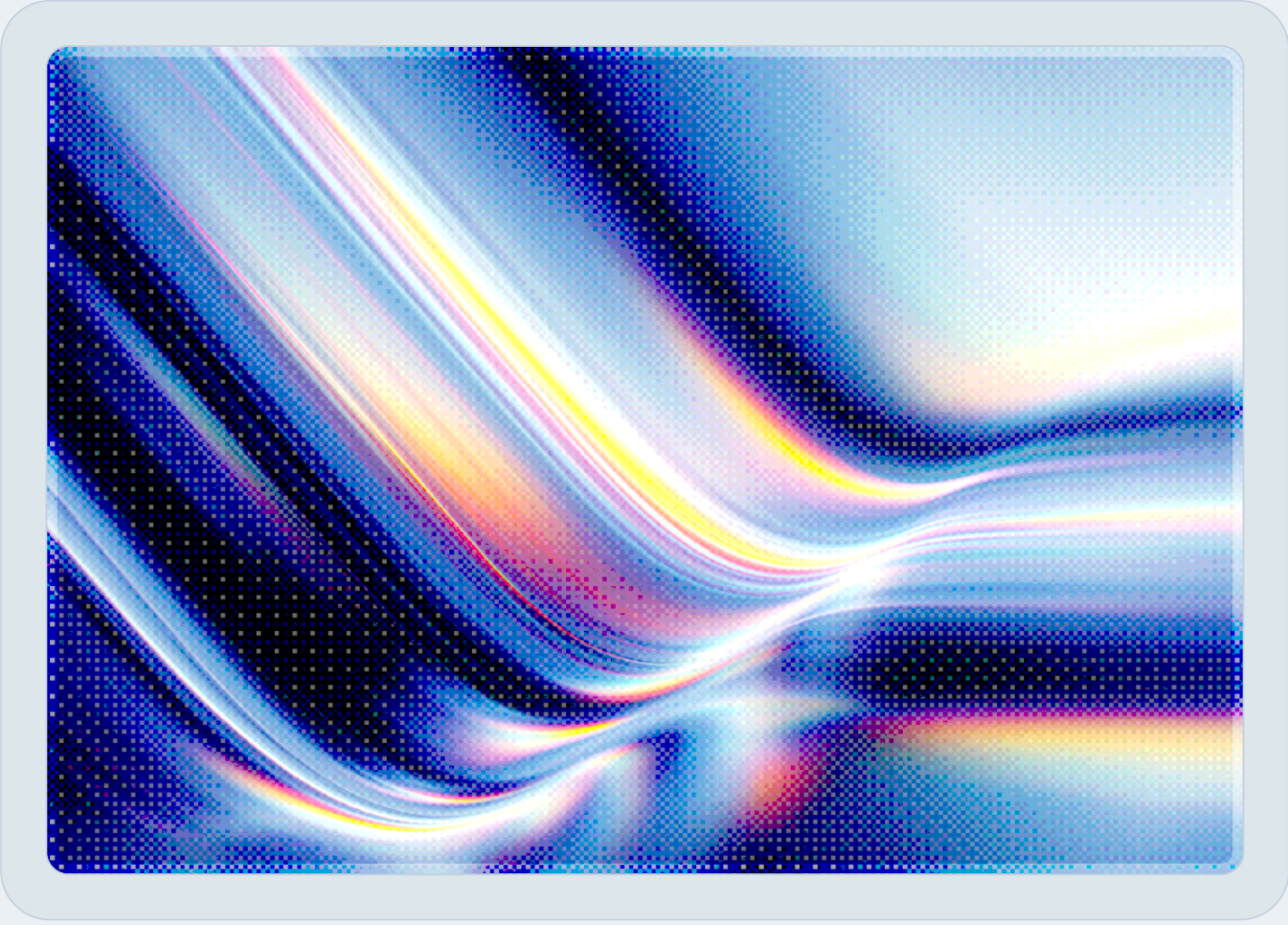
CSAI Foundation | Cloud Security Alliance

CIRCIA June 18: Last Call for Cloud and AI Providers

What IT-Sector Organizations Must Do Before the Final Rule Takes Shape

2026-06-04

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

Key Takeaways

- **June 18, 2026 is the last scheduled formal input opportunity in the current town hall series.** CISA's final CIRCIA town hall — dedicated to the Information Technology sector — takes place June 18. After this date, the agency will finalize the rule without further scheduled stakeholder engagement. Registration must be completed by June 16 at 5:00 PM ET.
- **Cloud and AI providers are likely covered entities.** The proposed IT sector criteria capture cloud infrastructure providers with more than $40 million in annual revenue, federal government IT contractors regardless of size, and developers of software that runs with elevated privileges, manages access controls, or controls access to data or operational technology. Many AI platform and model-hosting companies will qualify on one or more grounds.
- **Third-party breach liability extends further than the direct attack surface under the NPRM's proposed definitions.** Under the NPRM, a compromise of a cloud service provider, managed service provider, or third-party data hosting provider that enables unauthorized access to a customer's environment constitutes a covered cyber incident for that downstream customer — not merely for the breached vendor.
- **Core obligations are 72 hours and 24 hours.** Covered entities must report substantial cyber incidents to CISA within 72 hours of reasonably believing an incident occurred, and ransomware payments within 24 hours of making them. The 72-hour and 24-hour timelines were proposed in the NPRM and are widely expected to carry forward into the final rule, though the agency retains authority to modify them.
- **Multiple reporting frameworks remain in force simultaneously.** CIRCIA does not preempt SEC cybersecurity disclosure rules, HIPAA breach notification obligations, or state breach statutes. Cloud and AI providers subject to several of these regimes face compounding notification timelines during active incidents.

Background

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) directs the Cybersecurity and Infrastructure Security Agency to create mandatory incident reporting requirements for the nation's critical infrastructure. Congress enacted the law in response to a series of high-profile incidents — including the SolarWinds supply chain compromise and the Colonial Pipeline ransomware attack — that exposed the federal government's limited visibility into private-sector cyber events with systemic implications [1].

CISA published its Notice of Proposed Rulemaking in the Federal Register on April 4, 2024, proposing a framework that would require covered entities across 16 critical infrastructure sectors to report substantial cyber incidents within 72 hours and ransomware payments within 24 hours [2]. The NPRM attracted significant industry attention for the breadth of its proposed scope — CISA estimated approximately 316,000 entities would be covered [2] — and for unresolved questions about how to harmonize CIRCIA with the extensive landscape of overlapping federal and state reporting mandates [3].

The original deadline for a final rule was October 2025. The volume of public comments and the technical complexity of harmonizing requirements across sectors led CISA to push that target to May 2026 [4]. A subsequent lapse in Department of Homeland Security appropriations disrupted the town halls originally scheduled for March and April 2026, forcing further delays. On May 26, 2026, CISA announced a revised schedule of four virtual town halls to be held June 15 through June 18 [5][9]. These sessions represent the last scheduled structured engagement before the rule is finalized, though CISA may continue to accept written materials after the meetings.

The June 18 session is dedicated to Critical Infrastructure Sectors Grouping B, which includes the Information Technology sector alongside the Chemical, Commercial Facilities, Critical Manufacturing, Defense Industrial Base, Energy, Financial Services, and Nuclear sectors [5]. For cloud and AI providers, this is the directly relevant session.

Security Analysis

How the IT Sector Criteria Reach Cloud and AI Providers

The NPRM proposes two independent pathways to covered entity status [2]. Under the size-based pathway, an entity qualifies if it exceeds the Small Business Administration's small business threshold for its NAICS code. For cloud infrastructure providers classified under NAICS code 518210, that threshold is

annual revenue exceeding $40 million [11]. Software development firms under NAICS code 541511 qualify if revenue exceeds $34 million. Many cloud hyperscalers, AI platform providers, and infrastructure-as-a-service vendors will clear these thresholds comfortably.

The sector-based criteria are more expansive, covering entities regardless of size if they knowingly provide or support information technology hardware, software, systems, or services to the federal government [6]. This provision covers federal cloud contractors, government-facing AI API providers, and managed security service providers that hold any federal contract, without any revenue floor.

A third criterion within the sector-based pathway catches developers and vendors of software that runs with elevated privileges, manages system privileges, has direct or privileged access to networking or computing resources, or controls access to data or operational technology [6]. This criterion is notable for AI providers because model inference endpoints running with privileged operating system access, AI orchestration platforms that provision compute resources, and agentic AI systems that manipulate file systems or network configurations can all be read to fall within this language. The final rule may refine these definitions, and the June 18 town hall is specifically the venue for IT sector stakeholders to weigh in on whether current language creates overbroad or underspecified coverage.

What Constitutes a Reportable Incident

The NPRM defines a "covered cyber incident" as a substantial cyber incident that satisfies at least one of several threshold conditions [2]. These include substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network; serious impact on the safety and resilience of operational systems and processes; disruption of the entity's ability to engage in business operations or deliver goods and services; and unauthorized access to a covered entity's system or nonpublic information facilitated by a supply chain compromise.

The availability threshold is especially consequential for cloud and AI providers. The NPRM's language on what constitutes "substantial" loss of availability has been contested throughout the comment period: outages affecting more than a de minimis number of users for more than a de minimis period may qualify [2]. For providers operating services at large scale, even brief platform-wide incidents could trigger the 72-hour clock. The town halls are an opportunity for IT sector participants to propose clearer numerical or durational thresholds that distinguish operational incidents from security events requiring federal reporting.

Third-Party and Supply Chain Implications

One of the most operationally significant provisions in the NPRM addresses supply chain compromise. Under the proposed definition, unauthorized access to a covered entity's environment that is facilitated through or caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider is itself a covered cyber incident — from the perspective of the downstream customer entity [2]. This creates an indirect reporting obligation: a covered entity's customer may be required to report to CISA an incident in which the customer's own systems were never directly attacked, but were accessed as a result of a breach at the provider.

The practical implication for cloud and AI providers runs in both directions. First, as potential triggering parties, providers whose own compromises flow downstream to customers may see a cascade of CIRCIA reports naming their infrastructure as the vector — even if the provider itself does not qualify as a covered entity or has a separate reporting obligation of its own. Second, providers that are themselves customers of infrastructure services — a common model for AI companies relying on public cloud hyperscalers — face the same third-party trigger for their own CIRCIA obligations when upstream services are breached.

This creates direct compliance incentives for cloud and AI companies to map their dependencies in both directions: which customers rely on their infrastructure in ways that could trigger those customers' reporting clocks, and which upstream infrastructure providers could trigger the company's own obligations.

AI Systems and the Emerging Definition Question

The NPRM does not address artificial intelligence systems or AI infrastructure explicitly as a distinct category [2]. Industry analysis published during the comment period identified this silence as a significant gap in the framework's coverage of emerging technology risks [7]. This gap has become increasingly visible as AI deployment within critical infrastructure has grown since the NPRM's April 2024 publication. AI inference APIs, model deployment platforms, and agentic AI orchestration systems appear to be significantly more embedded in financial services, healthcare, and energy operations than they were when the comment period opened — a development not yet reflected in CIRCIA's proposed definitions.

The question of whether a disruption to an AI service — a model serving errors due to a poisoned update, an inference API made unavailable by a DDoS attack, or unauthorized access to proprietary training data — constitutes a "substantial cyber incident" under CIRCIA's definitions remains open. The June 18 town

hall represents an important opportunity for the AI industry to raise these questions directly with CISA, and to propose definitional language or sector-specific guidance that would give AI providers clear, workable reporting standards rather than requiring case-by-case analysis of ambiguous thresholds.

Regulatory Harmonization: The Unresolved Complexity

CIRCIA explicitly does not preempt existing cyber reporting requirements under other federal laws, and the current regulatory environment for cloud and AI providers includes several overlapping regimes [8]. Publicly traded technology companies must comply with SEC cybersecurity disclosure rules that require material incident disclosure within four business days [12]. Healthcare cloud providers face HIPAA breach notification obligations with their own scope definitions and timelines [13]. Defense contractors operate under DFARS reporting requirements. State breach notification laws in all 50 states impose their own triggers and deadlines.

The concern raised consistently during the NPRM comment period is that simultaneous compliance with multiple reporting frameworks creates operational confusion during active incidents, when security teams are managing response, communications, and evidence preservation concurrently [8]. CISA has acknowledged this concern and stated its intent to pursue harmonization, but the agency has also made clear that it does not expect other regulators to subordinate their requirements to CIRCIA [2]. The final rule may incorporate mechanisms for using CIRCIA reports to satisfy parallel obligations — a form of "report once, satisfy multiple" — but the June 2026 town halls are the last scheduled point in the rulemaking at which industry participants can advocate for specific harmonization mechanisms before the rule is finalized.

Recommendations

Immediate Actions (Before June 18)

Cloud and AI organizations that have not yet engaged the CIRCIA process should take several concrete steps before the June 18 town hall. First, determine whether the organization qualifies as a covered entity under the NPRM's size-based or sector-based IT criteria. This is not a purely mechanical exercise: the elevated-privilege software criterion in particular requires analysis of whether the organization's products meet the statutory definition, and the answer may differ across product lines. Legal counsel with regulatory expertise should lead this assessment.

Second, register for the June 18 town hall. Registration closes at 5:00 PM Eastern Time on June 16 and is available at cisa.gov/circia [5]. Organizations that want CISA to consider specific data or written materials in connection with the session must submit those materials within seven calendar days after the meeting [5]. If you have quantitative data on the operational burden of 72-hour reporting windows, on the ambiguity of the availability threshold for cloud services, or on the complexity of AI-specific incident classification, this is the moment to surface it with specificity.

Third, identify whether your organization has contractual upstream or downstream relationships that could trigger third-party reporting obligations — either for you as a customer of a cloud provider, or for customers that rely on your infrastructure. These dependency maps are necessary inputs both for the June 18 engagement and for the compliance program you will need to build regardless of what the final rule says.

Short-Term Mitigations (Next 90 Days)

As CISA moves toward finalizing the rule, organizations in the IT sector should begin standing up the internal capabilities that CIRCIA will require. At a minimum, this means establishing an incident classification process that can evaluate events against CIRCIA's substantial incident definition within the 72-hour window, designating a regulatory reporting function with clear escalation paths from the security operations center, and preserving evidence collection workflows that allow accurate post-incident reporting.

Organizations should also map their existing reporting obligations — SEC Form 8-K timelines, HIPAA breach notification procedures, state law triggers — against the proposed CIRCIA timeline to identify conflicts and gaps. The 72-hour CIRCIA clock and the SEC's four-business-day clock for material incidents are close enough to overlap in some scenarios, but not identical in their scoping; the same incident may qualify under one framework and not the other, or may require different content in each report. Documenting these differences now, before an incident occurs, substantially reduces decision latency during a crisis.

Strategic Considerations

Beyond compliance mechanics, CIRCIA creates a strategic opportunity for cloud and AI providers that engage proactively. CISA has stated its intent to use CIRCIA reports to build a national threat intelligence picture [1]; the agency has also described potential information-sharing benefits for covered entities, including threat context and mitigation guidance, though the specific scope of such benefits

remains subject to final rulemaking [2]. Providers that invest in reporting capabilities and develop relationships with CISA before the rule takes effect are better positioned to benefit from that intelligence-sharing dynamic.

Cloud and AI providers should also consider the industry-level advocacy dimension of the June 18 town hall. The outcome of that session will likely influence which IT sector issues receive attention in the final rule. Organizations with specific concerns about AI incident definitions, about the scope of the elevated-privilege software criterion, or about the feasibility of 72-hour reporting for multi-tenant cloud incidents should make those arguments publicly and on the record — both through direct town hall participation and through industry associations that can aggregate comments from multiple stakeholders.

CSA Resource Alignment

The Cloud Security Alliance's Cloud Incident Response Framework [10] provides a structured methodology for cloud security customers to build response capabilities aligned with CIRCIA's reporting requirements. The framework's emphasis on shared responsibility between cloud service providers and cloud service customers maps directly onto CIRCIA's third-party trigger provisions: the question of who bears the reporting obligation when a CSP compromise enables a downstream breach requires clear contractual and operational agreements of precisely the type the CIR Framework is designed to support.

CSA's Cloud Controls Matrix (CCM) and the AI Controls Matrix (AICM) provide control families relevant to incident detection, containment, and evidence preservation — the internal capabilities that feed any 72-hour external reporting process. CCM's Incident Management and Audit Assurance domains, combined with AICM controls addressing AI system integrity and access governance, constitute a practical starting point for the compliance program CIRCIA will require. Organizations that have already adopted CCM-aligned controls can leverage existing control attestation documentation as evidence of their security posture in CIRCIA reports.

The MAESTRO agentic AI threat model is also directly applicable to the open AI definitional questions in CIRCIA. MAESTRO's threat layer taxonomy — particularly its treatment of model inference infrastructure, orchestration platforms, and agentic system access controls — provides a vocabulary for articulating how AI system compromises differ from conventional IT incidents. Using MAESTRO as a reference in June 18 written comments, or in advocacy for AI-specific incident definitions in the final rule, would help ground the discussion in an established industry framework. Organizations may supplement CSA's MAESTRO vocabulary with NIST AI RMF and MITRE ATLAS terminology when engaging CISA, as the agency's own guidance references multiple frameworks.

References

[1] CISA. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)." CISA, 2022.

[2] Federal Register. "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements." Federal Register, April 4, 2024.

[3] Morrison Foerster. "CISA's Very Broad Proposed Rule for 'Critical Infrastructure' Entities to Report Cyber Incidents." Morrison Foerster, April 2024.

[4] Davis Wright Tremaine. "CISA Delays Cyber Incident Reporting Rules Until May 2026." DWT Privacy & Security Law Blog, September 2025.

[5] Federal Register. "Town Hall Meetings To Provide Input on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Rulemaking." Federal Register, May 26, 2026.

[6] Fisher Phillips LLP. "Silicon Valley Snapshot on Looming Cybersecurity Reporting Rules: Top CIRCIA Takeaways for the Tech Industry." Fisher Phillips, 2024.

[7] IBM. "CIRCIA Feedback Update: Critical Infrastructure Providers Weigh In on NPRM." IBM Think, 2024.

[8] Byte Back Law. "Navigating Cyber Disclosures in 2026: A Limited Renewal of CISA 2015, and 'Take Two' on Finalizing CIRCIA's Reporting Regulations." Byte Back Law Blog, February 2026.

[9] CISA. "CISA Announces Revised Town Hall Schedule to Engage with Stakeholders on Cyber Incident Reporting for Critical Infrastructure." CISA News, May 2026.

[10] Cloud Security Alliance. "Cloud Incident Response Framework." CSA, 2021.

[11] CISA. "Covered Entity Fact Sheet." CISA, 2024.

[12] Securities and Exchange Commission. "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." SEC Final Rule, Release No. 33-11216, effective December 18, 2023.

[13] U.S. Department of Health and Human Services. "HIPAA Breach Notification Rule." 45 CFR §§ 164.400–414, HHS.

