ANSELM INTELLIGENCE · WEEKLY

Anselm Intelligence Weekly: AI & Cyber Policy for Operators and Investors

Issue: week ending Friday, November 27, 2026 · Sample issue · Prepared by Anselm Intelligence using an AI-assisted process · Sources checked Nov 27, 2026 (ET)

Tags: V = verified against the primary source · V-2 = named secondary source, not re-checked · A = our assessment or estimate, with assumptions stated. This is general business analysis, not legal or investment advice.

The week in 60 seconds

- **Federal market access got a hard date.** FedRAMP says new Rev5 certifications won't be available after **June 11, 2027**. 20x is the path forward, and a High-baseline (Class D) pilot opens in **January 2027**. V
- **Compute export controls reset.** BIS's Nov 19 interim final rule formally rescinds the AI Diffusion Rule. It adds licenses for advanced chips to **Indonesia, Malaysia, Singapore, Thailand and Brazil** and controls on overseas data centers serving D:5-headquartered firms. It took effect immediately; comments are due **Jan 19, 2027**. V
- **January 1 is a cliff for AI deployers.** Three state regimes start that day: Colorado's ADMT Act (SB 26-189), with AG rules adopted **Nov 19**; Colorado's Chatbot Safety Act; and New York's RAISE Act for frontier developers. V
- **Cyber compliance is paused, not cancelled.** CMMC Phase 2 is still suspended (since Jul 13). The CIRCIA final rule is still pending. The EU CRA's 24h/72h reporting has been live since Sep 11. V
- **Platforms are absorbing AI security.** CrowdStrike–Zscaler ($43.9B, all-stock) and Palo Alto–Applied Compute ($4.5B, all-stock) both pitch "securing AI agents and models" as a platform capability. V

1. FedRAMP: the Rev5 door has a closing date

What happened. FedRAMP's 20x Phase 4 page says Phase 4 runs **Oct 1, 2026 – Jun 30, 2027**. "New FedRAMP Rev5 Certification won't be available after June 11, 2027," and a special project in early 2027 will try to get in-process, agency-sponsored Rev5 offerings certified before then. A **20x Class D (High) pilot starts January 2027** for selected Class C holders. Separately, FedRAMP's Nov 2 blog says the first 20x Class A certification was granted on **Aug 25, 2026** and the first full CR26-compliant Class C on **Oct 29, 2026**. V *Caveat: the Phase 4 page carries an "under development" banner. Re-check before relying on it.*

Who is affected. SaaS and AI vendors selling to civilian agencies, especially those mid-way through an agency-sponsored Rev5 package. Also High-baseline aspirants, such as AI platforms that want to host sensitive workloads.

Commercial impact. A For a startup with federal pipeline gated on authorization, the question is now *which path finishes first*. Illustrative assumptions: $4M federal pipeline, 60% of it gated on authorization, and a 25% chance a Rev5 package misses Jun 11, 2027 and has to restart on 20x with a 6-month slip. That puts about **$0.6M of pipeline** (4 × 0.6 × 0.25) at risk of a two-quarter push. Class A (built on a SOC 2 Type II or GovRAMP base) could *shorten* entry for low-risk products. Treat that as a sales-cycle upside worth modeling, not assuming.

When it bites. Jan 2027 (Class D pilot opens), Jun 11, 2027 (Rev5 cutoff) and Jun 30, 2027 (Phase 4 ends).

What executives should check. Is our package on track to finish Rev5 by June 11? If not, should we switch to 20x now? Does our SOC 2 Type II qualify us for Class A? Do federal pipeline forecasts assume an authorization date we can actually hit?

Sources: fedramp.gov/20x/phase4/ ; fedramp.gov/2026-11-02-memo-to-milestone/

2. BIS compute rule: AI Diffusion formally rescinded, new chokepoints added

What happened. BIS published an interim final rule (FR Doc. 2026-23529, RIN 0694-AK50), **effective Nov 19, 2026**, with comments due **Jan 19, 2027** (regulations.gov BIS-2026-0628). The rule does three things:

- It formally rescinds the regulations implementing the January 2025 AI Diffusion Rule, which BIS says "has never been enforced."
- It adds a license requirement for advanced semiconductors to **Indonesia, Malaysia, Singapore, Thailand and Brazil**. Chips going to US-headquartered companies are exempt if reporting conditions are met.

- It restricts exports to **overseas data centers that remotely supply significant compute to companies headquartered in Country Group D:5 or Macau**. Data centers, foundries and exporters must run ownership-based customer due diligence. Commercial recommender systems are carved out. V

Who is affected. Neoclouds and GPU-as-a-service providers with Southeast Asian or Brazilian capacity, chip distributors, model labs renting offshore compute, and investors underwriting data-center buildouts in those markets.

Commercial impact. A Non-US-headquartered operators in the five countries now face licensing lead time on new chip deliveries, which defers revenue on new capacity. US-headquartered operators keep an exemption but take on reporting and know-your-customer (KYC) cost. Customer due diligence on D:5 ownership becomes a contract term, which may lengthen enterprise sales cycles for compute resellers by a diligence step.

When it bites. It is in effect now. Jan 19, 2027 is the comment window to shape the final rule.

What executives should check. Do any of our compute contracts or data-center leases sit in the five countries? Can we show that no customer is ultimately owned in D:5 or Macau? Does our cap table or parent structure qualify for the US-HQ exemption?

Source: federalregister.gov/documents/full_text/html/2026/11/19/2026-23529.html

3. January 1, 2027: three state AI regimes start at once

What happened.

- **Colorado SB 26-189** (signed May 14, 2026) repeals and re-enacts SB 24-205. From **Jan 1, 2027**, developers of covered automated decision-making technology (ADMT) must give deployers technical documentation. Deployers must give point-of-interaction notice and a plain-language explanation within **30 days** of an adverse consequential decision. Consumers get rights to correction and to human review. Violations are deceptive trade practices; there is no new private right of action. A **60-day notice-and-cure** applies to AG actions before 2030. V
- **Colorado AG rules.** The AG's office **adopted the ADMT and Chatbot Safety rules on Nov 19, 2026**. They become final 20 days after publication, following an AG opinion. V
- **Colorado HB 26-1263 (Chatbot Safety Act)**, effective **Jan 1, 2027**, requires chatbot operators to: estimate users' ages, disclose that the user is talking to AI, maintain teen safeguards and self-harm protocols, and file annual reports to the AG. V
- **New York RAISE Act** (as amended Mar 27, 2026), effective **Jan 1, 2027**, applies to large frontier developers. It requires DFS registration through the RAISE Portal and **72-hour critical-incident reports**. V-2 (Wiley; DFS frontier-developer page)

Who is affected. Hiring, lending, insurance, housing and health AI vendors (as developers) and their customers (as deployers). Consumer chatbots and companion apps. A small set of frontier labs.

Commercial impact. A

- **Cost.** Assume 4–12 engineer-weeks at $4k per loaded week for notice, explanation and appeal workflows, plus outside counsel. That is about **$16k–$48k** of internal build per product, before counsel.
- **Sales cycle.** Enterprise deployers in Colorado will ask vendors for SB 26-189 documentation in procurement. Vendors that have it ready remove a step; vendors that don't will see deals slip into Q1.
- **Procurement.** Expect deployer customers to ask for the documentation pack in diligence and renewals; companies without one should plan for added review steps.

When it bites. Jan 1, 2027. The final Colorado rule text could land in late December, so rule details may arrive with days to spare.

What executives should check. Are we a "developer," a "deployer," or both? Do Colorado consumers face our product in employment, lending, insurance, housing or health decisions? Is our deployer documentation pack ready for procurement? Does our chatbot reach Colorado minors?

Sources: leg.colorado.gov/bills/sb26-189 ; coag.gov/ai/ ; dfs.ny.gov/digit/Frontier-Developers ; wiley.law (RAISE Act alert)

4. Cyber reporting and DIB compliance: paused, pending, and live

CMMC. DoW announced the immediate suspension of CMMC Phase II on **Jul 13, 2026** (Phase II had been planned for Nov 10, 2026). Phase I self-assessments (Level 1 annual; Level 2 self-assessment every three years against NIST SP 800-171 Rev 2) remain. A CMMC reform task force is reviewing the program under the Acquisition Transformation System directives. DFARS 252.204-7012 still applies. V - A Near term, this shortens sales cycles for Level 2 subcontractors,

because third-party (C3PAO) assessments are not gating awards. The restart date is the risk. Vendors that cut security spending now could face a compressed catch-up if Phase II returns with short notice. The Senate NDAA (S. 4784) would add CMMC Level 2 grants (§1626, $100k per company) V-2. Conference text was not released as of Nov 22 V-2.

CIRCIA. CISA's page says the agency "continues to work on the final rule." Reporting obligations (72-hour incident, 24-hour ransom payment) do not apply until a final rule takes effect. V The rule was reportedly sent to OIRA Oct 1, 2026. V-2 (HIPAA Journal; MeriTalk)

SEC Item 1.05. A tracker counts **18** Item 1.05 filers in 2026, 12 of them in health care or medical devices, with the latest an Oct 13 amendment (Park Dental Partners). V-2 (Komposite News) A Recent incidents are increasingly being disclosed voluntarily under Item 8.01 rather than as material under Item 1.05. Boards should document their materiality analysis either way.

EU CRA. Since **Sep 11, 2026**, manufacturers of products with digital elements sold in the EU must report actively exploited vulnerabilities and severe incidents through ENISA's Single Reporting Platform. Open-source stewards follow from Dec 11, 2027. V

What executives should check. If CMMC Phase II restarts, how many months do we need to reach C3PAO readiness? Are we a CIRCIA "covered entity" under the NPRM definitions? Does our EU-sold software already have a 24-hour reporting runbook?

Sources: dowcio.war.gov/cmmc/About/ ; cisa.gov/circia ; kompositenews.com (Item 1.05 tracker) ; digital-strategy.ec.europa.eu/en/policies/cra-reporting ; tbh.center (NDAA status, Nov 22)

5. Federal AI policy, procurement and enforcement

- **Terminology.** EO 14434, "Inaugurating the Era of Super Intelligence" (signed Sep 29; 91 FR 63129), directs agencies to use "Super Intelligence (SI)" in non-statutory documents. NIST's new drafts already use the term. V A Federal solicitations and documents will increasingly say "SI." Update proposal templates and keyword-based opportunity searches so they catch both terms.
- **Procurement rules in force.** OMB M-25-21 (use) and M-25-22 (acquisition) remain listed. **M-26-04** (Dec 11, 2025) requires "Unbiased AI Principles" contract terms in new LLM solicitations, and in existing contracts at option exercise. V A For LLM vendors with options coming due, contract modifications are a renewal-timing risk.
- **Standards.** NIST draft SP 2400-102e2026 (adversarial ML, with a new agentic-attack taxonomy) is open for comment until **Dec 18, 2026**. V (nist.gov, read via search index)
- **"SI-washing" enforcement.** On Oct 29, the SEC charged BG Wealth Sharing and DSJ Exchange (N.D. Cal.) over a $130M+ scheme marketed on "SI-generated" trading signals and false Form ADV and Form D filings (LR-26679). V In the same week, the FTC issued 6(b) orders on Oct 28 to nine firms (including Delta, Uber, DoorDash and Walmart) on personalized pricing and worker pay, with responses due in 45 days. V-2 (AP) A AI capability claims in investor and customer materials are now an enforcement surface. Fund LPs will ask about it in diligence.

Sources: federalregister.gov 2026-20321 ; whitehouse.gov/omb memoranda ; sec.gov LR-26679 and PR 2026-110 ; apnews.com (FTC 6(b))

6. Deals: what platform consolidation means for AI-security vendors

Deal	Terms	Status
CrowdStrike / Zscaler	~$43.9B all-stock; 1.135 CRWD per ZS; combined ARR >$10B; pitched as "Zero Trust for AI Safety... securing the last mile of agentic AI"	Announced Nov 23, 2026; 8-K filed V
Palo Alto Networks / Applied Compute	$4.5B all-stock (subject to adjustments); open-weight model post-training and inference; HSR clearance required	Announced Nov 18; expected close in PANW's fiscal Q3 2027 V
CrowdStrike / Fiddler AI	AI observability, folded into Falcon	Announced Nov 3 V; price ~$400M V-2 (TechCrunch citing WSJ)

A The largest security platforms are building AI-agent and model security into their own products: the network path, the model runtime, observability. Two of them now own adjacent capabilities, so expect partner-channel conflict and procurement consolidation in 2027 enterprise renewals. The operating question for an AI-security company is whether its product still wins a renewal once Falcon or Prisma bundles a "good enough" version.

7. Forward calendar, with change flags

Subscribers get this calendar filtered to their own exposure. Every date is re-checked weekly, and any date that moves is flagged in the next issue and in an alert.

Date	Event	Change flag	Tag
Dec 11, 2026	Continuing resolution expires; FY27 NDAA conference text expected around this window	NDAA **slipped**: no conference text as of Nov 22	V-2
~Dec 12, 2026	FTC 6(b) responses due (45 days from Oct 28)	—	V-2
Dec 18, 2026	NIST SP 2400-102e2026 (adversarial ML) comments close	**New** this month	V
Late Dec 2026	Colorado ADMT and Chatbot rules final 20 days after publication	**New**: adopted Nov 19	V
TBD	CIRCIA final rule publication (at OIRA since Oct 1)	**Slipped**: Unified Agenda had "09/00/2026"	V-2
Jan 1, 2027	Colorado SB 26-189 and HB 26-1263 effective; NY RAISE Act effective	Colorado **changed**: was Jun 30, 2026 under SB 24-205 as amended V-2	V / V-2
Jan 2027	FedRAMP 20x Class D (High) pilot begins	**New**	V
Jan 19, 2027	BIS compute IFR comments due	**New**	V
No date	CMMC Phase II (third-party Level 2 assessments)	**Changed**: was Nov 10, 2026; suspended Jul 13, 2026	V
Jun 11, 2027	Last date for new FedRAMP Rev5 certifications	**New** hard stop	V
Jun 30, 2027	FedRAMP 20x Phase 4 ends	—	V
Dec 2, 2027	EU AI Act Annex III high-risk obligations apply (AI Omnibus, in force Jul 27, 2026)	**Changed**: was Aug 2, 2026 (original Reg. 2024/1689 date V-2)	V
Dec 11, 2027	EU CRA reporting obligations extend to open-source stewards	—	V
Aug 2, 2028	EU AI Act Annex I (product-embedded) high-risk obligations apply	**Changed**: was Aug 2, 2027 (original date V-2)	V

What this means for your pipeline: a worked example

A *Illustrative company: a Series B AI-agent security vendor, $18M ARR, selling to US enterprises and two civilian agencies, with EU customers. All inputs are assumptions; subscribers' memos use their own.*

Exposure	Input (assumption)	Effect	Action this quarter
FedRAMP Rev5 cutoff (Jun 11, 2027)	$3M federal pipeline; package 70% complete	If it misses: ~$3M moves to the 20x track, a 1–2 quarter push	Decide Rev5 vs. 20x Class C by Jan 31
Colorado SB 26-189	15% of enterprise customers deploy in hiring or lending flows	Documentation requests in Q1 renewals; ~6 engineer-weeks	Ship the deployer documentation pack by Dec 31
EU CRA (live)	20% of ARR in the EU	24-hour exploited-vulnerability reporting now required	Test the ENISA reporting runbook
Platform bundles (CRWD+ZS, PANW)	30% of renewals compete with a platform	Price pressure in 2027 renewals	Build an evidence-grade differentiation brief

Sample 24-hour alert (format subscribers receive)

> **ANSELM ALERT · CIRCIA final rule published (illustrative trigger, not a real event)** · Sent within 24 hours of publication
> **What:** [FR citation, publication date, effective date, copied from the Federal Register] V · **Changed vs. NPRM:** [covered-entity definition; 72-hour/24-hour clocks; any new exemptions] V
> **Your exposure:** [subscriber's exposure map, e.g., "3 of your critical-infrastructure customers are likely covered entities"] A · **Your calendar:** CIRCIA moves from "TBD" to [date], flagged as changed.

> **Do this week:** confirm the incident-classification owner; update customer-facing reporting language; brief the board.

Every alert follows the same rules as the Weekly: primary citation, tag, and the subscriber's own deadline calendar updated.

For VC funds: portfolio view. The same exposure map and calendar are run across every portfolio company. The output is a single heat map (company × rule × date), alerts routed to the right deal partner, and LP-letter paragraphs. A It is scoped from the fund's public portfolio list; companies opt in to share any non-public detail.

8. Executive checklist for the week

1. **Sales:** re-base federal pipeline against the Jun 11, 2027 Rev5 cutoff and the CMMC restart risk.
2. **Legal/Product:** confirm your Colorado developer/deployer status and documentation pack before Jan 1.
3. **Infrastructure:** map compute and customers to the five newly licensed countries and to D:5 ownership.
4. **Marketing/IR:** audit "AI" and "SI" capability claims in decks, Form ADV/D, and the website.
5. **Investors:** tag portfolio companies by exposure: federal authorization, Colorado ADMT, EU CRA and the export rule.

Methodology: every item answers five questions (what happened, who is affected, commercial impact, when it bites, what to check). We use public sources only and claim no insider access. Corrections run at the top of the next issue. *© Anselm Intelligence.* *Sample issue, prepared by Anselm Intelligence using an AI-assisted process.*