DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 226

[Docket ID: CISA-2022-0010]

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Rulemaking; Town Hall Meetings

AGENCY: Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

ACTION: Notification of town hall meetings.

SUMMARY: This notice announces town hall meetings to allow external stakeholders a limited additional opportunity to provide input on refining the scope and burden of the CIRCIA Notice of Proposed Rulemaking (NPRM) issued in the *Federal Register* on April 4, 2024. The proposed CIRCIA rulemaking seeks to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended, by implementing covered cyber incident and ransom payment reporting requirements for covered entities.

DATES: Town hall meetings are scheduled to be held on the following dates:

- *Chemical Sector; Water and Wastewater Sector; Dams Sector; Energy Sector; and Nuclear Reactors, Materials, and Waste Sector* – March 9, 2026 – Virtual
- *Commercial Facilities Sector; Critical Manufacturing Sector; and Food and Agriculture Sector* – March 12, 2026 – Virtual
- *Emergency Services Sector, Government Facilities Sector, Healthcare and Public Health Sector* – March 17, 2026 – Virtual
- *Communications Sector; Transportation Systems Sector; and Financial Services Sector* – March 18, 2026 – Virtual
- *Defense Industrial Base Sector and Information Technology Sector* – March 19, 2026 – Virtual

CISA also plans to hold two general town hall meetings scheduled to be held on the following dates:

- General Session 1: March 31, 2026 – Virtual
- General Session 2: April 2, 2026 – Virtual

All town hall meetings are tentatively scheduled to take 2 hours. The start and end times will be during core business hours (Eastern Time) and will be posted on www.cisa.gov/circia. CISA reserves the right to extend the schedule, reschedule, or cancel any of these meetings for any reason, including for severe weather, a health emergency, a lack of registered attendees, or an incident that impacts CISA's ability to safely conduct these meetings at the proposed date, time, or location. Any changes or updates to dates, locations, or start and end times for these town hall meetings will be posted on www.cisa.gov/circia and communicated via email to registered attendees.

ADDRESSES: Registration is required to attend each town hall meeting. To register, visit www.cisa.gov/circia and follow the instructions to complete registration. Registration for each town hall meeting will be accepted until 5:00 p.m. Eastern Time two (2) business days before the meeting.

Docket: To view the docket, including documents, written materials, and comments related to the proposed rulemaking, go to https://www.regulations.gov, type CISA-2022-0010 in the search box, and click "Search."

FOR FURTHER INFORMATION CONTACT: Nichole Clagett, CIRCIA Deputy Associate Director, Cybersecurity and Infrastructure Security Agency, circia@cisa.dhs.gov, 202-815-4427.

SUPPLEMENTARY INFORMATION:

I. Background

Enacted in March 2022, CIRCIA directed CISA to issue a rulemaking requiring "covered entities" to report "covered cyber incidents" and "ransom payments" to CISA. (6 U.S.C. 681b(b); 6 U.S.C. 681 - 681g). Before initiating the rulemaking process, CISA published a

Request for Information (RFI), which was open for 60 days for public comment, and held listening sessions in person across the country and virtually with each of the 16 critical infrastructure sectors. (87 FR 55830 & 55833 (Sep. 12, 2022) and 87 FR 60409 (Oct. 5, 2022)). CISA received approximately 130 comments in response to the RFI and approximately 730 people attended the listening sessions. Consistent with CIRCIA's requirements, CISA published an NPRM on April 4, 2024, which was open for a 90-day public comment period. (89 FR 23644 and 37141).[1] CISA received approximately 300 comments in response to the NPRM.

CISA received many written comments and requests from critical infrastructure sector entities and other stakeholders to directly engage CISA further on the CIRCIA rulemaking. CISA appreciates stakeholders' interest and concern that CISA implement CIRCIA to maximize its impact on improving our nation's cybersecurity posture while minimizing unnecessary burden to entities in critical infrastructure sectors. CISA remains committed to working within the rulemaking process to enable stakeholders to provide input as CISA finalizes the rulemaking to strike an appropriate balance of costs and benefits.

Given the broad stakeholder community that CIRCIA may potentially impact, CISA will conduct a series of town hall meetings to solicit input on the NPRM. CISA selected this approach to additional engagement on the CIRCIA NPRM to provide access to CISA across the broad range of entities within the critical infrastructure sectors. This approach will also enable maintenance of a transparent and accurate record of stakeholder feedback. Because this is a limited engagement opportunity for stakeholders, CISA will not reopen the comment period for the NPRM at this time but may elect to do so in the future if CISA determines that doing so is warranted.

II. Specific Topics of Interest

[1] CISA also published a correction related to the Transportation Systems sector-based criteria on June 3, 2024. (89 FR 47471).

During the town hall meetings, CISA welcomes any specific, actionable improvements that CISA could implement in the final rule to clarify or reduce burden of CIRCIA's regulatory requirements while enhancing the federal government's visibility into the cyber threat landscape for critical infrastructure sectors. Input that would be most useful are examples on how the NPRM may impact regulated entities and specific improvements, including how such suggestions would increase the benefit of CIRCIA to critical infrastructure owners and operators. Specifically:

- The scope of entities that would only be considered covered entities because of size-based criterion and would not meet any of the sector-based criteria.
- The proposed decision to include a size-based criterion.
- The proposed sector-based criteria used in the Applicability Section to identify certain entities as covered entities.
- Potential alternative sector-based criteria for the Commercial Facilities Sector, Dams Sector, and Food and Agriculture Sector if CISA modifies or removes the general size-based threshold criterion.
- The use of the Environmental Protection Agency Risk Management Program (EPA RMP) as alternative sector-based criteria for the Chemical Sector given that CFATS remains unauthorized.
- CISA's proposal to incorporate Oil and Natural Gas Subsector entities primarily through the size-based threshold instead of developing one or more criteria specifically targeting Oil and Natural Gas Subsector entities—and whether this size threshold will capture the correct population of entities in this subsector.
- Whether CISA should include in the final rule specific criteria to cover Managed Service Providers (MSPs) or Cloud Service Providers (CSPs) utilizing open-source software or additional, specific criteria that would require reporting related to open-source code, open-source software, or code repositories.

- Whether there are other lists of entities in a critical infrastructure sector that should be included as covered entities (either instead of the applicability criteria for covered entity proposed in the NPRM or in addition to the proposed applicability criteria), to the extent that those listed entities fall within a critical infrastructure sector.
- The proposed examples of incidents that likely would or would not qualify as a substantial cyber incident, to include whether the examples provided by CISA are accurate and whether there are other types of incidents that it would be useful to include in the list of examples of incidents that likely would or would not qualify as a substantial cyber incident.
- CISA's proposed interpretations of what constitutes substantially similar information and a substantially similar timeframe.
- Improvements to the content of reports.
- Improvements to the proposed approach for RFIs and subpoenas.
- Potential approaches to harmonizing CIRCIA's regulatory reporting requirements with other existing federal or state local, tribal, or territorial (SLTT) laws, regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments.
- How to reduce actual, likely, or potential duplication or conflict between other federal or SLTT laws, regulations, directives, or policies and CIRCIA's reporting requirements.

III. Town Hall Meeting Procedures and Participation

Town hall meetings are intended to provide stakeholders with the opportunity to directly share their feedback on the CIRCIA NPRM with CISA. CISA will not be able to share non-public or deliberative information about the CIRCIA rulemaking during meetings, nor will CISA be able to commit to resolving policy issues impacting or impacted by the rulemaking in a specific manner.

Registration is required to attend each town hall meeting. See the ADDRESSES Section of this notice for instructions on how to register. CISA will send registered individuals a meeting-specific link and any other pertinent information necessary to participate in the meeting via email. CISA encourages individuals representing entities that they do not believe fall within a specific critical infrastructure sector to register for a general town hall meeting. Those individuals who are unable to attend a town hall meeting for their sector may also attend general town hall meetings.

Each town hall meeting is expected to last up to a total of two hours. To allow as many stakeholders as possible the opportunity to speak, CISA requests that speakers limit their remarks and responses to three minutes. CISA reserves the right to stop speakers who exceed the limit. Please note that a town hall meeting may adjourn early if all registered individuals present have had the opportunity to speak prior to the scheduled conclusion of the meeting.

Town hall meetings will be recorded and transcribed by CISA. After a meeting has taken place, CISA will post copies of the transcripts of the town hall meetings in the docket for the CIRCIA rulemaking. CISA will also include the name and organizational affiliation of each person that attends town hall meetings in the docket. Additionally, CISA will provide public notice that a meeting has taken place on www.cisa.gov/circia with a link to transcripts and any associated materials.

If a participant wants CISA to consider data or specific written materials as part of a town hall meeting, stakeholders must provide that information to CISA in writing no later than seven (7) calendar days after the meeting. Written material must be sent to CIRCIA@cisa.dhs.gov and will be made publicly available in the docket for the CIRCIA rulemaking.

CISA is committed to ensuring all participants have equal access to this opportunity regardless of disability status. If you require reasonable accommodation due to a disability to fully participate, please contact CISA at circia@cisa.dhs.gov as soon as possible prior to the town hall meeting that you wish to attend.

Madhu Gottumukkala
Acting Director
Cybersecurity and Infrastructure Security Agency

[FR Doc. 2026-02948 Filed: 2/12/2026 8:45 am; Publication Date: 2/13/2026]