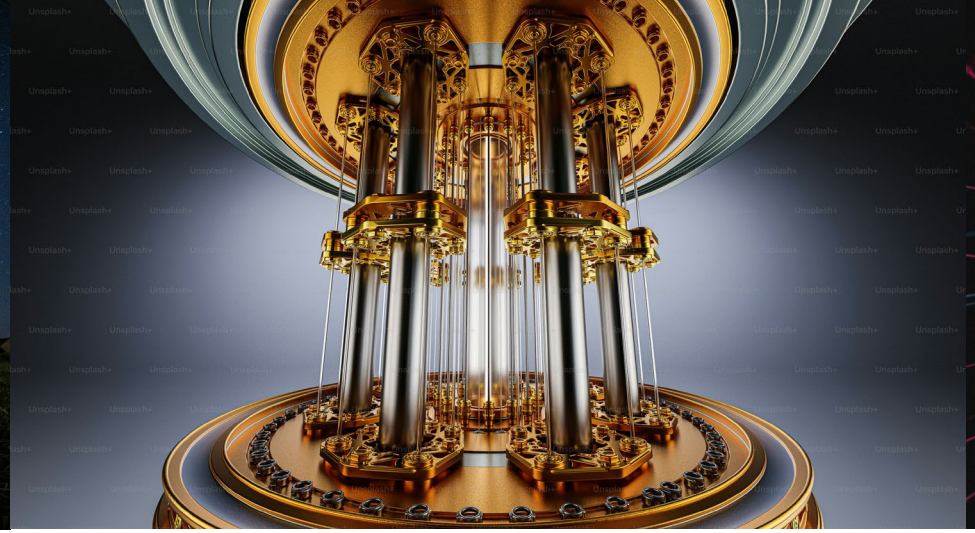
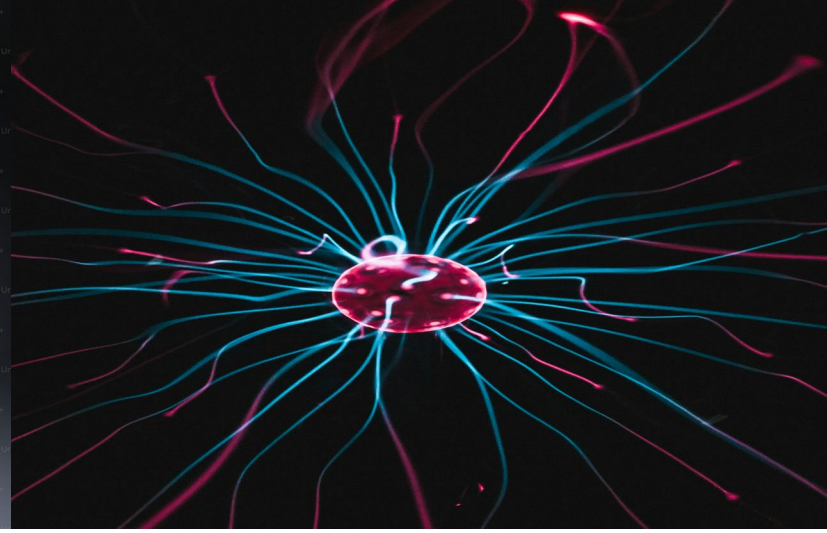




The New Technology Frontier

Quantum, AI, & Protecting Business from Regulatory Risk

Guillermo Christensen, Sanjeev Bhasker, & **Corey Bieber**
Partners, K&L Gates LLP

PRESENTERS



Guillermo Christensen
Partner, K&L Gates



Sanjeev Bhasker
Partner, K&L Gates



Corey Bieber
Partner, K&L Gates

Focus

A briefing on where quantum, AI, and national-security law are heading — and what to do about it now.

Introduction

Framing the convergence of quantum, AI, and national-security law.

Quantum

Quantum Advantage, Q-Day, post-quantum cryptography, and the executive orders.

Artificial Intelligence

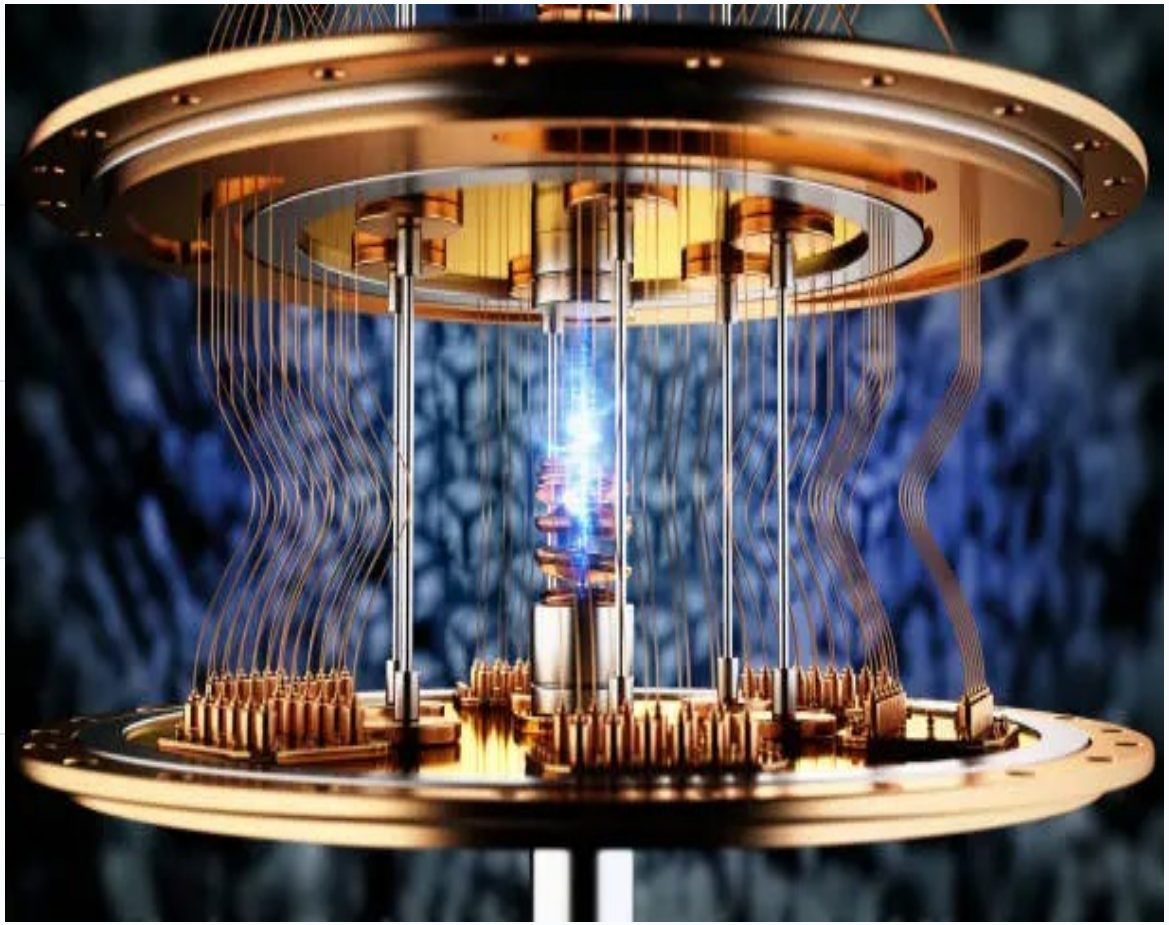
EO 14409, frontier-model oversight, and the GOLD EAGLE cyber clearinghouse.

National Security, Cyber, & Blockchain

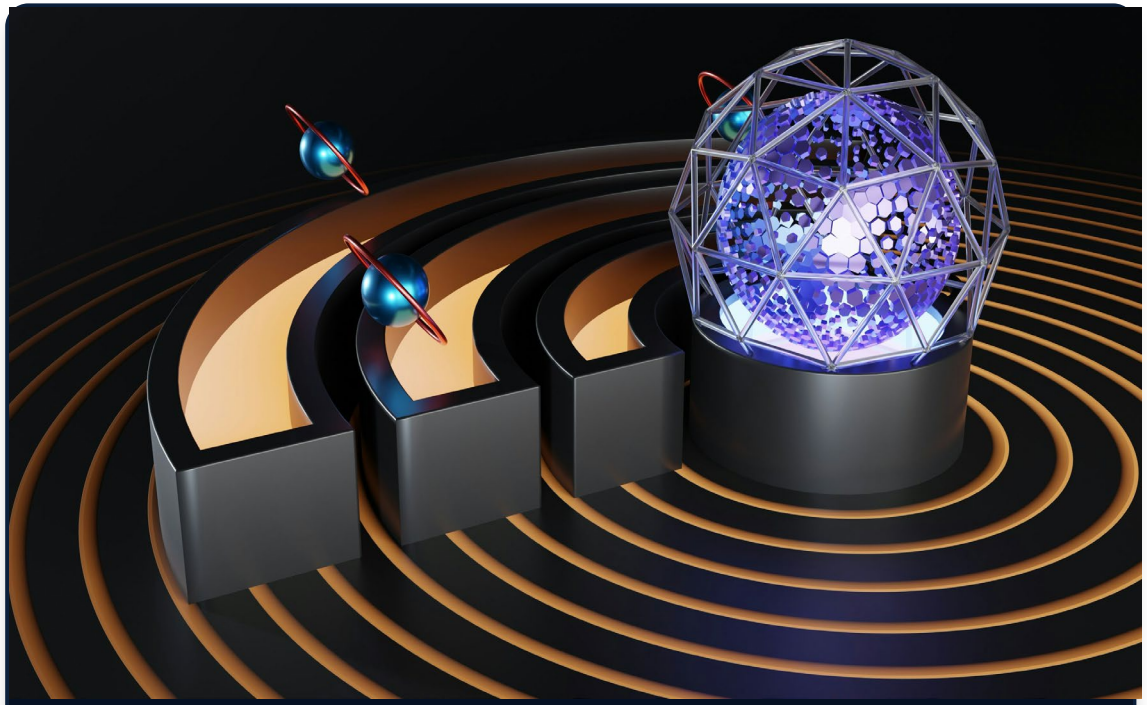
National Security, Digital Assets, CFIUS, and outbound investment.

Resources & Discussion

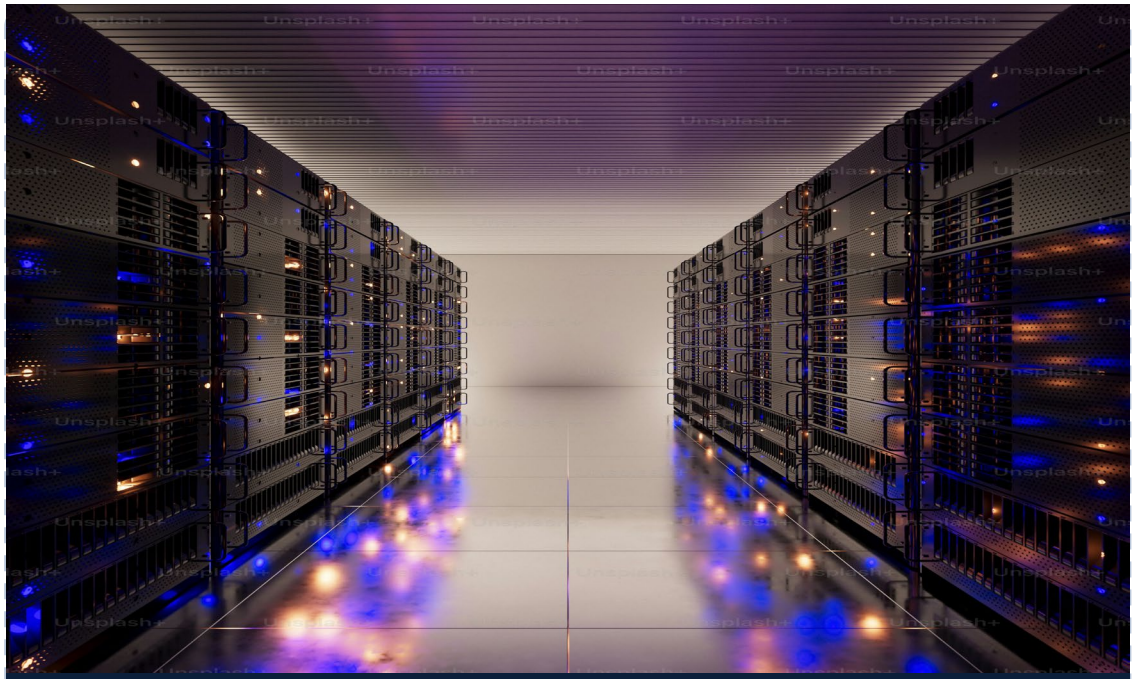
K&L Gates thought leadership and continuing the dialogue, next steps.



Quantum Advantage Meets National Security



Quantum Advantage & Innovation



Post-Quantum Cryptography (PQC) / National Security

QUANTUM

Quantum Computing: The Approaching Reality

Cryptographically relevant quantum computers

A sufficiently powerful quantum computer could break the public-key encryption that secures today's digital infrastructure.

"Q-Day" timing is uncertain — but the risk is not

Large-scale, fault-tolerant quantum computing may still be years away, but the window to prepare is closing.

A strategic priority on par with AI

Quantum now sits alongside AI and advanced semiconductors as a top-tier national strategic technology.

"Harvest Now, Decrypt Later"

Adversaries may already be collecting encrypted data today, wagering that future quantum computers will let them decrypt it years later.

Long-lived sensitive data at risk:

- Trade secrets & IP
- Financial & healthcare records
- Classified / export-controlled data

Industries quantum computing could transform:

Manufacturing • Pharmaceuticals • Energy • Agriculture • Logistics • Materials Science

Quantum Readiness & the NIST PQC Standards

What legal teams need to know about FIPS 203/204/205 and post-quantum cryptography

1 Quantum Readiness

Preparing systems, contracts, and data-retention practices now for the day sufficiently powerful quantum computers can break today's encryption — protecting data that must stay confidential for years ("harvest now, decrypt later" risk).

2 FIPS Standards

Federal Information Processing Standards (FIPS): publicly announced standards NIST develops for U.S. federal computer systems, widely adopted well beyond government. FIPS 203, 204, and 205 are NIST's finalized post-quantum cryptography (PQC) standards.

3 Their Role

These are the vetted benchmark algorithms for quantum-resistant key establishment and signatures. Migration should be risk-based and crypto-agile — prioritized by data sensitivity and lifetime. Not every RSA/ECC use can be replaced today.

NIST-Approved PQC Algorithms

Standard	Algorithm	Purpose
FIPS 203	ML-KEM (formerly CRYSTALS-Kyber)	Key encapsulation / key exchange
FIPS 204	ML-DSA (formerly CRYSTALS-Dilithium)	Digital signatures
FIPS 205	SLH-DSA (formerly SPHINCS+)	Digital signatures (hash-based, stateless)

In 2024, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) released its principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer. These three post-quantum cryptography standards can be implemented now to secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy. NIST continues to evaluate additional algorithms that could one day serve as backup standards.

Source: NIST Post-Quantum Cryptography Standardization — FIPS 203, 204, 205 (finalized 2024)

QUANTUM

Two Executive Orders Reset the National Quantum Strategy

Executive Orders 14412 and 14413, signed June 22, 2026 — a whole-of-government shift from research toward deployment, commercialization, and cyber resilience.



EO 14413 — Ushering in the Next Frontier of Quantum Innovation

- Establishes the QC-ADDS Effort — a DOE-sited quantum computer for science
- Expands quantum sensing & networking R&D
- Directs at least three quantum-sensor projects to be fielded by 30 Sept. 2028



EO 14412 — Securing the Nation Against Advanced Cryptographic Attacks

- Directs agencies to migrate high-value and high-impact systems to PQC
- Adopts NIST FIPS standards for PQC
- CISA/NIST to publish minimum elements for a cryptographic bill of materials

Key Compliance Deadlines

30 days

Each agency identifies its PQC migration lead (EO 14412 § 4(a))

90 days

OMB guidance: inventory high-value and high-impact systems; submit migration plans (§ 4(b))

180 days

FAR proposed rule on FIPS/PQC for contractors; NIST migration pilot; National Quantum Strategy update

270 days

CISA/NIST cryptographic bill-of-materials guidance (§ 5(d)); FAR vulnerability-disclosure rule (§ 6(d))

Dec. 2030 / 2031

High-value and high-impact systems: PQC key establishment, then digital signatures

Sources: Exec. Order No. 14412 & Exec. Order No. 14413 (June 22, 2026), 91 Fed. Reg. 38483, 38487 (June 25, 2026)

ARTIFICIAL INTELLIGENCE

EO 14409: Pairing AI Innovation With Security

"Promoting Advanced Artificial Intelligence Innovation and Security" — signed 2 June 2026

No mandatory AI licensing

Nothing in § 3 authorizes a mandatory licensing, preclearance, or permitting requirement for developing or releasing AI models (§ 3(c)).

"Covered frontier model" benchmarking

§ 3(a) requires a classified benchmarking process, due within 60 days, to set the threshold; NSA makes the designation.

Voluntary pre-release access

§ 3(b) directs a voluntary framework: developers may offer up to 30 days' access before release to trusted partners. Nothing compels participation.

Criminal-enforcement provisions

§ 4 directs the Attorney General to prioritize existing statutes — 18 U.S.C. §§ 1028, 1030, 1343. No new offenses are created.

EO 14409 sets policy — the operational rollout (GOLD EAGLE) is next.

Who Should Be Watching

AI developers

Track the frontier-model framework under Section 3.

Critical-infrastructure operators

§ 2(c) directs CISA to facilitate access to AI-enabled defensive tools and cybersecurity services.

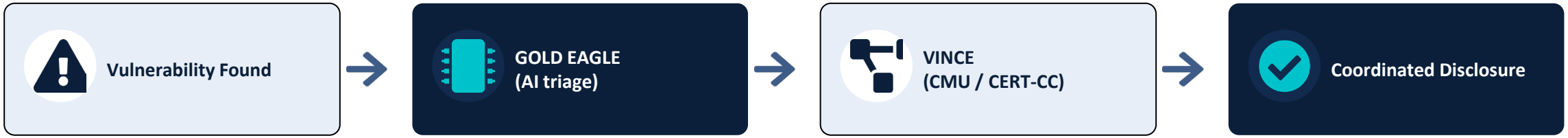
Government contractors

CISA BOD 26-04 (10 June 2026) followed § 2(c); directives bind federal civilian agencies, not industry.

Source: Exec. Order No. 14409 (June 2, 2026), 91 Fed. Reg. 34565 (June 5, 2026); CISA Binding Operational Directive 26-04 (June 10, 2026)

GOLD EAGLE: AI-Enabled Cyber Defense at Scale

Announced 14 July 2026 under EO 14409 § 2(d) — Treasury, DHS/CISA, and the Department of War, in voluntary collaboration with industry.



Voluntary participation

No mandatory reporting or licensing requirements for industry.

Financial-sector emphasis

Treasury's early outreach centers on financial institutions.

FFRDC custodian

Carnegie Mellon’s SEI, an FFRDC, operates VINCE, reported as the intake platform.

Protections may lapse

CISA 2015 liability & FOIA protections are authorized only through 11 Dec. 2026 (6 U.S.C. § 1510(a)).

Sources: Exec. Order No. 14409 § 2(d); White House announcement (July 14, 2026); 6 U.S.C. § 1510(a) (CISA 2015, sunset Dec. 11, 2026)

Blockchain & Digital Assets



Digital-asset policy

EO 14178 (Jan. 23, 2025) established the President's Working Group on Digital Asset Markets.

Strategic reserves

EO 14233 (Mar. 6, 2025) established the Strategic Bitcoin Reserve and U.S. Digital Asset Stockpile, capitalized with forfeited government digital assets.

GENIUS Act framework

First federal payment-stablecoin regime: full reserve backing, with supervision assigned by issuer type — OCC, Federal Reserve, FDIC, NCUA, or state regulators. OCC rule final Oct. 21, 2026; other rules pending. Act effective Jan. 18, 2027.

AML & sanctions obligations

The statute itself treats permitted issuers as financial institutions under the Bank Secrecy Act, carrying AML and sanctions duties. Implementing rules have been proposed and are not yet final.

Sources: Exec. Order Nos. 14178 & 14233 (2025); GENIUS Act (July 18, 2025); OCC final rule (Oct. 21, 2026); FinCEN/OFAC proposed rule (Apr. 8, 2026)

CFIUS and Outbound Investment: Two Gates, One Target

Treasury runs both regimes. CFIUS screens foreign capital coming in; the Outbound Investment Security Program (OISP) restricts U.S. capital going out.



CFIUS — Inbound (31 C.F.R. Parts 800 & 802)

- Reviews foreign investment in U.S. businesses for national security risk
- Reaches control deals and non-controlling "TID" investments in critical technology, critical infrastructure, and sensitive data
- Mandatory declarations for certain critical-technology deals; otherwise voluntary, but a non-notified team looks for unfiled deals
- Outcomes: clearance, mitigation, or presidential prohibition



OISP — Outbound (31 C.F.R. Part 850)

- In force since Jan. 2, 2025 (EO 14105); codified by the COINS Act in the FY2026 NDAA
- Applies to U.S. persons and the foreign entities they control
- Bright-line rules, not case-by-case review: a deal is prohibited, notifiable (within 30 days of closing), or permitted
- Targets China-linked companies in semiconductors, quantum, and AI

Where AI and Quantum Meet Both Regimes

Critical technology

Export-controlled AI chips and quantum items can trigger mandatory CFIUS filings.

Prohibited technology

Outbound rules bar U.S. investment in China-linked quantum computing and advanced AI developers.

Same adversaries

CFIUS policy and the COINS Act both name China, Cuba, Iran, North Korea, and Russia.

Active enforcement

CFIUS opened 62 non-notified inquiries in 2025; Treasury imposed its first OISP penalty in 2026.

Sources: 50 U.S.C. § 4565; 31 C.F.R. Parts 800, 802 & 850; Exec. Order No. 14105 (Aug. 9, 2023); COINS Act, FY2026 NDAA (Dec. 18, 2025)

INVESTMENT SECURITY

CFIUS: Where AI and Quantum Deals Draw Scrutiny

Critical-technology analysis is the gating question, and the Committee now has its own engineers to test the answer.

Mandatory filings follow export controls

Investment in a U.S. business that develops critical technology, such as advanced AI chips or quantum items controlled in 2024, can require a declaration 30 days before closing.

Minority stakes count

Board or observer seats, access to material nonpublic technical information, or a role in substantive decisions bring non-controlling deals into scope.

AI infrastructure is presumptively sensitive

Data centers, compute, and the power assets serving them touch several of the eight risk categories in CFIUS's July 2026 Risk Matrix.

Technical diligence is deeper

Treasury's Office of Research and Analysis (2025) uses scientists and engineers to test how parties describe a target's technology.

Jan. 2026: the President blocked HieFo's acquisition of EMCORE semiconductor assets. CFIUS reaches carve-outs, not just whole companies.

CFIUS by the Numbers (2025)

347 transactions reviewed (207 notices, 140 declarations)

166 involved U.S. critical-technology businesses

26% of declarations drew a request for a full notice

62 official inquiries into deals that were not filed

Sources: CFIUS Annual Report to Congress, CY 2025 (Aug. 7, 2026); CFIUS Risk Matrix (July 29, 2026); 31 C.F.R. §§ 800.211, 800.401; Presidential Order (Jan. 2026)

INVESTMENT SECURITY

CFIUS Under the America First Investment Policy

Feb. 21, 2025 presidential memorandum: welcome allied capital, and restrict adversary-linked investment in strategic technology.

Feb. 2025
America First Investment Policy issued

→

May 2025
Known Investor pilot launched

→

Feb. 2026
Known Investor RFI; comments closed Mar. 18

→

July 2026
Risk Matrix and new CFIUS website

→

Aug. 2026
Annual Report for 2025 released

Known Investor Program

A fast track for frequent filers (three or more filings in three years) with verifiable distance from adversary countries. Final framework still pending.

Adversary-linked capital

CFIUS is directed to use all available tools to restrict PRC-affiliated investment in technology, critical infrastructure, and other strategic sectors.

Mitigation recalibrated

The policy disfavors open-ended mitigation, yet 2025 mitigation held at about 12% of notices, and proxy agreements are now a listed tool.

What it means for AI & quantum

Allied investors may move faster. A China nexus among investors, co-investors, or suppliers can rule out fast-track treatment.

Sources: America First Investment Policy (Feb. 21, 2025); CFIUS Known Investor RFI, 91 Fed. Reg. 5694 (Feb. 9, 2026); CFIUS Annual Report, CY 2025 (Aug. 7, 2026)

Outbound Rules Today: AI and Quantum Under Part 850

In force since January 2, 2025, and still governing until a COINS Act final rule takes effect.

1 Who is covered

U.S. persons, including when they knowingly direct a deal or control a foreign entity that makes one.

2 Covered transactions

Equity and contingent equity, certain convertible debt, greenfield projects, joint ventures, and certain LP stakes.

3 Covered foreign persons

Persons of a country of concern (China, Hong Kong, Macau) engaged in a covered technology activity.

Sector	Prohibited	Notifiable
AI systems	AI designed exclusively for military, intelligence, or mass-surveillance end uses; or trained with more than 10^{25} operations (10^{24} if mainly biological sequence data)	AI for any such end use, or for cybersecurity, digital forensics, penetration testing, or robotic control; or trained with more than 10^{23} operations
Quantum	Quantum computers and critical components; quantum sensing for military, intelligence, or surveillance end uses; quantum networks for scaling computers or secure communications	None. All covered quantum activity is prohibited
Semiconductors	EDA tools, advanced-node fabrication, advanced packaging, and supercomputers	Design, fabrication, or packaging of other integrated circuits



First OISP enforcement (announced Oct. 2026): a $200,000 civil penalty against Amidi, LLC for failing to notify Treasury of a roughly $92,000 investment by its Chinese fund subsidiary in an embodied-AI company.

Sources: 31 C.F.R. Part 850 (incl. §§ 850.217, 850.224); Exec. Order No. 14105; Treasury OISP enforcement announcement (Oct. 2026)

The COINS Act NPRM: From “Notify” to “Prohibit”

Treasury’s proposed rule (Oct. 22, 2026) would replace Part 850 with a new Part 851 and sharply widen the AI and quantum restrictions.

1 COINS Act enacted
Dec. 18, 2025
FY2026 NDAA codifies the outbound program.

2 NPRM issued
Oct. 22, 2026
Proposed Part 851. Part 850 governs until the effective date.

3 Comments due
Dec. 7, 2026
Treasury seeks input on SI scope, definitions, de minimis, and knowledge.

4 Final rule
Date not yet set
The final rule will set the effective date.

AI becomes “Super Intelligence”

- Prohibits any covered deal with a covered foreign person developing any SI system
- Drops compute thresholds, end-use tests, and the AI notifiable tier
- Covers agent harnesses and embodied SI: robots, autonomous vehicles, unmanned systems
- Enhancing a third-party model counts as “development”; internal, non-commercial use does not

Quantum expands

- Keeps all current quantum prohibitions
- Adds development of quantum algorithms and applications
- Preamble cites an end-use limit missing from the reg text, a key comment point
- Supercomputers and enabling components prohibited; HPC interconnects notifiable

Broader reach

- Adds Cuba, Iran, North Korea, and Russia as countries of concern
- New sectors: HPC, hypersonics, and biotechnology
- “Direction or control” test; “develop” reaches affiliates and high-level oversight
- Non-binding feedback process; IEEPA-level penalties and forced divestment

Sources: Treasury NPRM, Outbound Investment Security Program (Oct. 22, 2026; Fed. Reg. Oct. 26, 2026); Treasury Press Release SB0667; Exec. Order No. 14434 (Sept. 29, 2026)

Deal Playbook: Managing Inbound and Outbound Risk

AI and quantum transactions now need both analyses, often on the same deal.



Inbound: CFIUS

- Classify the target's technology (ECCNs) early; it drives the mandatory-filing analysis
- Map the deal against the eight CFIUS Risk Matrix categories before signing
- Scrutinize minority rights: board and observer seats, technical-information access
- Weigh declaration vs. notice: 26% of 2025 declarations drew a notice request
- If not filing, document why. The non-notified team is looking



Outbound: OISP and COINS

- Comply with Part 850 now; cure 2025–2026 notice gaps and weigh self-disclosure
- Inventory China-linked AI and robotics deals: notifiable today may be prohibited later
- Document a "reasonable and diligent inquiry." Treasury will publish no screening list
- Lock in binding capital commitments before the effective date; review governance rights
- Consider commenting on the NPRM by December 7, 2026

Both regimes are Treasury-led, defined by technology, and actively enforced. Build them into AI and quantum deal timelines from the term sheet forward.

Sources: CFIUS Risk Matrix (July 2026); CFIUS Annual Report, CY 2025; 31 C.F.R. Part 850; Treasury COINS Act NPRM (Oct. 22, 2026)

RESOURCES

Guillermo Christensen
Partner, K&L Gates
Guillermo.Christiansen@klgates.com

Sanjeev Bhasker
Partner, K&L Gates
sanjeev.bhasker@klgates.com

Corey Bieber
Partner, K&L Gates
corey.bieber@klgates.com

Quantum

K&L Gates Quantum Industry Group

Alert: Preparing for Q-Day (6.26.26)

Artificial Intelligence

K&L Gates AI Solutions Group

Alert: GOLD EAGLE Takes Flight (7.29.26)

Digital Privacy

Data Protection, Privacy, and Security Group

Alert: The Chatrie Decision (7.8.26)

K&L GATES

