

May 30, 2024

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, DC 20373

Re: Docket No. CISA-2022-0010 - Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) Reporting Requirements

Dear Director Easterly,

The HIMSS Electronic Health Record (EHR) Association appreciates the opportunity to respond to the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) Reporting Requirements notice of proposed rulemaking issued by the Cybersecurity and Infrastructure Security Agency (CISA). As the national trade organization representing EHR developers, we are deeply invested in ensuring the cybersecurity and resilience of critical healthcare infrastructure.

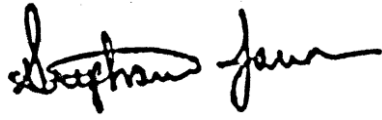
The 28 member companies of the EHR Association serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States. Together, we work to improve the quality and efficiency of care through the adoption and use of innovative, interoperable, and secure health information technology.

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 EHR stakeholders and the healthcare organizations and providers we serve.

We appreciate the potential for more effective collaboration on cybersecurity between industry and government. Our specific comments follow.

AdvancedMD	Elekta	Greenway Health	Netsmart	Sevocity
Altera Digital Health	EndoSoft	Harris Healthcare	Nextech	STI Computer Services
Athenahealth	Epic	MatrixCare	NextGen Healthcare	TruBridge
BestNotes	Flatiron Health	MEDHOST	Office Practicum	Varian – A Siemens Healthineers Company
CureMD	Foothold Technology	MEDITECH, Inc.	Oracle Health	Veradigm
eClinicalWorks		Modernizing Medicine	PointClickCare	

Sincerely,



Stephanie Jamison
Chair, EHR Association
Greenway Health

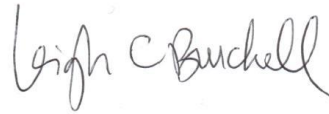


William J. Hayes, M.D., M.B.A.
Vice Chair, EHR Association
TruBridge

HIMSS EHR Association Executive Committee



David J. Bucciferro
Foothold Technology



Leigh Burchell
Altera Digital Health



Danielle Friend
Epic



Cherie Holmes-Henry
NextGen Healthcare



Ida Mantashi
Modernizing Medicine



Kayla Thomas
Oracle Health

Established in 2004, the Electronic Health Record (EHR) Association is comprised of 28 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

Electronic Health Record Association

Response to the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) Reporting Requirements Proposed Rule, Docket No. CISA-2022-0010

General Comments

Cyber Incident

The EHR Association 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." We believe the definition effectively describes the types of events that should be reportable, while excluding frivolous or intentional acts conducted to enhance cybersecurity, such as penetration testing.

Substantial Cyber Incident

The EHR Association 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 disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services, should be described as a "significant" or "substantial" disruption. 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.

Additionally, for criterion (4), we suggest that supply chain compromises include situations in which there is an exploitation of relied-upon open-source software vulnerabilities. Including these scenarios will help CISA gain a more comprehensive understanding of how known vulnerabilities in widely used software can lead to security events. This broader scope is crucial for developing effective strategies to mitigate such risks.

Substantial Cyber Incident: Minimum Requirements for a Cyber Incident To Be a Substantial Cyber Incident

The EHR Association agrees that the type of tactics, techniques, and procedures (TTP) used to perpetrate a cyber incident and cause the requisite level of impact is typically irrelevant 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.

Supply Chain Compromise

We support CISA's proposal to adopt the definition of "supply chain compromise" from 6 U.S.C. 650 verbatim for the regulation, with the exception of replacing the term "incident" with "cyber incident." The EHR Association suggests clarifying that this definition should explicitly include open-source software that an adversary exploits to perpetrate a substantial cyber incident. This clarification will ensure that the regulation comprehensively addresses potential vulnerabilities within the supply chain, including those arising from open-source software, and will provide CISA with a more complete view of how known vulnerabilities manifest in security events.

Sector-Based Criteria

Healthcare and Public Health Sector

The EHR Association applauds the decision to propose an overall size-based criterion based on SBA small business size standards. We agree with CISA's rationale that larger hospitals have a greater likelihood of experiencing significant impacts if they fall victim to a covered cyber incident and are more likely to have in-house or accessible cyber expertise to respond to and report a cyber incident. Additionally, CISA's standards would capture other large entities that play a critical role in the operations of the healthcare system, such as large claims clearinghouses. Focusing the reporting obligation on large entities avoids placing a disproportionate burden on smaller healthcare organizations, which are already facing operational challenges with limited resources, potentially diverting critical attention away from patient care and essential services.

Proposed Content To Be Included in All CIRCIA Reports

As CISA considers the content to be included in CIRCIA reports, the EHR Association emphasizes the importance of recognizing that the amount of information available to reporters of a covered cyber incident at the 72-hour mark will be limited. As such, we suggest the reporting form should have the flexibility to accommodate this constraint and encourage CISA to acknowledge that some details will only become available in supplemental reports.