Insights, News & Events

NEW FEDERAL CYBERSECURITY REPORTING RULES ARE ON THEIR WAY: FAQS FOR BUSINESSES ABOUT CIRCIA REGULATIONS

Insights
Apr 7, 2026

New Federal Cybersecurity Reporting Rules are on Their Way: FAQs for Businesses About CIRCIA Regulations

A sweeping new federal cybersecurity mandate is on its way, and now is the time for businesses to build the infrastructure you'll need to comply. The Cybersecurity and Infrastructure Security Agency (CISA) is finalizing draft rules that will require a massive swath of American businesses to report certain cyber incidents, putting more structure and teeth behind the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). While the agency has been targeting May 2026 for the release of the final rule, recent federal appropriations disruptions could alter that timeline. But the core obligations are not expected to change from the draft rule, and businesses that wait for the ink to dry before preparing will be starting from behind. Here's a set of FAQs to help you understand what's about to happen and what you should do.

What is CIRCIA, and why should my business care?

CIRCIA was passed in 2022 as the federal government's first comprehensive, cross-sector approach to mandatory cyber incident reporting. Once the regulations take effect, the law will establish two core reporting obligations for covered entities:

- report significant cyber incidents to CISA **within 72 hours** of reasonably believing one has occurred; and

Related People

Daniel Pepper, CIPP/US
Partner

303.218.3661

Service Focus

Counseling and Advice

Data Protection and Cybersecurity

Privacy and Cyber

Industry Focus

Agriculture

- report ransomware payments **within 24 hours** of making them.

Why does the government want this information?

By collecting timely reports, CISA can deploy resources to assist victims, identify attack trends across sectors, and rapidly warn other potential targets before they fall prey to the same threat actor or technique.

Does CIRCIA apply to my business?

CISA estimates more than 300,000 entities across 16 critical infrastructure sectors will be subject to these requirements. The proposed rule uses a two-track test for coverage, and either track is sufficient to bring you in.

- The first is **size based**. Any entity operating in a critical infrastructure sector that exceeds the Small Business Administration's small business size standards is covered. Those thresholds vary by industry – generally ranging from 100 to 1,500 employees or between $2.25 million and $47 million in annual revenue, depending on the sector. If you clear those thresholds and you're in a covered sector, you're in scope.
- The second track is **sector-based criteria**, which can capture entities regardless of size. Under the proposed rule, 16 specific categories of businesses are covered no matter how small because of the outsized risk their disruption would pose.

What are the 16 business categories that are covered regardless of size?

The 16 critical infrastructure sectors covered are:

- chemical
- commercial facilities
- communications
- critical manufacturing
- dams
- defense industrial base
- emergency services

Healthcare

Manufacturing

Technology Transactions

Transportation and Supply Chain

- energy
- financial services
- food and agriculture
- government facilities
- healthcare and public health
- information technology
- nuclear reactors, materials, and waste
- transportation
- water and wastewater systems

This broad scope captures hospitals and health systems, banks and payment processors, managed service providers, SaaS companies serving enterprise clients in covered sectors, telecom carriers, airlines, utilities, and federal contractors. Many businesses that have never thought of themselves as "critical infrastructure" will find themselves squarely in scope.

What counts as a reportable incident?

The proposed rule defines a "substantial cyber incident" very broadly. Any of the following triggers a reporting obligation:

- Substantial loss of confidentiality, integrity, or availability of your information systems or data
- Serious impact on the safety or resilience of your operational systems and processes
- Disruption of your ability to deliver goods or services
- Unauthorized access caused by a supply chain compromise, including a breach at a vendor, managed service provider, or cloud platform with access to your systems

Has CISA provided examples of attacks that qualify?

Yes, CISA has offered concrete examples of what qualifies: a ransomware attack that encrypts core business systems, a DDoS attack that renders services unavailable for an

extended period, unauthorized access via compromised credentials from an MSP, and exploitation of a vulnerability causing extended system downtime.

When does the 72-hour clock start ticking?

The 72-hour clock starts when you "reasonably believe" a covered incident has occurred, not when your investigation confirms it. That distinction matters enormously for how quickly your internal escalation processes need to move.

What types of reports are required?

The proposed rule establishes four report types:

- **Covered Cyber Incident Report** (due within 72 hours)
- **Ransom Payment Report** (due within 24 hours of payment)
- **Joint Covered Cyber Incident and Ransom Payment Report** if you experience a covered incident and pay a ransom (due within 72 hours)
- **Supplemental Report**, filed whenever significant new or different information emerges after an initial report, or when a correction is needed

How do we submit reports?

Reports are submitted through CISA's web-based reporting form. CISA has indicated it will create a dedicated online portal at cisa.gov for submissions, and the agency may approve alternative submission methods.

What must the report include?

The reports must include a description of affected systems and networks, the nature of the attack, a timeline of the incident, the tactics and techniques used, the impact on operations, and the amount of any ransom payments made and the outcome. CISA acknowledges that initial reports may be incomplete given how early in an investigation the 72-hour deadline falls; supplemental filings are the mechanism for filling in gaps.

Can third parties submit reports for a business?

Yes, a third party like outside counsel, a managed service provider, or a cybersecurity firm can submit reports on your

behalf. But legal responsibility stays with you. If the report is wrong, incomplete, or late, the covered entity bears the consequences.

What records must be preserved?

Covered entities must preserve incident-related records (system and network logs, indicators of compromise, forensic artifacts, records related to ransom payments, etc.) for two years from the date the report was submitted or required.

What happens if we don't comply?

If CISA learns of a potential covered incident (through a press release, a law enforcement referral, or any other source) and has not received a report, it can issue a Request for Information requiring a response within 72 hours. A non-response or inadequate response can escalate to a subpoena compelling disclosure.

Information provided in response to a subpoena can be shared with the Department of Justice and other regulatory agencies for civil or criminal enforcement. That referral pathway cannot be appealed. And if false or fraudulent statements appear anywhere in a CIRCIA report or response, the exposure includes up to five years of imprisonment, and up to eight years if the offense involves terrorism.

Are there other consequences for federal contractors?

For federal contractors, the consequences extend further. CISA can refer noncompliance to the DHS Suspension and Debarment Official, putting a company's ability to do business with the federal government at risk.

How does CIRCIA interact with other reporting obligations we already have?

Many covered entities already operate under a patchwork of cyber reporting requirements, like HIPAA breach notification for healthcare organizations, SEC cyber disclosure rules for public companies, state breach notification statutes, or DFARS and CMMC obligations for defense contractors. CIRCIA doesn't displace those obligations. It adds to them.

The proposed rule includes a "substantially similar" exemption that could allow a CIRCIA report to be satisfied if the entity already reported to another federal agency under

a separate law. But this only applies if CISA has a formal agreement in place with that agency establishing the equivalence. Those agreements are still being worked out, and the exemption is narrow.

Critically, state reporting requirements will not satisfy CIRCIA. Dual reporting – to both CISA and state regulators – will be required in most situations.

What is the timing and expectation for the rule to be finalized?

CISA was originally required to finalize the CIRCIA regulations by October 2025. The agency pushed that deadline to May 2026, citing the volume of public comments received and the need to streamline requirements and harmonize CIRCIA with other federal cyber reporting frameworks.

To gather additional stakeholder input before finalizing the rule, CISA had announced a series of virtual town hall meetings for early 2026, organized by sector. Those sessions were disrupted when a federal government appropriations lapse forced their postponement.

CISA has indicated it will reschedule once funding is restored, but the delay makes a further extension past May 2026 increasingly likely. Regardless of the precise publication date, the core reporting obligations (72-hour incident reporting and 24-hour ransomware payment reporting) are not expected to change.

What should we be doing right now to prepare?

Businesses that treat the remaining runway as preparation time will be in a fundamentally better position than those waiting for official publication. Here's where to focus:

- **Determine your coverage status and document it.** Don't assume you're out of scope. Conduct a deliberate analysis against both the size-based and sector-based criteria. Memorialize your conclusion in writing. If regulators later question whether you engaged the issue in good faith, that documentation matters.
- **Assign ownership before an incident occurs.** The 72-hour clock starts the moment someone in your organization reasonably believes a covered incident has occurred. Designate a cross-functional response team

(legal, IT/security, communications, and senior leadership) and define in advance who has authority to make the call to file.

- **Audit and update your incident response plan.** Most existing plans were not built with CIRCIA's timelines in mind. Map the 72-hour and 24-hour reporting windows explicitly into your escalation workflows. Then pressure-test them. Can your team detect, assess, and report within the window? Where are the gaps?
- **Invest in detection and monitoring.** You cannot report what you cannot see. CIRCIA's deadlines require real-time visibility into your systems and networks. Organizations without 24/7 monitoring capability will struggle to meet the "reasonable belief" trigger and execute reporting in time.
- **Map your supply chain exposure.** A breach at one of your vendors, MSPs, or cloud providers that results in unauthorized access to your systems is a covered incident under CIRCIA. Review third-party contracts for notification obligations that flow to you, and know which external parties have access to your systems and data.
- **Build your data retention practices now.** Two years of incident-related records (logs, forensic artifacts, indicators of compromise, etc.) is a significant retention obligation. Assess whether your current systems and policies can support it and make adjustments before an incident puts the requirement in play.
- **Coordinate your reporting obligations.** If you're already subject to HIPAA, SEC disclosure rules, state breach laws, or federal contractor requirements, build a unified reporting workflow that accounts for all of them.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney on our Data Protection and Cybersecurity Team.