June 28, 2024

The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security
2707 Martin Luther King Jr Ave SE
Washington, DC 20528-0525

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

Submitted electronically to: http://www.regulations.gov

RE: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule [Docket No. CISA-2022-0010]

Dear Secretary Mayorkas and Director Easterly:

Premier Inc. appreciates the opportunity to submit comments to the Cybersecurity and Infrastructure Security Agency (CISA) regarding its proposed rule to establish cyber incident reporting requirements for critical infrastructure organizations under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Healthcare is one of the critical infrastructure sectors most vulnerable to and most frequently victimized by cybercrime. As a number of recent high-profile incidents have proven, disruptions to healthcare pose significant privacy, security and safety risks to the US population. Premier is committed to developing a more robust cybersecurity profile across healthcare – from hospitals to payers to medical device manufacturers – in order to preserve patient safety and critical healthcare capabilities in the face of increasingly pernicious threats from a range of bad actors. In our comments, Premier specifically recommends that CISA consider the following:

- Clarifying both the definition of "significant" cybersecurity incidents and the scope of information requested by CISA reporting to be more narrow, targeted, impactful and in alignment with other federal cyber reporting programs;
- More precisely defining "covered entities" in order to reduce confusion and simplify compliance across the complexity of healthcare vendor relationships, supply chains and data exchange;
- Ensuring that liability protections for entities reporting cybersecurity events extend through the process of CISA sharing data with other federal agencies; and
- Extending reporting timelines so that affected entities can focus first on addressing the cybersecurity incident at hand, and then on voluntarily reporting details to CISA.

Premier's recommendations are described in greater detail below.

I. BACKGROUND ON PREMIER INC.

Premier Inc. is a leading healthcare improvement company and national supply chain leader, uniting an alliance of 4,350 hospitals and approximately 300,000 continuum of care providers to transform healthcare. With integrated data and analytics, collaboratives, supply chain solutions, consulting and other services, Premier enables better care and outcomes at a lower cost. Premier's sophisticated technology systems contain robust data gleaned from nearly half of U.S. hospital discharges, 812 million hospital outpatient and clinic encounters and 131 million physician office visits. Premier is a data-driven organization with a 360-

degree view of the supply chain, working with more than 1,400 manufacturers to source the highest quality and most cost-effective products and services. Premier's work is closely aligned with healthcare providers, who drive the product and service contracting decisions using a data driven approach to remove biases in product sourcing and contracting and assure access to the highest quality products. In addition, Premier operates the nation's largest population health collaborative, having worked with more than 200 accountable care organizations (ACOs).

A Malcolm Baldrige National Quality Award recipient, Premier plays a critical role in the rapidly evolving healthcare industry, collaborating with healthcare providers, manufacturers, distributors, government and other entities to co-develop long-term innovations that reinvent and improve the way care is delivered to patients nationwide. Headquartered in Charlotte, North Carolina, Premier is passionate about transforming American healthcare. Premier is focused on leveraging cutting-edge technology to move the needle on cost and quality in healthcare, including:

- Premier's Clinical Decision Support (CDS) designs AI-enabled technology to reduce low-value and unnecessary care. CDS leverages natural language processing AI technology to read unstructured data such as physician notes in electronic health records and ties together unstructured data with established practice guidelines to generate real-time alerts and relevant analytics, guiding physician's decisions toward higher-quality, lower-cost healthcare. CDS's mission is to measurably improve the quality and safety of patient care while reducing the cost of care by enabling context-specific information integrated into the provider workflow.

- Premier's Applied Sciences (PAS) is a trusted leader in accelerating healthcare improvement through AI-powered solutions that span the continuum of care and enable sustainable innovation and rigorous research. Our services and real-world data drive research and quality improvement in pharmaceutical, device and diagnostic industries, academia, federal and national healthcare agencies, as well as hospitals and health systems. PAS leverages Premier's robust data resources to design and deploy AI-powered solutions for clinical trial recruitment, and to help collate disparate patient records to tell a complete patient story, leading to higher-quality care.

- Conductiv, a Premier purchased services subsidiary, harnesses AI to help hospitals and health systems streamline contract negotiations, benchmark service providers and manage spend based on historical supply chain data. Conductiv also works to enable a healthy, competitive services market by creating new opportunities for smaller, diverse suppliers and helping hospitals invest locally across many different categories of their business.

- Premier's award-winning Supply Chain Disruption Manager (SCDM) builds resilience and mitigates risks to the healthcare supply chain by harnessing machine learning AI technology to predict when critical drugs, devices and other medical supplies are anticipated to become unavailable up to six weeks in advance of a supply chain disruption. SCDM allows hospitals and health systems to access clinically approved alternative products to avoid delays in care or quality, and it allows for communication to federal agencies and other partners about pending shortages to help proactively develop mitigation strategies.

II. DEFINING COVERED CYBERSECURITY INCIDENTS

Premier and our member hospitals, health systems and continuum of care providers are on the front lines of mitigating cybersecurity threats and advancing patient safety, allowing the healthcare and public health sector to continue to operate its critical life-saving functions. As such, Premier acknowledges the importance of collecting data and responding in a timely manner to a broad range of cybersecurity incidents, consistent with the intent of this proposed rule.

However, even among critical infrastructure sectors, the complexity of the healthcare ecosystem and the immense volume of data stored and exchanged across organizations create unique challenges to incident reporting. In this proposed rule, CISA argues that it does not intend to create undue burden or overwhelm the agency with insignificant reports. If the intent of this proposed rule is to limit covered incident reporting to only significant cyber incidents, further specification and criteria are necessary to define a covered cyber incident for healthcare.

As such, ***Premier recommends that incidents with an impact below a certain scale for healthcare specifically should be excluded from reporting requirements to reduce the burden on small providers and healthcare IT companies.*** In healthcare, cyber incidents are an ever-present threat. While the four qualitative metrics included in this proposed rule create a perfectly defensible definition of a cyber incident, the resulting definition is too academic to capture only significant healthcare incidents. Premier believes that, as constructed, these requirements may lead to an overrepresentation or overreporting of healthcare incidents.

CISA outlines loss of confidentiality, integrity, or availability; impact on operational systems; disruption of ability to engage in business and unauthorized network access as the qualifiers for a significant (thus covered) cyber incident. However, in healthcare, the volume of patient records, large number of vendors for various business and operational systems, and the potential for incidents that compromise operations in one location or department make these qualifiers over-inclusive.

Rather, Premier suggests that CISA adopt further criteria in the definition of healthcare covered cyber incidents specifically. Under HIPAA Breach Notification guidelines, health organizations must only report a breach when it affects over 500 patient records. This prevents day-to-day security challenges from becoming reportable incidents, reducing the burden on both health organizations and government regulators while still capturing information on significant events. ***Premier urges CISA to adopt a similar benchmark that includes a minimum number of patient records that must be impacted to better construct the definition of covered cyber incident for healthcare.***

Additionally, Premier urges CISA to specifically clarify whether cyber incidents resulting in the compromise of deidentified, anonymized or synthetic data counts as a "loss of confidentiality, integrity, or availability." Deidentified data is no longer considered protected health information under the HIPAA Privacy Rule as it is no longer individually identifiable. Thus, ***Premier urges CISA to clarify this point and include a stated exception for properly de-identified health data in both the definition of covered incidents and in the examples of covered cyber incidents.***

Consistent with CISA's own analysis, Premier believes that the "sophistication or novelty of the tactics" involved in a cyber incident should not impact thresholds for reporting. Such a requirement would place an undue burden on reporting organizations, particularly in healthcare, and introduce a subjective judgement where reporting organizations must guess if the novelty of an incident rises to reportable levels. This poses additional challenges at a time where organizations are devoting attention and resources to responding to a cyber incident. ***Premier urges CISA to keep its definition of covered cyber incident independent of additional reporting requirements based on sophistication or tactics; or at the very least, to provide clear and unambiguous guidelines about what "novel tactics" would rise to the level of reportability.***

III. DEFINING COVERED ENTITIES

Similar to the definition of covered cyber incidents, the current definition of covered entities, specifically for the healthcare sector of critical infrastructure, is overly broad and should be narrowed to prevent unnecessary reporting burden and uncertainty around which healthcare entities are covered. The healthcare sector is large and complex, including but not limited to an extensive network of payers, providers, pharmaceutical companies, research centers, labs, medical device manufacturers, medical

suppliers and IT and data vendors. The current definition, as well as the documentation it refers to, does not provide a clearly defined boundary between covered and non-covered entities.

Premier urges CISA to more clearly define "the healthcare critical infrastructure sector" and the scope of the covered entity definition within each healthcare subvertical. Premier acknowledges the intent behind a broad, criteria-based definition of critical infrastructure. For many sectors, it will be straightforward for entities to determine whether or not they fall in a critical infrastructure sector. However, for healthcare, the proposed definition is not sufficient.

First, the Sector-Specific Plans, which this proposed rule refers to as a guide to the scope of critical infrastructure sectors, have for the most part gone without update since 2015, despite the expected four-year updates alluded to in this document. For the healthcare sector, the document does not capture recent changes to the data landscape, AI applications to medical practice or the evolving interoperability between large entities and small healthcare information technology (HCIT) vendors. ***The scale of the healthcare sector and its highly complex data and HCIT relationships necessitate a narrower, or at least more clearly demarcated, criteria for what types of entities are included in the healthcare critical infrastructure sector.***

While this purpose can be partially accomplished by narrowing the definition of covered entity in the healthcare sector, there remains a broader challenge. The evolution and interconnectedness of the healthcare sector requires a more adaptable, more easily applied definition for critical infrastructure than a decade-old document, or even a document updated every four years. As with the definition of covered cyber incident, the reality of the healthcare sector would suggest that nearly every entity, even several levels removed from a hospital or insurer, would be considered critical infrastructure. ***Furthermore, Premier requests that CISA provide clarity into which entities are responsible for reporting covered incidents that affect multiple covered entities, such as an incident that compromises a vendor and a provider.***

Premier specifically urges CISA to acknowledge the complexity and variety of entities that may be considered "health IT providers," which would broadly be included as covered entities under this proposed rule, and to provide clear guidelines for the functions, sizes, business relationships and type of data assets that would result in a health IT provider being considered a covered entity. Otherwise, CISA risks creating confusion for entities that may fall between the separate "healthcare" and "health IT" definitions, leaving entities uncertain if they are covered by neither, one or both definitions. Premier also recommends that CISA provide specific guidance on whether small health IT providers - which under the current broad definition may include single-individual or self-employed health IT consultants - qualify as covered entities. ***Premier would support an interpretation rule, such as a general exclusion of all entities below the Small Business Administration Table of Small Business Size Standards for healthcare entities.***

Additionally, as constructed, the proposed definition of covered entity seems to exclude health IT companies suffering data breaches from required reporting. However, data breaches could be construed as covered cyber incidents under the criteria established in this proposed rule. ***If CISA's intent is to fully exclude health IT from reporting cyber incidents involving health data breaches, this should be clarified explicitly in the proposed rule.***

IV. REDUCING BURDEN

Premier would like to highlight the importance of reducing burden on the entire healthcare system, particularly small entities or vendors, in the implementation of this proposed rule. Premier specifically recommends that CISA reconsider its proposal to require covered entities to report cyber incidents within 72 hours and instead finalize a reporting timeframe that allows covered entities to focus immediate attention in the wake of a cyber attack on protecting patients and keeping healthcare services operational, rather than focusing on filing paperwork with federal agencies.

Given CISA's description of the information that the agency requests for each cyber incident report, ***Premier believes that requiring healthcare organizations to complete reporting within 72 hours of a cyber incident would draw crucial human and technical resources away from an organization's top priority – providing healthcare services and keeping patients safe.*** Under the current proposals, even if an affected organization managed to submit partial information to CISA by the 72-hour mark, the process of submitting a supplemental report and possibly navigating one or more RFIs during an ongoing cyber incident would be a distraction at best and a serious misallocation of resources at worst.

Given the immediate risks to health, life and privacy associated with most cyber incidents in the healthcare sector, CISA should consider either relaxing the timeline for reporting or reducing the volume of technical information it hopes to collect from incident reports.

Premier recommends that CISA extend the proposed reporting timeline to 96 hours, or four days beyond discovery of the incident, to match reporting requirements implemented by the Securities and Exchange Commission through 2023's 88 FR 51896. This recent rule found a four-day reporting timeline reasonable in response to comments raising concerns about the disclosure of incomplete or inaccurate information, incongruity with other healthcare-specific disclosure windows and interruption to ongoing response efforts.

Further, Premier requests that CISA clarify when the clock starts for covered entities to report following a covered incident. ***Rather than requiring reporting within 72 hours (or 96 hours, as Premier has suggested) of "reasonable belief" that a cyber incident has occurred, Premier urges CISA to modify this language to allow for a 96-hour reporting timeframe from when the covered entity determines an incident is material/significant enough to qualify as a covered incident, which also aligns with recent SEC requirements.*** This will limit over-reporting, in alignment with CISA's aims for this proposed rule.

V. LIABILITY AND ENFORCEMENT MECHANISMS

Premier recognizes CISA's desire to propose mechanisms (e.g., formal requests for information and subpoenas) to help ensure statutorily-required information collection occurs, even when it is not voluntarily reported. However, Premier is concerned that the mechanisms proposed in this rulemaking could allow CISA to request information beyond what is required by statute. CISA should implement additional regulatory safeguards around the use of RFI and subpoena authority to prevent abuse of these powers that expands the scope of CIRCIA requests beyond the original purpose of the statute. ***Premier suggests that CISA make clear only the information included in the final, approved CIRCIA reporting form is subject to RFI or subpoena.***

Additionally, Premier urges CISA to refrain from, or severely limit, requesting information on CIRCIA reports that concern a company's mitigation efforts and response to ongoing incidents. As CISA acknowledges, this information was not included in the CIRCIA report parameters specified in statute, and for good reason. This information is often confidential, rapidly evolving and, in some cases, legally sensitive. Even if companies were willing and able to share such information, it would not be materially actionable for other organizations seeking to take defensive action against a similar threat. Cybersecurity incident response is by its very nature a rapidly evolving process, with many changing variables and evolving decision patterns. This renders the information reported at any one point in time relatively useless to CISA under the stated purpose of including these questions. Further, should a company's strategy for mitigating an incident change, and should CISA then require supplemental reports or use an RFI to request this information, such action would be well beyond the scope of this statute and would place an undue burden on covered entities while they are responding to an ongoing incident.

Required (rather than voluntary) reporting, particularly in a format that could be used for a coordinated government response, is likely to face numerous challenges during implementation. Not even last year's SEC rulemaking requiring disclosure of cyber incidents forced companies to disclose information about their incident response. ***Premier urges CISA to remove these questions from the CIRCIA form, or, at the very least, only ask these questions after the incident has concluded and exclude them from any information sharing agreement with other agencies or private sector actors, even in anonymized format***.

Even beyond the reporting of confidential information concerning covered entity response and mitigation efforts, CISA's proposed CIRCIA reporting form is overly broad and intrusive. Premier urges CISA to revisit the content it has selected for inclusion in the report with the intent to narrow reporting requirements on any information that could place an organization at risk for further attacks. ***CIRCIA reporting should be based on the principle of collecting the least amount of information necessary for CISA to achieve its objectives under statute – in this case, only such information necessary for CISA to understand risks of disruption to critical infrastructure sectors and respond adequately on a national scale.***

At present, CISA is attempting to consolidate multiple objectives and purposes within a single legislative mandate, to the detriment of the original purpose of developing timely and comprehensive visibility into threats across the nation's critical infrastructure. The information CISA proposes to collect on CIRCIA forms is too detailed – CISA is not a regulatory agency conducting an investigation, nor is it mandated to conduct a forensic review of cyber incidents that may happen to target critical infrastructure entities. By requiring the disclosure of information including, but not limited to, a covered entity's security controls; the bad actor and vulnerability they used to compromise the covered entity; and any security failures that may have affected the covered entity, CISA further complicates incident response and risks failing to accomplish any of its regulatory objectives.

CISA neither needs information this detailed to understand the scope of threats to a critical infrastructure sector, to respond to incidents itself, nor to issue alerts or warnings to other potentially effected entities. Each of these objectives could be fully executed by collecting more limited information that does not threaten covered entities with further liability or disclosure of private cybersecurity incident prevention, response and mitigation measures.

Premier would point to the long-established reality of cyber incident response and internal investigation, which are conducted under attorney-client privilege. Mandatory reporting of this extensive set of highly detailed, highly sensitive, and business-critical information may disincentivize thorough internal investigation into cybersecurity incidents at covered entities. Furthermore, these requirements may foster extensive internal debates about the scope of reporting that will distract from urgent incident response and mitigation efforts.

Public reporting of these metrics, even anonymized and aggregated, may create a template for bad actors seeking to identify targets, vulnerabilities and weaknesses in cybersecurity approaches, and likelihood of collecting on ransom payments. Premier urges CISA to put careful thought into the information published in its quarterly unclassified summaries of CIRCIA reports. For example, small and rural hospitals may be particularly vulnerable to cyberattacks and extortion for ransomware payments, so much so that the Biden Administration recently announced additional support to strengthen their cybersecurity posture. Should CISA publish quarterly reports showing, for example, that certain classes of hospitals or healthcare entities almost always paid the ransomware demand, it would provide a roadmap for bad actors and create a feedback loop where the most vulnerable organizations and those most likely to pay the ransom are targeted more and more frequently. While Premier fully supports CISA's proposal to exempt hospitals with fewer than 100 beds from reporting, this does not fully mitigate this potential risk. ***Premier urges CISA to implement a process by which covered entities may apply for exemption of their covered incident being included in public reporting to ensure that affected entities have a say in preserving their anonymity and protecting themselves from future attacks.***

Finally, Premier would like to note that government agencies have been subject to cyber attacks that have disclosed all manner of sensitive and confidential information, with entities like the Office of Personnel Management and CISA itself suffering high-profile data breaches. ***By collecting and storing high volumes of sensitive company information, including vulnerabilities and response strategies, CISA creates a high-profile target for state-backed bad actors.***

VI. HARMONIZATION WITH OTHER FEDERAL REQUIREMENTS

Premier supports CISA's stated intent to harmonize the reporting process for cyber incidents with that required by other agencies. Premier also appreciates CISA's intent to shield voluntarily-reported information from liability and use in regulatory action. However, other incident reporting requirements in healthcare, including HIPAA Breach Notifications and Food and Drug Administration (FDA) medical device vulnerability reporting, ***do*** carry potential penalties and are inherently different from the spirit and purpose of CIRCIA. Thus, Premier urges CISA to set appropriate guardrails from liability when voluntarily-reported data is shared from CISA to other federal healthcare regulators. Specifically, Premier urges CISA to ensure that any information sharing, coordinated government response, or harmonization efforts do not result in the unprotected sharing of confidential information, particularly concerning entity response or mitigation efforts.

It is important to note that FDA and Health and Human Services incident reporting does carry penalties and liability. Premier appreciates CISA's inclusion of stated intent to carry over liability protections for CIRCIA reports to harmonization efforts. However, this objective will have to be achieved during implementation. Premier urges CISA to carefully consider whether the disclosure of information reported through CIRCIA to another agency will give that agency cause to further investigate an entity following a cyber incident, even if the report itself is not used as cause.

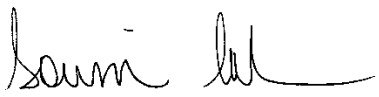
As this will be practically impossible to avoid in reality, Premier again recommends that CISA review carefully the information it requests on the CIRCIA form, as well as the information it allows to be shared during joint agency action. All information on entity response and mitigation, as well as any information beyond that directly related to the nature of the breach and the bad actor, should be shielded in this manner.

Furthermore, given the number of existing incident reporting requirements already governing the healthcare sector, Premier urges CISA to address these challenges expeditiously so as not to delay the implementation of CIRCIA Agreements for substantially similar reporting requirements, a mechanism which will help defray the burden that CIRCIA will create.

VII. CONCLUSION

Premier appreciates the opportunity to comment on CISA's cyber incident reporting proposed rule. If you have any questions regarding our comments, or if Premier can serve as a resource on these issues to the Administration in its policy development, please contact Mason Ingram, Director of Payer Policy, at Mason_Ingram@premierinc.com or 334.318.5016.

Sincerely,



Soumi Saha, PharmD, JD
Senior Vice President of Government Affairs
Premier Inc.