HDA
Healthcare Distribution Alliance

HEALTH DELIVERED

July 3, 2024

FILED BY ELECTRONIC SUBMISSION

Jen Easterly, Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
1100 Hampton Park Blvd
Capitol Heights, MD 20743-0630

Todd Klessman, CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
1100 Hampton Park Blvd
Capitol Heights, MD 20743-0630

Re: Docket No. CISA–2022–0010; Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Dear Director Easterly and Team Lead Klessman,

The Healthcare Distribution Alliance (HDA) thanks the Cybersecurity and Infrastructure Security Agency (CISA) for the opportunity to submit comments to its "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements" (the "Proposed Rule").[1] HDA represents primary pharmaceutical distributors — the vital link between the nation's pharmaceutical manufacturers and pharmacies, hospitals, long-term care facilities, clinics and others nationwide. Since 1876, HDA has helped members navigate regulations and innovations to get the right medicines to the right patients at the right time, safely and efficiently.

Wholesale drug distributors ("distributors") continue to prioritize cybersecurity for the continuity of their business operations and the integrity of the supply chain. Further, HDA appreciates CISA's efforts to enhance cybersecurity and resiliency across industry and the government. Indeed, just this April HDA's Board of Directors invited CISA's Deputy Director Nitin Natarajan to speak on CISA's efforts to combat cyber threats, as well as distributors' continued interest to collaborate with the Agency on this important matter.

Any regulatory requirement to address cyber threats, however, should be carefully designed and balanced to address national security risks without unduly affecting business operations, services, cyber incident investigations, and proprietary information. **As currently written, it is HDA's position that there are still opportunities for CISA to improve clarity within the Proposed Rule. Specifically, HDA encourages CISA to refine the Proposed Rule to: 1) avoid redundant or conflicting regulatory reporting requirements, and 2) ensure that CISA implements standards and safeguards for digital security as well as data preservation and confidentiality.**

[1] 89 Fed. Reg. 23644 (Apr. 4, 2024).

1. **The Proposed Rule should avoid redundant and conflicting regulatory reporting requirements**.

In the Proposed Rule, CISA seeks comments on "[p]otential approaches to harmonizing CIRCIA's regulatory reporting requirements with other existing [f]ederal or [state, local, tribal, or territorial (SLTT)] laws, regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments."[2]

As a general matter, HDA highlights that regulatory requirements should eliminate redundancy and conflicts by simplifying reporting processes and minimizing duplicative efforts.[3] Doing so reduces unnecessary administrative burdens on distributors, allowing them to concentrate appropriate resources within their businesses. To that end, it is important that CISA streamline CIRCIA's reporting requirements with existing laws.

For example, **HDA recommends that CISA create a common reporting framework by consulting with federal and SLTT partners to streamline reporting forms, deadlines, and data elements. We also recommend that CISA consider developing a centralized point for covered entities to submit reports on cyber incidents and that covered entities could determine whether the report is disseminated to other government entities.** Regulators should not use the mere submission of a CIRCIA report or response as grounds to initiate an investigation into the covered entity.

Additionally, **HDA recommends that CISA consider simplifying the initial reporting requirements to the date of the incident, the known entities involved, and the type of incident,** which could prevent sensitive vulnerabilities from being exposed before they are remediated. Finally, **HDA recommends that CISA establish a pathway for covered entities to provide information on any operational challenges with redundant or conflicting reporting requirements.** CISA should use this information to improve regulatory reporting requirements for cyber threats.

2. **The Proposed Rule should ensure that CISA implements standards and safeguards for digital security as well as data preservation and confidentiality.**

CISA seeks comments on its "proposed approach to the treatment of information, restrictions of use, and applicable protections, including [but not limited to] the following:

> [] The proposed approach to designating CIRCIA Reports, responses to RFIs, or the information contained therein as commercial, financial, and proprietary information;
>
> [] The proposed application of the exemption from disclosure under FOIA and similar freedom of information laws;

[2] 89 Fed. Reg. 23654.
[3] HDA recently highlighted that "measures taken by the public and private sector to increase data transparency must be done carefully to avoid redundancy and unnecessary reporting burdens, while ensuring the value and usability of the data exchanged." Healthcare Supply Chain Resilience and Data Illumination (2023), *available at* https://www.hda.org/preparedness-and-response/.

> [] The proposed implementation of the statement that submission of a CIRCIA Report or response to RFI does not waive any applicable privilege or protection . . .".[4]

Submissions under CIRCIA will contain sensitive security details, business information, and other proprietary or confidential data. This sensitive information might involve events still under investigation, which could compromise such investigations if exposed to unauthorized third parties. Therefore, **HDA recommends that CISA implement strong digital security safeguards to protect this information from unauthorized access, retrieval, and utilization.** CISA should also conduct regular review of its safeguards to ensure that they are effective.

Beyond these safeguards, **HDA recommends that CISA develop guidance for federal agencies on how to uniformly handle data preservation and the confidentiality of information derived from CIRCIA reporting requirements.** With respect to data preservation, CISA should ensure that the scope of information collected from covered entites is only for the information necessary for the purposes stated in the Proposed Rule. Then, confidentiality requirements for that information should be specific as to the application of liability, privacy, due process, and evidentiary protections to organizations other than CISA. CISA should also clarify these data preservation and confidentiality requirements when sharing information from CIRCIA reporting requirements with non-government partners.

HDA recommends that reporting requirements should by default be designated as commercial, financial, and proprietary information. With respect to FOIA exemptions, HDA agrees that CISA should assert an exemption from disclosure in the event the Agency receives a FOIA request for information derived from reporting requirements. Finally, HDA agrees with CISA's interpretation that no privileges are waived in any situation where state or federal privileges and protections apply.

Conclusion

Thank you for the opportunity to provide comments on the Proposed Rule. If you have any questions, please contact me at kshankle@hda.org.

Sincerely,

/s/ Kala Shankle

Kala Shankle
Vice President, Regulatory Affairs

[4] *Id.* at 23741.