PDA Global Headquarters
Bethesda Towers,
Suite 600
4350 East West Highway
Bethesda, MD 20814 USA
TEL: +1 (301) 656-5900
FAX: +1 (301) 986-0296

PDA Europe gGmbH
Am Borsigturm 60
13507 Berlin
Germany

OFFICERS

Chair
Anil Sawant, PhD

Chair-Elect
Melissa Seymour, MBA

Secretary
Bettine Boltres, PhD

Treasurer
Emma Ramnarine, PhD

Immediate Past Chair
Susan Schniepp

President & CEO
Glenn E. Wright

DIRECTORS

Lisa Bennett

Cristiana Campa, PhD

Andrew Chang, PhD

Cylia Chen Ooi, MA

Mirko Gabriele, PhD

Marc Glogovsky, MS

Andrew Hopkins

Stephan O. Krause, PhD

Ivy Louis, MBA

Amy McDaniel, PhD

Brigitte Reutter-Haerle

Osamu Shirokizawa

3 July 2024

Jen M. Easterly
Director
U.S. Department of Homeland Security (DHS)
Cybersecurity and Infrastructure Security Agency (CISA)
245 Murray Lane
Washington, D.C. 20528-0380

Reference: Department of Homeland Security - Docket No. CISA-2022-0010 for "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," proposed rule.

Dear Director Easterly,

PDA appreciates the opportunity to provide feedback to the DHS as the agency develops and establishes best practices for the efficient prioritization, development, issuance, and use of the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). In our attached comments, PDA offers specific comments and feedback that we believe will be instrumental in further developing this program.

To be effective and successful, PDA believes harmonization with the requirements of other agencies is important to ensure compliance requirements are met. PDA appreciates the reference to Appendix A of the report Essential Medicines Supply Chain and Manufacturing Resilience Assessment; however, the report represents a static list of products that will likely be subject to continuous change. PDA suggests, if possible, that any references to essential medicines and/or medicines on drug shortage, etc., can be directed toward the source databases to ensure covered entities are accessing the most current information.

PDA is a non-profit international professional association of more than 10,000 individual members scientists having an interest in fields of pharmaceutical, biological, device manufacturing, and quality. Our comments have been prepared by a committee of PDA members with expertise in the areas covered in the Public Docket on behalf of PDA's Regulatory Affairs and Quality Advisory Board.

If you have any questions, please do not hesitate to contact me via email at wright@pda.org.

CONNECTING PEOPLE SCIENCE AND REGULATION®

Sincerely,

Glenn E. Wright
President and CEO

cc. Josh Eaton, PDA; Carrie Horton, PDA; Jessie Linder, PDA

PDA Member response: Department of Homeland Security - "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," proposed rule. (Docket No. CISA-2022-0010)

Responses to CISA: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

III. Background and Purpose

Page	Referenced Text	Proposed changes/recommendation
23654	**D. Harmonization Efforts** "Federal regimes that require the reporting of cyber incidents or ransom payments and discuss areas where CISA and its **Federal counterparts might want to, and be able to, harmonize their respective reporting requirements**. CISA leveraged the information gained via the RFI, listening sessions, and Federal consultations in the development of this NPRM, and intends to continue to engage Federal partners during the development and implementation of the final rule to harmonize reporting requirements and reduce the burden on potential covered entities, where practicable."	PDA strongly agrees that to the extent possible, the final rule should be harmonized with the requirements of other regulatory agencies. It would be prudent to have a register of all agencies that have harmonized requirements to support the covered entity in reducing duplication of reporting of cyber incidents.

IV. Discussion of Proposed Rule

A. Definitions

ii. Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident

Page	Referenced Text	Proposed changes/recommendation
23661	**3. Substantial Cyber Incident** "Consistent with these minimum requirements, CISA proposes the term substantial cyber incident to mean a cyber incident that leads to any of the following: (a) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;"	PDA proposes adding privacy to the referenced text. "(a) a substantial loss of confidentiality, **privacy**, integrity, or availability of a covered entity's information system or network;"

IV. Discussion of Proposed Rule (continue)

A. Definitions

ii. Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident

Page	Referenced Text	Proposed changes/recommendation
23662	**3. Substantial Cyber Incident** “**i. Impact 1: Substantial Loss of Confidentiality, Integrity, or Availability**” “For example, if an unauthorized individual steals credentials or uses a brute force attack to gain access to a system, they have caused a loss of the **confidentiality of a system**.”	The text includes the term ‘‘Confidentiality,’’ the personal privacy and proprietary information, but private data may not be confidential, and a specific treatment of the privacy concept, PDA suggests adding the word Privacy. “i. Impact 1: Substantial Loss of Confidentiality, **Privacy**, Integrity, or Availability…” PDA suggests adding an example of a substantial cyber incident related to private data and expanding on the definition of confidentiality of a system to include “if an entity or individual publishes personal information without the authorization of the owners.” Confidentiality does not necessarily enclose privacy, and a specific example of a privacy violation by a substantial cyber incident would help to understand the implications. “Personal Information” is defined on pg. 23672, but the definition does not include the “confidential” concept.
23665	**b. Guidance for Assessing Whether an Impact Threshold Is Met** “If, however, the covered entity knows with certainty the cause of the incident, then the covered entity only needs to report the incident if the incident was perpetrated without lawful authority.”	**PDA suggests removing** this text as it could confuse the issue of reportable incidents. If an event were lawfully occurring, it is not an incident and is not reportable. Also, allowing a report to not go into detail on the incident’s circumstances and corrective actions taken defeats the purpose of the report in the first place. This contradicts the spirit of reporting a significant incident, which is, by definition, an incident. If it were lawfully authorized, then it would not be an incident.

IV. Discussion of Proposed Rule

A. Definitions

Page	Referenced Text	Proposed changes/recommendation
23675	**v. Request for Comments on Proposed Definitions** 7. "As noted in the preamble, CISA believes…" "Similarly, should CISA use sophistication or novelty of a tactic as a justification for including or excluding any specific categories of incidents from the population of cyber incidents required to be reported?"	The type of TTP should not influence the reporting criteria. Instead, the impact of the incident determines it. PDA proposes revising the paragraph to read, "**Reporting requirements will not be determined by TTP** sophistication or novelty **but by impact. The approach used in the intrusion will inform the problem statement and root cause analysis, ultimately leading to the appropriate corrective action. CISA will use the report to inform the industry of incident trends.**"

IV. Discussion of Proposed Rule

B. Applicability

Page	Referenced Text	Proposed changes/recommendation
23679	**iii. Clear Description of the Types of Entities that Constitutes Covered Entities Based on Statutory Factors** "This risk ''equation'' is often summarized as Risk = Consequence ×Threat × Vulnerability. Viewed through this framing, CISA interprets the three factors listed in 6 U.S.C. 681b(c)(1) to each represent a different aspect of the risk equation: … speaks, albeit indirectly, to vulnerability, *i.e.*, the extent to which compromise of this entity could increase the vulnerability of critical infrastructure."	PDA suggests adding the text, "This risk equation…the vulnerability of critical infrastructure." "**Regardless of what was done to prevent an incident, reporting is required once it occurs to a covered entity**."

IV. Discussion of Proposed Rule

B. Applicability

iv. Explanation of Specific Proposed Applicability Criteria

Page	Referenced Text	Proposed changes/recommendation
23694	**i. Healthcare and Public Health Sector** “The second public health and healthcare sector sector-based criterion CISA is proposing would require reporting from manufacturers of drugs listed in Appendix A of the report *Essential Medicines Supply Chain and Manufacturing Resilience Assessment, …”*	Drug manufacturers are highly dependent on key suppliers like vials or API suppliers (lesson learned from the COVID-19 pandemic). The restricted list referred to in Appendix A could lead to companies misunderstanding which types of healthcare sectors are subject to reporting. PDA suggests adding clarity to the text “…is proposing would require reporting from manufacturers of drugs**,** listed in Appendix A of the report *Essential Medicines Supply Chain and Manufacturing Resilience Assessment, …” Clarify what the expectations are for key suppliers of covered entities in the event of a cyber incident.*

IV. Discussion of Proposed Rule

Page	Referenced Text	Proposed changes/recommendation
23730	**F. Data and Records Preservation Requirements** “To implement this requirement, CISA is to include in the final rule, a clear description of the types of data that covered entities must preserve, the period of time for which the data must be preserved, and allowable uses, processes, and procedures. “	To implement this requirement, PDA suggests that knowing the type of storage where the data to be preserved will be located gives crucial information about managing potential cyber incidents. The description of the data to be preserved should also include the storage identification (logic, physical, cloud, etc.) and the data warehousing mechanism.

V. Statutory and Regulatory Analyses

A: Regulatory Planning and Review

Page	Referenced Text	Proposed Text to be Introduced
23744	**i: Industry Cost** The main costs to industry associated with this proposed rule are (…) **becoming sufficiently familiar** with the rule to determine whether they are covered, and if it is determined that they meet one or more of the criteria for a covered entity, becoming familiar with how to comply with the requirements. The second largest cost associated with this rule would be **data and records preservation costs, followed by the cost for covered entities to complete the forms f**or the CIRCIA Reports (including preparation time)	There is a significant cost associated with implementing internal processes that would ensure compliance with the regulation, as well as initial and refresher training of relevant personnel PDA suggests identifying three levels of cost instead of just a standard cost. Instead of a table have the cost based on number of incidents and the size of the company and region. Assess the impact on US operations, though it does not occur outside the US. These events will be reported to CISA. Based on: • Number of incidents • Size of the company • Region PDA would appreciate more clarity, guidance, and harmonization amongst other agencies and international governing bodies, N1S2 Directive EI-wide legislation on cybersecurity.

VI. Proposed Regulation

Page	Referenced Text	Proposed changes/recommendation
23766	**226.1 Definitions** “Covered cyber incident means a substantial cyber incident experienced by a covered entity.”	PDA suggests adding specific text to clarify how the proposed regulation will apply to organizations with multinational operations. “Covered cyber incident means a substantial cyber incident experienced by **US-based operations** of a covered entity.”
23766	**226.1 Definitions** “Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including, but not limited to, operational technology systems such as industrial control systems, supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.”	PDA proposes adding **“business information systems,”** and **“enterprise resource planning,”** to clarify information systems “Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including, but not limited to, **business information systems, enterprise resource planning,** operational technology systems such as industrial control systems, supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.”

VI. Proposed Regulation (Continued)

Page	Referenced Text	Proposed changes/recommendation
23767	**226.1 Definitions** (4) "Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a: (i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (ii) Supply chain compromise."	PDA suggests adding a sub-point on "**compromise of internal infrastructure** " **or** **(iii) Compromise of internal infrastructure**
23767	**226.2 Applicability** "This part applies to an entity in a critical infrastructure sector that either: …"	PDA proposes clarifying in 226.2 Applicability that only US-based operations are in scope or modifying the definition of Covered cyber incident on page 23766. Industry needs clear direction on how the proposed regulation will apply to organizations with multinational operations.
23769	**VI. Proposed Regulation (cont.)** **226.3 Required reporting on covered cyber incidents and ransom payments.** "…until such date that the covered entity notifies CISA that the covered cyber incident at issue has concluded and has been fully mitigated and resolved." "(2) **Optional** notification that a covered cyber incident has concluded. A covered entity may submit a Supplemental Report to inform CISA that a covered cyber incident previously reported in accordance with paragraph (a) of this section has concluded and been fully mitigated and resolved."	PDA members understand that the first statement implies that CISA must be notified that the covered cyber incident at issue has concluded and has been fully mitigated and resolved. However, (2) states that notification via a supplemental report is optional, and no other mechanism is provided in the proposed regulation. PDA suggests clarifying what other "mechanisms" may be used to notify CISA that the covered cyber incident at issue has been concluded and fully remediated.

VI. Proposed Regulation (Continued)

Page	Referenced Text	Proposed changes/recommendation
23771	**226.9 Required information for Ransom Payment Reports.** (1) Identification and description of the function of the affected networks, devices, and/or information systems that were, or are reasonably believed to have been, affected by the ransomware attack, including but not limited to: (i) **Technical details and physical locations of such networks, devices, and/or information systems;**	PDA recommends that CISA consider balancing the resource load and technical items necessary to run the report. We recommend removing the “(i) **Technical details and physical locations of such networks, devices, and/or information systems”** from the proposed rule.
23772	**VI. Proposed Regulation** **226.11 Required information for Supplemental Reports.** (c) **Optional** information to provide notification that a covered cyber incident has concluded. Covered entities that choose to submit a notification to CISA that a covered cyber incident has concluded and has been fully mitigated and resolved may submit optional information related to the conclusion of the covered cyber incident.	PDA suggests the alignment of these two sections. Remove ‘**optional’** from section (c) to align with NIH 2. This would also align with an earlier text (p. 23769), which implies that CISA **must be notified** that the covered cyber incident has concluded and been fully mitigated and resolved. However, (2) states that notification via a supplemental report is optional, and there is no other mechanism provided in the proposed regulation

General Comments	PDA Discussion
The CISA report describes actions to be performed differently for medical device manufacturers than drug manufacturers and further refers to the drugs listed in Appendix A of the Essential Medicines Supply Chain and Manufacturing Resilience Assessment, sponsored by the U.S. Department of Health and Human Services (HHS) Administration for Strategic Preparedness and Response (ASPR). **Reference to Appendix A** CISA Covered Entity Criteria for the Healthcare and Public Health Sector: • The first criterion CISA proposes related to this sector will mean that certain entities providing direct patient care will be considered covered entities. • The second public health and healthcare sector sector-based criterion CISA is proposing would require reporting from manufacturers of drugs listed in **Appendix A of the report Essential Medicines Supply Chain and Manufacturing Resilience Assessment**, sponsored by the U.S. Department of Health and Human Services (HHS) Administration for Strategic Preparedness and Response (ASPR). • https://www.armiusa.org/wp-content/uploads/2022/07/ARMI_Essential-Medicines_Supply-Chain-Report_508.pdf	PDA appreciates the reference to Appendix A of the report *Essential Medicines Supply Chain and Manufacturing Resilience Assessment;* however, the report represents a static list of products that will likely be subject to continuous change. PDA suggests, if possible, that any references to essential medicines and/or medicines on drug shortage, etc., can be directed towards the source databases to assure covered entities are accessing the most current information.