The Honorable Jennie M. Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane SW
Washington, DC, 20528

Dear Director Easterly:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide comments in response to Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements proposed rule issued by the Cybersecurity and Infrastructure Security Agency (CISA). HIMSS appreciates the opportunity to leverage our members' expertise to share feedback on this critical topic, and we look forward to continued dialogue with you, your office, and the Department of Homeland Security (DHS) on the implementation on this rule as we all continue to help protect our critical infrastructure.

HIMSS is a global advisor and thought leader and member-based society committed to reforming the global health ecosystem through the power of information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology driven by health equity. Through our innovation engine, HIMSS delivers key insights, education and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. Our members include more than 125,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations. Our global headquarters is in Rotterdam, The Netherlands and our Americas headquarters is in Chicago, Illinois.

We support CISA's efforts to enhance incident reporting protocols and believe that clear, practical guidelines are essential for safeguarding health information systems against evolving cyber threats. Our response aims to provide constructive feedback to help refine these requirements, ensuring they are both effective and feasible for the broad and diverse healthcare community, where the concern for patient safety must always remain paramount.

Our comments align with our previous comments we provided to the Request for Information you sought on this topic during the Fall of 2022. In those comments, as in this response to the proposed rule, we believe CISA should consider these points in implementing a final rule:

- Reducing Reporting Burden
- Balanced Reporting Requirements
- Granularity of Reporting
- Confidential handling and protection of Reported Information

HIMSS supports CISA's proposed definition of a cyber incident, "an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system" consistent with the definition of "incident" as put forth at 6 USC 650. We believe the definition effectively describes the types of events that should be reportable, while excluding incidents that do not meet this threshold as well as authorized actions conducted to improve cybersecurity posture, such as security assessments and penetration testing.

HIMSS agrees with CISA's proposal to define a substantial cyber incident as a cyber incident that leads to significant adverse effects. We recommend, for criterion (3), that the definition specifies that the covered entity's disruption of critical business operations or IT/OT operations or disruption of essential services to customers, clients, or other stakeholders, should be described as a "significant" or "substantial" disruption. This should include a disruption that may be internal to the organization or a disruption that is caused by a third-party or fourth-party supplier of that organization.) This clarification would make reporting more meaningful to CISA and less burdensome to covered entities by focusing on incidents that are more likely to have a material impact on other stakeholders.

HIMSS agrees that the tactics, techniques, and procedures (TTP) used to perpetrate a cyber incident and cause the requisite level of impact is typically not relevant to determining whether an incident is a substantial cyber incident. Given that covered entities may not be well suited to determining whether the TTPs are novel, we agree with CISA that it is appropriate to include all substantial incidents, without considering their novelty, but ask for leniency around the type and details of information that needs to be reported. In determining whether a substantial cyber incident has occurred, the means by which the cyber incident occurred is generally not pertinent but the resulting impact on the organization is what matters.

We support CISA's proposal to adopt the definition of "supply chain compromise" from 6 U.S.C. 650 verbatim for the regulation, except for replacing the term "incident" with "cyber incident."

Healthcare and Public Health Sector Specific Criteria

HIMSS understands the reasoning behind CISA's decision to propose an overall size-based criterion based on SBA small business size standards. We believe that all parts of the Healthcare and Public Health Sector should be working towards stronger cybersecurity resilience and are all vulnerable to cyber-attacks, as such, all cover entities in the sector, no matter their size, should be required to meet the reporting requirement proposed in this rule. While we recognize this could be difficult, especially for smaller entities, we think the whole sector would benefit from the information sharing that reporting would provide. Such a process aligns with our recommendation that all parts of the sector use the Department of the Health and Human Services' Cybersecurity Performance Goals, and strive to achieve those Enhanced Goals, whenever possible. We applaud the work for the Health Sector Cybersecurity Coordination Center (HC3) of the US Department of Health and Human Services. We

believe that HC3 can help facilitate the information sharing within our healthcare sector.

As CISA considers the content to be included in CIRCIA reports, HIMSS emphasizes the importance of recognizing that the amount of information available to covered entities regarding a covered cyber incident at the 72-hour mark considering a reasonable belief that the covered cyber incident has occurred will be limited. Patient safety in the healthcare sector means not just ensuring access to care but ensuring that patient safety is not jeopardized. Adding an additional requirement to provide detailed reporting of all the vulnerabilities exploited during a significant incident should not be prioritized over patient safety. Additionally, there may be situations in which law enforcement may request a delay in reporting of the incident. Therefore, considerations should be given to the 72-hour reporting mandate and what precisely is required during this period, when a healthcare stakeholder is appropriately prioritizing and triaging patients during this impacted window. As such, we suggest the reporting form should have the flexibility to accommodate the constraint and encourage CISA to acknowledge that some details will only become available in supplemental reports.

We look forward to discussing these issues in more depth. Please feel free to contact Eli Fleet, Senior Director of Government Relations, Eli.Fleet@himss.org with questions or to request more information.

Sincerely,

Thomas M. Leary, MA, CAE, FHIMSS
Senior Vice President and Head of Government Relations