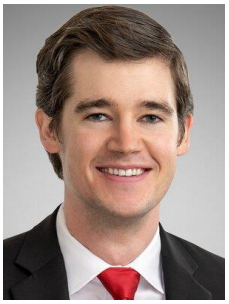
Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

CISA Town Halls Signal Key Cyber Rule Changes Ahead

By **Ashden Fein, Caleb Skeath and Web Leslie** (September 4, 2026, 12:54 PM EDT)


Ashden Fein


Caleb Skeath


Web Leslie

More than two years after proposed regulations were published, the final rule to implement sweeping notification requirements under the Cyber Incident Reporting for Critical Infrastructure Act, or CIRCIA, may finally be taking shape.

In June, the Cybersecurity and Infrastructure Security Agency held a series of town halls to gather additional stakeholder input on the proposed rule, offering potential insights into how the agency may address key issues in the final rule.

This article summarizes central themes from the town halls and highlights practical considerations to help organizations ready themselves for publication of the final incident reporting regulations under CIRCIA, which could be as soon as this month.[1]

Background and Context

CIRCIA requires covered entities to report any covered cyber incident within 72 hours, and any ransomware attack resulting in a ransom payment within 24 hours, to CISA.

At a high level, these obligations apply to a broad swath of critical infrastructure owners and operators within one of the 16 sectors established under Presidential Policy Directive 21.[2] Although these core reporting requirements are set forth in the statute, key aspects of CIRCIA are subject to rulemaking, and the final rule could materially affect the scope and implementation of these requirements.

While CISA has not announced a publication date, a final rule could be issued as soon as this month. On July 3, after the CIRCIA town halls concluded, the administration published the 2026 Unified Agenda of Federal Regulatory and Deregulatory Actions, which identified September as the target for publication.[3]

However, other issues may still delay publication. CISA stated in its original town hall announcement that the agency could decide to reopen the formal comment period for CIRCIA "if doing so is warranted."[4] Additionally, the final rule will likely undergo review by the White House's Office of Information and Regulatory Affairs, a process that can take up to 90 days.

Against this backdrop, a September publication date might be less likely, but organizations should still

consider taking steps to prepare for the final rule.

CIRCIA Town Halls

Following CISA's publication of the proposed rule in April 2024, industry and other stakeholders submitted hundreds of comments.

How CISA might address those comments remained unclear until the agency announced earlier this year that it would host a series of town halls to gather additional stakeholder input.[5] The town halls, which were held in June, provided potential insights into how CISA may address several key issues in the final rule.

Across these topics, perhaps the most notable feature was CISA's repeated push for concrete implementation recommendations.

When participants urged narrowing the rule, CISA often asked for proposed language, examples or objective criteria, suggesting that practical administrability may be central to how the agency evaluates potential revisions.

Covered Entity Definition

According to the statute, a covered entity is an entity in a critical infrastructure sector that satisfies the definition established by CISA in the final rule, delegating the task of defining covered entities to subsequent rulemaking.

Under the proposed rule, CISA broadly defined "covered entity" to include any entity within one of the 16 critical infrastructure sectors that either (1) does not qualify as a small business under applicable Small Business Administration regulations, or (2) meets one or more sector-specific criteria.

Numerous town hall participants urged CISA to narrow these applicability criteria, and many called for eliminating the size-based criterion altogether. CISA did not commit to narrowing the definition, but agency officials repeatedly sought more concrete input on how sector-specific applicability criteria could be refined, suggesting that CISA may be considering targeted technical clarifications.

It remains unclear whether the final rule will clarify other aspects of the definition, including the potential that CIRCIA may apply extraterritorially to non-U.S. entities or critical infrastructure located outside the U.S.

Covered Cyber Incident Definition

The definition of a "covered cyber incident" in the proposed rule turns on four impact-based criteria: (1) substantial loss of confidentiality, integrity or availability; (2) serious effect on safety and resilience; (3) significant operational disruption; and (4) significant third-party compromise.

Any incident experienced by the covered entity that meets one or more criteria would trigger reporting obligations, even if the affected systems or data are not themselves considered critical infrastructure. Several town hall participants stated that the current standard could result in overreporting and inundate CISA with low-value information.

Again, CISA did not commit to changes, but it repeatedly asked speakers for specific language and objective criteria, suggesting that CISA is evaluating whether additional clarifications could be incorporated into the final rule.

Harmonization, Timing and Report Contents

CIRCIA provides an exception under which covered entities need not report to CISA if they make a legally required report to another federal agency that contains substantially similar information, on a substantially similar time frame, and that can be shared with CISA under an interagency information-sharing agreement.

However, in the proposed rule, CISA did not identify any existing requirements that would satisfy this exception. Participants from various sectors called for renewed efforts to harmonize CIRCIA with the Health Insurance Portability and Accountability Act, U.S. Securities and Exchange Commission disclosure rules, and other federal, state and sectoral regimes under this exception.

CISA acknowledged this concern and committed to coordinating with relevant partners to avoid unduly burdening the regulated community. However, CISA stopped short of committing to revisit the "substantially similar" standard, and its careful framing suggests that any significant harmonization between the final rule and existing reporting requirements could be limited.

Participants also pressed CISA on the 72-hour reporting clock and the breadth of information covered entities must report within that time frame. In response, CISA pointed to the proposed rule's supplemental reporting mechanism, explaining that entities can submit substantially new or different information after their initial report, if they have only limited details at the time of reporting.

Regarding the contents of reports, some participants emphasized the security risk of aggregating sensitive information about covered entities' system architecture, controls and unmitigated vulnerabilities. CISA acknowledged these concerns and signaled willingness to receive additional stakeholder input on how to scope down content requirements. CISA's reference to the supplemental reporting mechanism suggests it will continue to prioritize rapid reporting, but may also be willing to narrow content requirements to facilitate speed and potentially address security concerns as well.

How to Prepare

While the contours of the final rule remain unknown, the text of CIRCIA and the town hall discussions suggest that the requirements are unlikely to change substantially when the CIRCIA rule goes into effect. Organizations should consider the following preparations.

- Update incident response plans and notification procedures in anticipation of new reporting requirements, including the potential need to compile and submit detailed information under a compressed time frame.

- Stress-test incident response plans through tabletop exercises to evaluate readiness and sharpen decision-making and communications processes.

- Inventory current reporting obligations to prepare for potential challenges when CIRCIA goes into effect, in particular where CIRCIA requirements may result in duplicative reporting — such as public reporting under SEC disclosure rules, the European Union's Network and Information

Systems Directive 2, the Cyber Resilience Act or other obligations — or implicate other legal risks.

- Update third-party contracts to require prompt vendor and service provider notification of incidents that may trigger CIRCIA reporting obligations.

- Assess the scope and potential applicability of CIRCIA and its information-sharing protections, including Freedom of Information Act exemptions, nonwaivers of legal privilege and prohibitions on regulatory enforcement based on CIRCIA report contents.

Ashden Fein is a partner and co-chair of the data privacy and cybersecurity practice at Covington & Burling LLP.

Caleb Skeath is a partner at the firm.

Web Leslie is an associate at the firm.

[1] Town hall transcripts, an attendees list, and supplemental materials that CISA received within seven days of the meetings are also available on the public CIRCIA rulemaking docket. https://www.regulations.gov/docket/CISA-2022-0010.

[2] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[3] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=1670-AA04.

[4] https://www.federalregister.gov/documents/2026/02/13/2026-02948/cyber-incident-reporting-for-critical-infrastructure-act-circia-rulemaking-town-hall-meetings#p-20.

[5] https://www.federalregister.gov/documents/2026/02/13/2026-02948/cyber-incident-reporting-for-critical-infrastructure-act-circia-rulemaking-town-hall-meetings?utm_campaign=subscription+mailing+list&utm_medium=email&utm_source=federalregister.gov.