Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, DC 20528-0380

November 14, 2022

Subject: Request for Information: The Cyber Incident Reporting for Critical Infrastructure Act of 2022; Docket ID: CISA-2022-0010

The Health Information Sharing and Analysis Center (Health-ISAC) and the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group appreciate the opportunity to submit comments related to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

Health-ISAC is a trusted community of critical infrastructure owners and operators within the Healthcare and Public Health (HPH) sector. The community is primarily focused on sharing timely, actionable, and relevant information including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques, and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material. Sharing can occur via machine to machine or human to human. Health-ISAC also fosters the building of relationships and networking through a number of educational events in order to facilitate trust. Working groups and committees focus on topics and activities of importance to the sector. Shared Services offer enhanced services for the Health-ISAC community to leverage for the benefit of all.

The HSCC represents the primary healthcare subsectors of direct patient care; public health; health plans and payers; pharma, blood and labs; medical technology; health information technology; and funeral homes and mass fatality managers. The mission of the HSCC Cybersecurity Working Group (CWG) is to collaborate with the Department of Health and Human Services and other federal agencies to identify and mitigate systemic risks that affect patient safety, security, and privacy, and consequently, national confidence in the healthcare system. Primary HSCC outputs for risk mitigation are the development of recommendations, best practices, and guidance for enterprise cybersecurity improvements, as well as advice to government partners about policy and regulatory solutions that facilitate mitigation of cybersecurity threats to the sector.

The H-ISAC and the HSCC jointly submit the below comments for consideration as CISA develops the regulations to implement the CIRCIA.

Errol S. Weiss
Chief Security Officer
Health-ISAC

Greg Garcia
Executive Director, Cyber Security
Health Sector Coordinating Council

Health-ISAC and HSCC CIRCIA RFI responses

1. Definitions, Criteria, and Scope of Regulatory Coverage
    a. Covered Entity
        i. Regulations should clarify if public sector, non-profits, and not for profit organizations are considered covered entities
        ii. The definition of covered entity should include common third-party service providers upon whom covered entities are dependent to provide their critical services. This could include things such as:
            1. Fuel
            2. Water
            3. Food
            4. Technology services
    b. Covered Incident
        i. Has a significant impact on the ability of the covered entity to produce or deliver critical services
        ii. Creates a direct and imminent threat to human life
    c. Supply Chain Compromise
        i. Clarify what is meant by the "supply chain of an information system"? An information system is comprised of people, processes, and technology. Is the intent that only the technology aspects of the system would be included?
    d. General Comment
        i. Would like to see the regulation create or reference a source to serve as a common set of definitions related to cyber incidents and reporting
2. Report Contents and Submission Procedures
    a. CISA should have a secure portal to receive reports and any supplementally reported information
    b. CISA should consider mandatory reporting requirements to be satisfied if those reports are sent by covered entities through their respective critical infrastructure sector ISACs to CISA. The ISAC path allows the covered entity to report the required information while doing so without attribution to the specific covered entity if that organization desires such anonymity.
3. Other Incident Reporting Requirements and Security Vulnerability Information Sharing
    a. Other federal reporting includes:
        i. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) HIPAA reporting requirements
        ii. Security and Exchange Commission reporting for material activities, plus proposed reporting requirements for information on cybersecurity programs

b. Additionally, there are numerous state and local reporting requirements such as:
    i. New York State General Business Law
    ii. New York State Health Law
    iii. Privacy laws in numerous states
c. Would like CISA to focus on harmonizing and minimizing the reporting burden for health sector organizations that are already heavily regulated
    i. CISA should identify other federal regulatory reporting requirements for incident reporting which, when complied with, would qualify as having met the reporting requirements under CIRCIA
    ii. If necessary, CISA should seek additional authorities in order to truly harmonize regulations related to incident reporting
    iii. CISA should work with international partners to harmonize incident reporting requirements from different nations

4. Additional Policies, Procedures, and Requirements
    a. None to submit
5. Other Considerations
    a. CISA should clarify the protections afforded to information submitted under this authority as well as what expectations covered entities can have of government.
    b. Protections
        i. The legislation provides certain protections for information that is reported under CIRCIA
            1. The regulation should emphasize that these protections continue even in the event the reports are compromised after they are submitted
            2. The regulation should also reinforce that all reporting, including but not limited to: initial reports, updated reports, third party reports, responses to questions from government officials (to include law enforcement), maintain those legal protections
    c. Expectations from the government
        i. The regulation should delineate:
            1. The type of information, general timelines, and methodology CISA will use to share information with ISACs and individual covered entities
            2. The type of support services that will be available to covered entities after they report a covered incident