INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 14:17 UTC

Proposed US Legislation Would Mandate CISA to Update Critical Infrastructure Cybersecurity Plans for AI and Emerging Threats

GOVERNANCE | MEDIUM

SCC Item ID	SCC-GOV-2026-0054
Type	Governance
Severity	MEDIUM
Affected Products	CISA, all 16 US critical infrastructure sectors (as defined under Presidential Policy Directive 21)
Published	2026-06-12
Discovery Source	Gemini

Executive Summary

A U.S. Senator has introduced the Combat Emerging Threats to Critical Infrastructure Act of 2026, which would require CISA to update sector-specific cybersecurity plans across all 16 critical infrastructure sectors to address AI-enhanced attacks, deepfake social engineering, AI supply chain risks, and quantum-enabled cryptographic threats. Organizations operating within or supplying to critical infrastructure sectors face potential new compliance obligations if the legislation passes. The bill signals that regulators view current protection frameworks as outdated relative to the AI-era threat landscape, and organizations are advised to begin gap assessments now, as waiting for final rulemaking typically compresses compliance timelines.

Technical Analysis

This item is a legislative development, not a technical vulnerability. No CVE, CWE, or CVSS score applies. The bill targets four threat categories: (1) AI-enhanced cyberattacks, where adversaries use machine learning to accelerate reconnaissance, evasion, and exploitation; (2) AI supply chain vulnerabilities, where malicious or compromised AI models and training pipelines introduce risk into critical systems; (3) deepfake-based social engineering, where synthetic audio and video are used to deceive operators and administrators; and (4) quantum-enabled cryptographic attacks, which threaten RSA and ECC-based encryption as quantum computing matures. The legislative mechanism would require CISA to formally revise sector-specific cybersecurity plans under the critical infrastructure framework established by Presidential Policy Directive 21. Confirm bill status and text via congress.gov before integrating this item into compliance planning, as official legislative sources are

authoritative and may have updates not reflected here.

Action Checklist

1. Step 1: Awareness. Assign a GRC or policy owner to monitor this bill's progress through Congress. Check congress.gov for the current status of the Combat Emerging Threats to Critical Infrastructure Act of 2026 and set an alert for committee markups or floor votes.
2. Step 2: Gap Assessment. Map your current critical infrastructure cybersecurity plans against the four threat categories named in the bill (AI-enhanced attacks, AI supply chain, deepfake social engineering, quantum cryptography). Identify where existing plans reference pre-AI threat models. Review NIST SI-5 (Security Alerts, Advisories, and Directives) to ensure your organization has a defined process for receiving and evaluating emerging legislative and regulatory changes.
3. Step 3: Framework Alignment. Review your sector-specific plans against CISA's current Critical Infrastructure Security and Resilience guidance (cisa.gov/topics/critical-infrastructure-security-and-resilience). Identify controls that address AI-era threats and document gaps. CIS 7.1 (Establish and Maintain a Vulnerability Management Process) provides a baseline process for incorporating emerging threat categories into ongoing risk management.
4. Step 4: Cryptographic Inventory. Begin or accelerate a cryptographic asset inventory to identify RSA and ECC dependencies that would be vulnerable to quantum-enabled attacks. NIST SC-12 (Cryptographic Key Establishment and Management) and SC-13 (Cryptographic Protection) are the relevant controls for managing cryptographic assets and planning post-quantum migration. Cross-reference NIST's post-quantum cryptography standards (FIPS 203, 204, 205) for migration planning.
5. Step 5: Post-Legislation Readiness. When the bill passes or CISA initiates rulemaking, your documented gap assessment becomes the baseline for your compliance response. Capture lessons from this planning cycle: which threat categories had no mapped controls, which sector plans were last updated before 2022, and which third-party suppliers have no AI or quantum risk posture documented.

IR / Forensic Enrichment

Triage Priority	DEFERRED
Escalation Criteria	Escalate from deferred to standard if the bill advances out of committee or CISA publishes an advance notice of proposed rulemaking (ANPRM), or immediately if your organization is subject to an existing CISA binding operational directive or sector-specific regulatory framework (e.g., NERC CIP, TSA Security Directives, NRC cybersecurity rules) that CISA could amend under the new authority — those sectors face compounded compliance timelines.
Recovery Notes	There is no system recovery action associated with this governance threat; the post-legislation readiness posture is the operative endpoint. Once the bill passes or rulemaking begins, validate that gap assessment artifacts from this cycle are version-controlled and accessible to the compliance response team, that cryptographic inventory outputs are current within the prior 90 days, and that third-party supplier AI and quantum risk questionnaires have been distributed. Monitor the CISA Federal Register docket and cisa.gov/critical-infrastructure-security-and-resilience for sector plan update publications on at minimum a 30-day review cycle throughout the rulemaking comment period.

Forensic Artifacts	Congressional record snapshot: dated export from congress.gov capturing the bill's full text, committee referral, co-sponsor list, and last action — establishes the regulatory signal timeline for audit purposes | Sector plan version history: version-controlled copies of all organization-held critical infrastructure cybersecurity plans with original creation and last-modified metadata, documenting which plans predate AI-era threat models (pre-January 2023 NIST AI RMF publication) | Cryptographic asset inventory: enumeration of all deployed RSA and ECC certificates and keys with associated service bindings, key sizes, and expiration dates — baseline evidence required to demonstrate quantum migration readiness under anticipated CISA sector plan updates | Supplier AI and quantum risk posture records: third-party vendor risk assessment responses or attestation letters specifically addressing AI-enhanced attack exposure and post-quantum cryptography migration status, timestamped at collection to show pre-legislation baseline state | Gap assessment artifact with SHA-256 integrity hashes: the completed threat-category-to-control mapping document from Step 2, hashed and stored with the hash record in a separate location, providing tamper-evident evidence of what control gaps existed before any rulemaking obligation attached

Per-Action IR Details

Step 1: Awareness — Assign a GRC or policy owner to monitor this bill's progress through Congress. Check congress.gov for the current status of the Combat Emerging Threats to Critical Infrastructure Act of 2026 and set an alert for committee markups or floor votes.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing the organizational capability and awareness structures needed to respond to regulatory change before it becomes a compliance obligation

Controls: NIST IR-1 (Policy And Procedures), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, And Directives)

Compensating: A 2-person GRC team can implement cost-free congressional monitoring using congress.gov RSS feeds for the bill's specific page, combined with a free Google Alert on 'Combat Emerging Threats to Critical Infrastructure Act' to catch committee markup announcements, floor scheduling notices, and press coverage without any tooling budget.

Evidence: This step does not alter live system state; no volatile capture is required. Document the bill's current committee assignment, co-sponsor list, and last action date from congress.gov as the baseline record — this timestamped snapshot becomes audit evidence that the organization tracked the legislation from its earliest observable stage.

Step 2: Gap Assessment — Map your current critical infrastructure cybersecurity plans against the four threat categories named in the bill (AI-enhanced attacks, AI supply chain, deepfake social engineering, quantum cryptography). Identify where existing plans reference pre-AI threat models. Reference NIST SI-5 (Security Alerts, Advisories, and Directives) to ensure your process captures emerging legislative and regulatory signals.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: assessing the current state of plans and controls against known and emerging threat categories so that gaps are identified before a compliance deadline or a real-world AI-enhanced or quantum-enabled incident forces reactive triage

Controls: NIST SI-5 (Security Alerts, Advisories, And Directives), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: A 2-person team can conduct this gap assessment using a structured spreadsheet mapping each of the bill's four threat categories (AI-enhanced attacks, AI supply chain risks, deepfake social engineering, quantum cryptography) against existing sector plan controls, with a simple date-of-last-update column to flag plans predating

NIST AI RMF (January 2023) or NIST's post-quantum standards timeline as definitively pre-AI-era documents requiring revision.

Evidence: This step involves document review only and does not alter live system state; no volatile capture is required. Preserve version-controlled copies of all current sector-specific cybersecurity plans with their original metadata intact before any gap-assessment annotations are made, so the pre-assessment baseline remains available as an audit artifact.

Step 3: Framework Alignment — Review your sector-specific plans against CISA's current Critical Infrastructure Security and Resilience guidance (cisa.gov/topics/critical-infrastructure-security-and-resilience). Identify controls that address AI-era threats and document gaps. CIS 7.1 (Establish and Maintain a Vulnerability Management Process) provides a baseline process for incorporating emerging threat categories into ongoing risk management.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: aligning organizational plans to authoritative sector guidance so that when CISA initiates rulemaking under the proposed Act, the organization's control framework is already anchored to the agency's own published standards rather than constructed reactively

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: A 2-person team can perform this alignment using CISA's freely published National Infrastructure Protection Plan (NIPP) sector-specific plans and the CISA Cross-Sector Cybersecurity Performance Goals (CPGs) as a checklist, annotating each CPG objective with a pass/fail/partial status and a note on whether the control explicitly addresses AI-enhanced threats, deepfake vectors, AI supply chain risk, or quantum-vulnerable cryptography.

Evidence: This step involves document review and does not alter live system state; no volatile capture is required. Archive a dated, read-only copy of the CISA guidance pages and sector plans reviewed (including page metadata or PDF download timestamps) to establish that the alignment assessment was performed against the versions of guidance current as of the review date, which is material if CISA updates those pages during rulemaking.

Step 4: Cryptographic Inventory — Begin or accelerate a cryptographic asset inventory to identify RSA and ECC dependencies that would be vulnerable to quantum-enabled attacks. NIST SI-7 (Software, Firmware, and Information Integrity) supports integrity verification practices that would need updating under post-quantum migration. Cross-reference NIST's post-quantum cryptography standards (FIPS 203, 204, 205) for migration planning.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: proactively inventorying cryptographic dependencies so that when CISA's updated sector plans mandate post-quantum migration timelines under the proposed Act, the organization has an actionable asset map rather than needing to build one under a compliance deadline

Controls: NIST SI-7 (Software, Firmware, And Information Integrity), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: A 2-person team can conduct a cryptographic inventory using free tools: run OpenSSL's `openssl s_client` and `openssl x509` commands against exposed endpoints to enumerate certificate key types and sizes; use `certutil -store` on Windows hosts to enumerate certificate stores; deploy a free tool such as NIST's National Cybersecurity Center of Excellence (NCCoE) Migration to Post-Quantum Cryptography project worksheets as an inventory template. For code-level RSA/ECC dependency discovery in open-source repositories, `grep -rn 'RSA\|EC_KEY\|ECDSA\|rsa_generate' ./src` provides a low-cost starting scan.

Evidence: This step involves passive enumeration and does not alter live system state in its inventory phase; no volatile capture is required before the inventory itself. However, if the inventory triggers any certificate replacement or key rotation actions, document all currently deployed certificate thumbprints, key sizes, expiration dates, and associated service bindings before any rotation begins, as this baseline is required to verify migration completeness and to support rollback if a replacement certificate causes a service outage.

Step 5: Post-Legislation Readiness — When the bill passes or CISA initiates rulemaking, your documented gap assessment becomes the baseline for your compliance response. Capture lessons from this planning cycle: which threat categories had no mapped controls, which sector plans were last updated before 2022, and which third-party suppliers have no AI or quantum risk posture documented.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: translating the lessons captured during the preparation and assessment cycle into documented improvements to plans, supplier oversight processes, and control coverage before the next compliance event or threat materialization, consistent with the post-incident lessons-learned function applied here to a regulatory planning cycle

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: A 2-person team can formalize this readiness review using a structured lessons-learned document that captures three specific columns: (1) threat category with zero mapped controls in the current sector plan, (2) sector plans last reviewed prior to January 2022 (pre-NIST AI RMF, pre-FIPS post-quantum drafts), and (3) third-party suppliers with no documented AI or quantum risk posture in their most recent vendor risk assessment. This document, version-controlled and dated, serves as the compliance baseline artifact if CISA initiates formal rulemaking.

Evidence: This step involves documentation only and does not alter live system state; no volatile capture is required. Preserve the complete gap assessment outputs from Steps 2 through 4 as immutable records (hash them with SHA-256 and store the hashes in a separate location) so the pre-legislation baseline cannot be inadvertently overwritten when post-rulemaking updates begin — regulators and auditors may require evidence of what the organization knew and when.

Detection Guidance

No technical indicators of compromise apply to this item. Focus on organizational readiness: (1) Monitor cisa.gov/topics/critical-infrastructure-security-and-resilience for updated sector plans and CISA directives. Per NIST SI-5, your organization should have a defined process for receiving and acting on CISA advisories and directives. (2) If your organization uses AI systems in critical infrastructure contexts, establish a logging and anomaly detection baseline for AI pipeline inputs and outputs to prepare for potential future audit requirements. NIST AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) provide the framework for defining and reviewing relevant event categories. (3) For deepfake social engineering risk, review existing phishing and vishing detection controls and assess whether voice and video verification procedures exist for high-trust operational decisions.

Framework Mappings

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

NIST-800-53R5

- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

Sources

Source	URL	Tier
Critical Infrastructure Sectors - CISA	https://www.cisa.gov/topics/critical-infrastructure-security-and-re...	T1
Critical Infrastructure Security and Resilience - CISA	https://www.cisa.gov/topics/critical-infrastructure-security-and-re...	T1
Known Exploited Vulnerabilities Catalog - CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
How CISA Helps Protect Critical Infrastructure in America - UpGuard	https://www.upguard.com/blog/how-cisa-helps-protect-critical-infras...	T3
CISA 2025 Year in Review focuses on driving security and ...	https://industrialcyber.co/cisa/cisa-2025-year-in-review-focuses-on...	T3

Generated 2026-06-12 14:17 UTC by TJS Security Command Center