Insights, News & Events

SILICON VALLEY SNAPSHOT ON LOOMING CYBERSECURITY REPORTING RULES: TOP CIRCIA TAKEAWAYS FOR THE TECH INDUSTRY

Insights
May 12, 2026

Silicon Valley Snapshot on Looming Cybersecurity Reporting Rules: Top CIRCIA Takeaways for the Tech Industry

Many tech companies will soon need to comply with new cybersecurity reporting obligations as federal officials close in on finalizing a proposed rule that will carry out core goals of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). These sweeping new requirements will create a significant compliance burden for Silicon Valley businesses and across the information technology sector. This snapshot will provide a quick recap of what this is all about and offer five key takeaways for your industry.

Quick Background

CIRCIA was enacted in 2022 as the federal government's first comprehensive, cross-sector approach to mandatory cyber incident reporting. As required by the law, the Cybersecurity and Infrastructure Security Agency (CISA) issued a proposed rule in 2024 to implement covered cyber incident and ransom payment reporting requirements for covered entities.

While CISA had aimed to finalize the rule by May 2026, lapses in federal appropriations forced the agency to postpone a CIRCIA town hall meeting series, and the agency will issue a final rule only after these town hall meetings take place.

Related People

Brandon Kahoush
Partner

415.490.9034

Brett P. Owens
Partner

813.769.7512

Overview of CIRCIA Reporting Requirements

Once the CIRCIA regulation is finalized, covered entities will be required to report substantial cyber incidents, ransomware payments, and supplemental information to CISA and comply with record preservation obligations. All CIRCIA reports will need to meet strict rules regarding timing, content, manner, and format. CISA will have a variety of powerful mechanisms to enforce this new cyber reporting framework – which will largely operate in addition to any other state or federal reporting obligations applicable to your business.

> For more details about the new federal cybersecurity reporting rules on their way, check out our **FAQs for Businesses About CIRCIA Regulations**.

Top 5 Takeaways for Silicon Valley and the Tech Industry

1. Information Technology Treated as a Critical Infrastructure Sector

The proposed CIRCIA rule applies to any entity in a **critical infrastructure sector** that meets certain size-based or sector-based criteria (as discussed further below). Information technology is one of the 16 critical infrastructures explicitly listed, and the rule's definition of "covered entity" is so broad that "companies that do not actually constitute critical infrastructure may be swept into the reporting requirement," according to a public comment submitted by the Information Technology Industry Council (ITI) in 2024.

The ITI urged CISA to, among other things, narrow the scope of covered entities "based on a criticality assessment that is tied to economic or national security" and to limit coverage to only a company's offerings that constitute critical infrastructure.

2. Even Smaller Tech Businesses and Startups May Be Covered

If your business is in a critical infrastructure sector (such as IT), it is a covered entity under the proposed rule so long as it exceeds the small business threshold **or** meets certain sector-based criteria. Many major technology companies

Service Focus

Data Protection and Cybersecurity

Industry Focus

Tech

Related Offices

Silicon Valley

will likely satisfy both coverage tests – but meeting just one of them is enough to be covered.

Size-Based Criteria

Your business will be a covered entity if it exceeds the **small business size standard** applicable to your industry as designated by the North American Industry Classification System (NAICS). These thresholds can be based on number of employees or annual revenue, depending on the industry.

Size-Based Criteria Examples:

- A **cloud infrastructure provider** categorized under NAICS Code 518210 would meet the size-based criteria if it had annual revenue exceeding **$40 million**.
- A **software development firm** categorized under NAICS Code 541511 would meet the size-based criteria if it had annual revenue exceeding **$34 million**.
- An **AI developer categorized** under NAICS Code 541715 would meet the sized-based criteria if it had more than **1,000 employees**.

Each example assumes that the entity is considered to be in a critical infrastructure sector. However, the proposed rule only explicitly mentions broad sectors, not specific entity types, and companies should work with counsel to determine if they will be covered.

Size-Based Criteria

Your business will be a covered entity if it exceeds the **small business size standard** applicable to your industry as designated by the North American Industry Classification System (NAICS). These thresholds can be based on number of employees or annual revenue, depending on the industry.

IT Sector-Based Criteria Example. Any entity (regardless of size or sector, so long as it is in a critical infrastructure sector) will meet the IT sector-based criteria if one or more of the following applies:

- The entity knowingly provides or supports information technology hardware, software, systems, or services to the Federal government.

- The entity has developed and continues to sell, license, or maintain any software that has, or has direct software dependencies upon, one or more components that:
  - is designed to run with elevated privilege or manage privileges;
  - has direct or privileged access to networking or computing resources;
  - is designed to control access to data or operational technology;
  - performs a function critical to trust; **or**
  - operates outside of normal trust boundaries with privileged access.
- The entity is an original equipment manufacturer, vendor, or integrator of operational technology hardware or software components.
- The entity performs functions related to domain name operations.

Remember, the sector-based test can be met if any criterion for any sector applies.

3. Reportable Cyber Incidents Are Defined Broadly

The proposed rule requires covered entities to report cyber incidents that lead to **any** of the following:

- substantial loss of confidentiality, integrity, or availability of your information systems or networks;
- a serious impact on the safety and resiliency of your operational systems and processes;
- a disruption of your ability to engage in business or industrial operations, or deliver goods and services; **or**
- unauthorized access to your information system or network (or any nonpublic information contained in it) caused by either (1) a compromise of a cloud service provider, managed service provider, or other third-party hosting provider, or (2) a cyber incident within the supply

chain of an information system that an adversary "can" or does leverage for specific purposes.

In the ITI's 2024 public comment, it expressed several concerns over the breadth of cyber incidents that could trigger reporting obligations under the proposed rule, as well as confusion over "where in the supply chain reporting responsibilities fall." For example, ITI said that the last bullet point above "seems to indicate that unauthorized access *without actual disruption* anywhere in the supply chain" would be a reportable cyber incident.

4. The Reporting Timelines Are Very Aggressive

Once the regulations take effect, covered entities will be required to submit CIRCIA reports to CISA for:

- covered cyber incidents **within 72 hours** of reasonably believing one has occurred; and
- ransomware payments **within 24 hours** of making them (even if the ransomware attack underlying the ransom payment is not a covered cyber incident).

Note that the reporting clock starts before an investigation is complete, requiring companies to report to the federal government while investigations are still unfolding. And companies will be required to continue filing supplemental reports each time significant new or different information emerges from an initial report, or when a correction is needed, until the company "notifies CISA that the covered cyber incident at issue has concluded and has been fully mitigated and resolved."

5. Don't Wait for the Rule to Be Finalized to Start Preparing

Even if finalization of the proposed CIRCIA rule appears to be stuck in a holding pattern due to recent federal appropriations disruptions, businesses that wait for the ink to dry before preparing will be behind. Check out our **FAQs for Businesses About CIRCIA Regulations** for more details about the rule and specific steps you should consider taking now to put your business in a strong position by the time the rule kicks in.

You should also look out for CISA to release new dates for the town hall series (including one focused on the Defense Industrial Base Sector and the Information Technology Sector), as the purpose of these meetings is to allow the

agency to solicit input from stakeholders on "refining the scope and burden" of the proposed CIRCIA rule. Consider reaching out to the FP Advocacy team to help develop best strategies for having your voice heard on this subject.

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 authors of this Insight, or any attorney in our Silicon Valley office or on our Tech Industry Team or Data Protection and Cybersecurity Team.