wiley

ALERT

CISA Reopens Comment Opportunity on Cyber Incident Reporting Requirements

February 13, 2026

The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is working to finalize a rule that would require large segments of industry to rapidly report to the government when they become victims of cybersecurity incidents. As we noted in March 2024, Congress mandated CISA's proposed new cyber incident reporting framework under the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Signed into law on March 15, 2022, CIRCIA directed CISA to (1) issue a Notice of Proposed Rulemaking (NPRM) by March 15, 2024, and (2) issue a final rule within 18 months of publication of the NPRM (i.e., fall 2025). In response to significant public and industry pushback against its broad NPRM, CISA is now taking additional time to develop the final rule.

During the proceeding, commenters expressed significant concerns about the number and scope of companies that would be covered, a definition of reportable cyber incident that would flood CISA with low-impact reporting, the lack of substantial steps proposed to harmonize CIRCIA requirements with other cybersecurity regulatory requirements, and expansive proposed reporting requirements that would gather sensitive information from victim companies.

CISA Will Hold Sector-Focused "Town Halls"

CISA announced in a Federal Register notice on February 13, 2026 that it will host a series of virtual "town hall" meetings between March 9 and April 2, 2026 to obtain additional feedback on the CIRCIA rulemaking. Each of the town halls combine several critical infrastructure sectors together with the exception of a general session.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy and Cybersecurity Litigation and Investigations

Privacy, Cyber & Data Governance

- Chemical Sector; Water and Wastewater Sector; Dams Sector; Energy Sector; and Nuclear Reactors, Materials, and Waste Sector – March 9, 2026
- Commercial Facilities Sector; Critical Manufacturing Sector; and Food and Agriculture Sector – March 12, 2026
- Emergency Services Sector, Government Facilities Sector, Healthcare and Public Health Sector – March 17, 2026
- Communications Sector; Transportation Systems Sector; and Financial Services Sector – March 18, 2026
- Defense Industrial Base Sector and Information Technology Sector – March 19, 2026
- General session 1 (i.e., not focused on a particular sector) – March 31, 2026, and general session 2 – April 2, 2026.

Interested parties should register via CISA.gov to participate in the meetings. CISA has announced that the purpose of the town hall meetings is "to solicit input on the NPRM," and that CISA will be unable to share deliberative information about the rulemaking nor commit to particular policy outcomes. As a result, attendees should not expect to hear new substantive information from the agency about the forthcoming rule – rather, the town halls are an additional opportunity for potentially impacted stakeholders to provide feedback to CISA. CISA had previously announced via a regulatory filing with the Office of Management and Budget that the agency intended to finalize the CIRCIA rule by May 2026. That date is likely to slip later to accommodate what we expect to be substantive feedback from stakeholders through these town halls.

Industry Should Consider Identifying "Specific, Actionable" Improvements to the NPRM

CISA's announcement frames the agency's questions in terms of the impact of the NPRM on regulated entities and improvements to increase the benefit to critical infrastructure entities. Specifically, CISA seeks "specific and actionable" improvements to the NPRM, including:

- Potential modifications to, or elimination of, the size-based criteria for defining a "covered entity" that would have to report incidents;
- Examples of cybersecurity incidents that should not qualify as "substantial" incidents that would be required to be reported to CISA under the NPRM;
- Proposed interpretations of how CISA could find another agency's reporting requirement to be "substantially similar" and allow CISA to accept that agency's report in lieu of a CIRCIA report (in turn reducing reporting burdens on the affected company);
- Improvements to the content of required reports; and
- Specific "covered entity" definition criteria addressing open-source code, software, or code repositories.

In addition to the town hall series, CISA will accept written materials or data into the record for town hall meeting no later than seven (7) calendar days after that meeting. While CISA's announcement says that the agency is not reopening the comment period on the NPRM at this time, the town halls offer interested stakeholders an important opportunity to educate the agency on the potential impacts of the CIRCIA rule.

***

Wiley's Privacy, Cyber & Data Governance team has helped companies of all sizes from various sectors proactively address risks and compliance with new cybersecurity laws and requirements. Our team has been actively involved in advocacy to CISA on these new rules. Please reach out to any of the authors with questions.