Scope Issues For Cos. To Consider Ahead Of Cyber Rules

By **Megan Brown, Lyn Brown and Sydney White** (September 2, 2026)

Megan Brown

Lyn Brown

Sydney White

As the federal government moves toward more regulation of critical infrastructure cybersecurity, organizations face a challenge: determining whether they operate within one of 16 critical infrastructure sectors and therefore are likely to fall under rules implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which are expected to be finalized this fall.

Uncertainty stems from inconsistent critical infrastructure sector definitions and overlapping sector boundaries.

The Cybersecurity and Infrastructure Security Agency published a notice of proposed rulemaking, or NPRM, in the Federal Register on April 4, 2024, proposing cyber incident and ransomware payment reporting requirements for 16 sectors.

CISA estimated that over 300,000 entities across the 16 critical infrastructure sectors will fall within CIRCIA's scope, but the rules' application is not clear. This creates compliance risk and operational uncertainty, particularly for organizations operating at sector boundaries or providing services that support multiple sectors.

This article identifies scoping issues and offers practical steps to consider, as organizations anticipate the effect of the forthcoming rules.

Why Sector Classification Matters

Understanding whether an organization falls within a critical infrastructure sector has substantial consequences for operations, regulatory compliance and legal liability.

Under CIRCIA, covered entities must report covered cyber incidents to CISA within 72 hours and ransomware payments within 24 hours.

In the draft rules, CISA proposes applying requirements to "covered entities," defined as entities in one of the critical infrastructure sectors that exceed a small business size standard or meet one or more designated sector-based criteria.

The effect varies by sector. For example, a large retailer may be covered because it is part of the commercial facilities sector and exceeds the small business threshold. But in some sectors, entities that meet sector-based criteria would be covered, regardless of size.

In addition, some sectors include organizations "involved with" certain functions, while others focus on those that own or operate infrastructure. That approach received considerable criticism in comments on the NPRM, so the definition of covered entities may change, adding uncertainty for those preparing for new rules.

Why does this matter? Organizations that incorrectly assume they are not covered may face

significant consequences, including penalties if they fail to report a cyber incident.

The stakes are particularly high for government contractors, where overlap between companies operating in critical infrastructure and those holding government contracts means CIRCIA requirements will broadly affect this sector and create duplicative reporting obligations.

Four examples illustrate the varied approaches in the proposed rules.

Communications Sector: No Size-Based Safe Harbor

The communications sector represents a well-defined yet broadly scoped sector, made up of wireless, broadcast, satellite, wireline and cable operators, with numerous interdependencies to other sectors.[1]

The communications sector would not be subject to size-based exemptions, creating challenges for regional and smaller companies, rural operators, and specialized providers who would have to meet the same reporting requirements as larger players, but with fewer resources.

CIRCIA regulations will complicate operations because parts of the communications sector already face some incident reporting obligations, such as under Federal Communications Commission rules governing customer proprietary network information, U.S. Securities and Exchange Commission rules for public company cyber reporting, government contracting obligations, and state obligations.

CIRCIA rules will add to that reporting landscape.

Transportation Sector: Broad Scope Across Modes

The transportation systems sector encompasses entities across multiple modes. CISA's National Critical Functions framework identifies multiple transportation-related functions, including transport of cargo or passengers by air, rail, road, vessel, pipeline and mass transit.[2]

The scope of the sector under the new CIRCIA rules is unclear because many organizations provide services that support transportation without directly operating transportation assets. Organizations play a supporting role in transportation by providing fuel, maintenance services, logistics software or transportation management systems.

Some transportation sector entities already face cybersecurity reporting obligations, including security directives from the Transportation Security Administration that apply to pipeline and rail operations, and SEC and state data breach notification obligations.[3] The proposed CIRCIA rules will overlap with those obligations, rather than replace them.

Information Technology Sector: Complex Exemptions and Criteria

Organizations in the information technology sector face complex classification challenges due to the proposed rules' size-based exemptions and sector-specific criteria that create multiple pathways to coverage.

The U.S. Department of Homeland Security's 2016 IT Sector-Specific Plan describes numerous things as critical functions: those that produce hardware, software, and IT

systems and services, often in collaboration with the communications sector.[4] Some IT organizations provide services that could be classified as either IT or communications.

The rules' approach is complex. For example, the proposed rules establish size-based thresholds for computing infrastructure providers and computer facilities management entities, while exempting smaller organizations in those categories from reporting requirements.

CISA proposed four sector-based criteria that can trigger coverage regardless of size: federal IT service providers who contract with government agencies; critical software vendors whose products are widely deployed in critical infrastructure; operational technology original equipment manufacturers who produce industrial control systems; and domain name system operators who provide internet naming and routing services.[5]

Multiple classification pathways mean that an organization might fall below size thresholds but still be covered under functional criteria or operate in multiple IT subsectors with different applicability determinations.

Food and Agriculture Sector: Farm-to-Table Complexity

The food and agriculture sector encompasses the food supply chain and includes farms, ranches, food processing facilities, distribution networks, grocery retailers and restaurants. Organizations must determine whether their primary function places them in food and agriculture or whether a supporting role categorizes them in transportation, IT or another sector.

Small and medium agricultural businesses face additional uncertainty, as they will have to consider whether their function is sufficiently critical and whether they meet one or more size thresholds.

Determining the reach of the rules may be challenging for organizations like agricultural technology companies that provide precision farming software and sensors, food safety testing laboratories, agricultural-chemical distributors or cold-storage warehouse operators. Many of these entities support the food supply chain with IT and operational support, without directly producing or processing food products, raising questions about their classification.

The Data Center Dilemma

Data centers represent a classification challenge. Executive actions, DHS guidance and IT sector planning documents suggest data centers may be critical infrastructure.

Executive Order No. 14318, issued in July 2025, was aimed at accelerating federal permitting of data centers, and identifies AI data centers as essential to national security, economic prosperity and scientific leadership. This suggests explicit national security concerns, but data centers' sector classification under CIRCIA is not clear.

The CIRCIA NPRM mentions data centers only in the definition of a managed service provider, which is not determinative of critical infrastructure status, though they may fall within the IT and critical manufacturing sectors.

In addition to several government documents suggesting data centers are a part of critical infrastructure, a House Homeland Security Committee hearing in April framed data centers

alongside telecommunications infrastructure and space systems, suggesting recognition as independent critical infrastructure.

Practical Steps Amid Uncertainty

As CISA settles on the ultimate scope of CIRCIA coverage, organizations can take practical steps to reduce compliance risk and avoid being caught flat-footed.

First, organizations should consider where they may fit under the proposed rules. Even if the rules are trimmed back, an organization may be able to come to an informed judgment about the likelihood that they will be in scope, based on the language of the statute and the core elements of each sector as described by CISA in the proposed rules.

Second, organizations can inventory existing cyber incident, data security, contractual and government-contractor reporting obligations to identify requirements and areas where processes may need to be harmonized.

Some organizations may need to build a rapid government-reporting program from the ground up, while others may already manage multiple reporting regimes and only need to incorporate CISA-specific reporting into their existing plans and procedures. Public companies may want to consider how new obligations would affect their approaches to materiality determinations under the SEC's cyber disclosure regime.

Federal contractors may think they are ready to handle another 72-hour reporting obligation, but will want to consider how to manage different triggers and information requirements. And organizations may want to consider how they would support mandatory supplemental reports made on an unclear timeline.

Third, companies can get ahead of potential new obligations by identifying who would make key determinations, such as when a company reasonably believes that a covered incident has occurred; who would approve reports to the government; what information could be collected in the first 24 to 72 hours of an incident; and how legal, security, communications and business teams would coordinate.

This may be relatively easy to add to mature cyber incident response plans, but it may require new thinking by organizations that are not as familiar with the life cycle of incident response and reporting.

Fourth, organizations anticipating that they may be covered should consider whether they can meet the data retention obligations that are in — or are similar to — the proposed rules. The proposed rules contemplate significant data preservation obligations that organizations can start to prepare for. Those data preservation obligations differ from existing rules that require preservation of forensic data upon government request, or retention that companies do as a best practice.

Finally, companies can evaluate supply chain and vendor relationships with partners that are clearly in critical infrastructure. CIRCIA-related obligations may emerge in customer flow-downs, managed service provider requirements, incident-notification clauses, software security attestations, audit rights or information-sharing commitments. Mapping vendors, customers and services against critical infrastructure functions can help organizations anticipate where indirect obligations may arise and negotiate contract terms that are operationally realistic.

In short, uncertainty about coverage is not a reason to wait — it is a reason to build a flexible framework that can be adapted as CISA finalizes the rules.

Megan Brown is partner and co-chair of the privacy, cyber and data governance practice at Wiley Rein LLP.

Lyn Brown is a partner at the firm.

Sydney White is special counsel at the firm.

[1] See Communications Sector Coordinating Council, https://comms-scc.org/about/.

[2] See DHS CISA, National Critical Functions, https://www.cisa.gov/national-critical-functions-set.

[3] Enhancing Pipeline Cybersecurity, TSA SD Pipeline-2021-01G (Jan. 9, 2026); Enhancing Rail Cybersecurity, TSA SD 1580-21-01E (Jan. 16, 2026).

[4] 2016 IT Sector Specific Plan, https://www.it-scc.org/uploads/4/7/2/3/47232717/2016_information_technology_sector_specific_plan.pdf.

[5] 89 Fed. Reg. 23644, 23696 (April 4, 2024).