style="list-style-type: none"> • No loss of Tangible assets or resources. • No disruption of operations or information systems.

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.

REPORT CONTENTS AND SUBMISSION PROCEDURES

CISA seeks input on several specific questions related to the topic of reporting requirements, although these questions are not intended to be exhaustive.

Reporting Methods:

a. How covered entities should submit reports on covered cyber incidents, the specific information that should be required to be included in the reports (taking into consideration the requirements in section 2242(c)(4)), any specific format or manner in which information should be submitted (taking into consideration the requirements in section 2242(c)(8)(A)), any specific information that should be included in reports to facilitate appropriate sharing of reports among federal partners, and any other aspects of the process, manner, form, content, or other items related to covered cyber incident reporting that would be beneficial for CISA to clarify in the regulations.

Comment: UnityPoint Health requests that CISA develop a standardized reporting form that contains a limited, core set of fields that every reporting entity must answer. Beyond the core questions, the reporting form should have different fields depending on the incident being reported or the type of covered entity reporting the incident.

Ultimately, the rule should be flexible on reporting methods, such as machine-to-machine reporting and other methods, to ensure minimal or no additional burden on the entities. Options for reporting outside of portals, such as via a phone call, should be considered in case a cyber incident has made systems untrustworthy or unavailable. Additionally, **CISA should 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.**

Timing of Reporting:

b. What constitutes “reasonable belief” that a covered cyber incident has occurred, which would initiate the time for the 72-hour deadline for reporting covered cyber incidents under section 2242(a)(1).

c. How covered entities should submit reports on ransom payments, the specific information that should be required to be included in the reports (taking into consideration the requirements in section 2242(c)(5)), any specific format or manner in which information should be submitted (taking into consideration the requirements in section 2242(c)(8)(A)), and any other aspects of the process, manner, form, content, or other items related to ransom payments that would be beneficial for CISA to clarify in the regulations.

e. When should the time for the 24-hour deadline for reporting ransom payments begin (i.e., when a ransom payment is considered to have been “made”).

Comment: 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. To ensure compliance concerns do not slow down response and recovery activities, it is crucial that the submission process and timing are straightforward. UnityPoint Health recommends

that the rule require reporting no sooner than 72 hours following covered entity confirmation of a covered cyber incident with an impact that requires reporting.

As for reporting ransomware payments, while the statute calls for reporting no later than 24 hours, CISA should keep the contents of the ransomware report consistent with the statute to minimize burden in the wake of what is likely an ongoing recovery from the ransomware attack. CISA should also be mindful that victims will be reporting to the FBI and consider how to harmonize that reporting channel with CIRCIA requirements.

The 24-hour time deadline for reporting ransom payments should be triggered once the covered entity or cyber insurance company identifies a payment will be authorized. The ransom payment decision itself must be completed within the cyber criminal's timeline, which may only provide 24 hours, 36 hours, or 48 hours to make the ransom payment before the impacted organization's data would be made unrecoverable or erased. **As a victim, reporting requirements for a ransom payment should not further victimize the covered entity through imposing federal penalties, freezing of assets, or delaying/preventing the recovery of services or data.**

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 preferable, rather than imposing multiple reporting obligations on an impacted covered entity, which is simultaneously dealing with a live cybersecurity event.

Situation Awareness:

h. What CISA should consider when "balanc[ing] the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations" when establishing deadlines and criteria for supplemental reports.

Comment: CISA should ensure situational awareness between industry and federal stakeholders without hindering active cyber incident response. **A daily National Incident Report provided after CISA's analysis of cyber incident reports should be provided to all industry sectors to protect national security and supply-chain.** This report should extend beyond a list of incidents and include CISA feedback and recommendations for proactive actions that can be taken to strengthen our nation's security.

Third Party Reporting and Data Collection for Security Vendors:

i. Guidelines or procedures regarding the use of third-party submitters, consistent with section 2242(d).

Comment: As stated in the statute, "a covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a)." It also states that "third-party reporting under this subparagraph does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission." **We**

encourage CISA to clarify that third-party reporting equals a covered entity's compliance with reporting. The regulation should further clarify that third parties have no obligation to report a cyber incident independent of the covered entity.

For efficiency and more comprehensive data, we believe CISA should utilize major key security software providers, internet service providers (ISPs), and cloud vendors that collect billions of cyber incidents and vulnerabilities each month and pre-analyze and consolidate like instances for a more proactive approach to national security. These vendors can provide key analyses and incident consolidation since they have access to multiple covered entities at once across all sectors. Analyses of data from key vendors would be more efficient (fewer and more organized) and such aggregation would facilitate more timely action than collecting information from thousands of covered entities.

OTHER INCIDENT REPORTING REQUIREMENTS AND SECURITY VULNERABILITY INFORMATION SHARING

CISA seeks input on several specific questions related to the topic of other incident reporting requirements, although these questions are not intended to be exhaustive.

Protection of Covered Entity for Incident Reporting:

- a. Other existing or proposed federal or state regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments, and any areas of actual, likely, or potential overlap, duplication, or conflict between those regulations, directives, or policies and CIRCIA's reporting requirements.*
- b. What federal departments, agencies, commissions, or other federal entities receive reports of cyber incidents or ransom payments from critical infrastructure owners and operators.*

Comment: To the extent allowable under statute, **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. We agree that disclosing the Industry Sector in which the cyber incident occurred is important, but disclosing the name of the covered entity should not be required. **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.

Cost of Incident Reporting and Funding for Security Controls:

- c. The amount it typically costs and time it takes, including personnel salary costs (with associated personnel titles if possible), to compile and report information about a cyber incident under existing reporting requirements or voluntary sharing, and the impact that the size or type of cyber incident may have on the estimated cost of reporting.*

d. The amount it costs per incident to use a third-party entity to submit a covered cyber incident report or ransom payment report on behalf of a covered entity.

e. The amount it typically costs to retain data related to cyber incidents.

Comment: We are pleased that CISA is requesting stakeholder input on cost and administrative burden, as this rule will impact covered entities of all sizes. 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. Ensuring the information reported and the covered entities required to report are aligned with the intent of addressing national security concerns will be beneficial and could make it less likely to negatively impact recovery efforts.

While considering costs, UnityPoint Health urges CISA to contemplate how to minimize costs, including funding for security controls. The majority of medium and small covered entities and even larger not-for-profit covered entities may not have the funding or revenue for all key security solutions necessary to implement a fully hardened domain name security (DNS). CISA could solve this DNS gap, since this is a key area for improving national security. In particular, CISA should examine providing direct resources. This could include a program to provide covered entities with robust security tools at free or more affordable pricing and to offer vouchers for maintaining up-to-date equipment. In tandem with direct resources, we urge CISA to continue effort to stop, catch, and prosecute cyber criminals and prevent future attacks on a national scale. Individual covered entities and industries 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.

ADDITIONAL POLICIES, PROCEDURES, AND REQUIREMENTS

CISA seeks input on several specific questions related to the topic of additional policies and/or requirements, although these questions are not intended to be exhaustive.

Policies and Procedures and Frameworks:

c. Any other policies, procedures, or requirements that it would benefit the regulated community for CISA to address in the proposed rule.

Comment: UnityPoint Health recommends that CISA place Guidelines, Policy, and Procedures in the NIST 800 and ISO20001 standards framework requirements to ensure covered entities have documented guidance that is clear and consistent. Additionally, CISA should develop standard policy language for reporting requirements related to the enforcement of CIRCIA for covered entities to adopt and incorporate into their own Policies and Procedures for consistency.

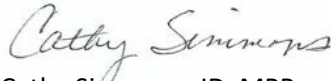
We are pleased to provide input on this request for information and its impact on our patients and communities. To discuss our comments or for additional information on any of the addressed topics,

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