KPMG

Regulatory Alert

Regulatory Insights

September 2026

The White House National Security Science and Technology Strategy

KPMG Regulatory Insights:

Science and Technology Leadership as National Security: *Details science and technology (S&T) leadership as a national security objective for the Administration and sets out how federal research and development would support national security.*

Public-Private Partnership: *Calls for fostering increased public support for private R&D and technology enterprises, including incentives and rewards for private partners and alignment of infrastructure and funding with security priorities.*

Emerging Technologies Guide Priorities: *Builds on federal initiatives to advance emerging technologies, including AI infrastructure and quantum innovation, indicating priorities for future federal research and agency and department efforts.*

The White House has issued its National Security Science and Technology Strategy (the Strategy) outlining how federal science and technology (S&T) activities should "support and enable" the 2025 National Security Strategy. The Strategy emphasizes S&T innovation and competition relevant to military capabilities, homeland defense and resilience, and other national security applications, while providing priorities and direction for federally funded research and development.

The Strategy is organized around four pillars:

1. **Focus Techno-Strategic Competition**, including advancing battlefield advantage, countering strategic threats to the homeland, and shaping competition.
2. **Build Technological Resilience**, including focusing on national security challenges and opportunities, leading in transformative emerging technologies, enabling national resilience architecture, and controlling access to critical technology systems and supply chains.
3. **Accelerate the Pace of Innovation**, including incentivizing innovators and federally funded researchers, removing administrative and regulatory burdens, and accelerating acquisition reforms.
4. **Protect National Security S&T**, including strengthening research security, modernizing foreign investment screening and security, streamlining outbound investment, export controls, and data transfer restrictions.

The Strategy builds on recent White House actions addressing technology innovation, infrastructure, and national security, such as the July 2025 AI Action Plan (which addresses innovation, infrastructure, and diplomacy and security) as well as executive orders addressing data-center infrastructure, AI technology exports, and federal procurement of large language models (see KPMG Regulatory Alert, here). More recent executive orders have addressed related topics, including quantum innovation and protection against advanced cryptographic attacks (see KPMG Regulatory Alert, here).

Pillar 1: Focus Techno-Strategic Competition

The Strategy prioritizes technological advantage in areas integral to deterring attack and prevailing in conflict against sophisticated and capable adversaries, capitalizing on existing areas of U.S. advantage. Key priorities include:

Area	Key Priorities
Technological Battlefield Advantage	Maintain and advance U.S. technological advantage on the battlefield, including: — Submarine survivability and anti-submarine warfare. — Space superiority in technology to detect, characterize, and counter threats in very low-Earth orbit and cislunar space. — AI and autonomy applications in national security. — Air superiority. — Long-range strike capability. — Command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance (C5ISR). Prioritize leadership in and application of key enabling technologies, such as advanced manufacturing and materials; AI and autonomy; communications and networking; nuclear energy; space technologies.
Homeland Defense	Leverage technology to counter strategic threats to the U.S. homeland, including: — Land, air, and maritime border security. — Nuclear deterrent forces. — Missile defense shield (re: Golden Dome Initiative). — Critical data, network, asset, and infrastructure protections. — Biological weapon threats.
Technology Competition	Shape technology competition toward areas of U.S. strength, including: — Embracing novel approaches to national security challenges. — Seeking optimal combinations of lower cost/low-tech platforms and sophisticated platforms that may shift an adversary's allocation of resources. — Avoiding technological competition where it favors adversaries and expends resources without improving U.S. security. — Pursuing cooperative mutual restraint in areas, such as prohibitions on biological and chemical weapons, while maintaining persistent readiness to deter adversaries that may abandon such restraint. — Collaborating with partners to shape norms, standards and governance for Critical and Emerging Technologies (CET), including U.S. participation in international standards bodies.

Pillar 2: Build Technological Resilience

Technological resilience requires avoiding overreliance on vulnerable technologies and supply chains, deploying solutions that reduce adverse consequences for national security functions, and ensuring that adversary S&T advances are very unlikely to upset the United States' ability to protect its vital interests. Key priorities include:

Area	Key Priorities
National Security Challenges and Opportunities	Anticipate national security challenges and emerging opportunities through ongoing, iterative and forward-looking assessments, which include: — Identifying of technology-based single points of failure. — Observing technology use and adaptation in combat. — Anticipating effects of fundamental scientific discovery on the security environment. — Ensure and expand threat and vulnerability information sharing across agencies and with the private sector.
Transformative Emerging Technologies	Build long-term technology resilience by focusing on transformative emerging technologies, which may include: — AI and autonomy. — Biotechnology. — Quantum information technology.
National Resilience Architecture	Enable the national resilience architecture through modernizing critical infrastructure, "distributing risk through optimal redundancy," and simplifying/accelerating the U.S. response to adversary attacks and events, in areas such as: — Nuclear-powered microgrids. — Weather and Earth-system natural disaster modeling. — AI-enabled bio-surveillance. — Biomanufacturing. — Critical network segmentation. — Cryptography and cyber infrastructure. — Cyber-physical threat modeling and AI-driven anomaly detection. — Novel material substitutions. — Bio-incident response.
Critical Technology Systems and Supply Chains	Guard against foreign adversary access to critical technology systems and supply chains, through efforts to: — Prioritize homeshoring and domestic product development. — Facilitate "reindustrialization" and energy dominance. — Identify material substitution for critical components. — Work with trusted partner suppliers. — Utilize protective authorities (e.g., Federal Communication Commission's (FCC) Covered List). — Coordinate with ally and partner governments.

Pillar 3: Accelerate the Pace of Innovation

The Strategy seeks to increase S&T agility – stating that agility sustains U.S. advantage in critical areas over time, denies advantage to adversaries as their capabilities evolve, and underwrites technological resilience. Key priorities include these areas:

Area	Key Priorities
Innovators	Incentivize and enable innovation in all sectors to contribute to national security through various measures, including: — Rapid R&D funding for CET areas. — Short-turnaround innovation challenge competitions. — Rewards for private and academic participants that meet priority mission needs. Incentivize and empower federally funded researchers to enable new discoveries and rapid learning, including encouraging trial and error efforts, reducing aversion to risk, permitting "fail fast" approaches, and embracing a readiness to pivot to adjacent or complementary research.
Administrative and Regulatory Burdens	Remove "administrative and regulatory burdens" while protecting safety and security, by: — Updating or removing "burdensome and outdated" federal regulations. — Streamlining waivers and exemptions for testing and evaluation applications. — Using advisory boards effectively. — Accelerating security-clearance processes.
Acquisition Reform	Accelerate acquisition reform by shortening development and acquisition cycles in the defense and broader national security sectors, by: — Using Other Transaction Authorities (OTA) where appropriate for research, prototype, and production projects. — Employing milestone-based fixed-cost contracting mechanisms with competition and performance-based down-select. — Mixing traditional and nontraditional contracting mechanisms.

Pillar 4: Protect National Security S&T

The U.S. will seek to protect its S&T ecosystem against foreign theft, diversion, and exploitation while maintaining its productivity and agility and addressing risks to U.S. economic and military strength and competitiveness. Key priorities include:

Area	Key Priorities
Research Security	Strengthen research security in U.S. and international R&D environments through efforts to: — Establish processes to track federal research funding recipients. — Restrict research funding for high-risk entities. — Create risk-based reviews and a repository of sharable information to enhance efficiency. — Require universal reporting forms. — Automate vetting and monitoring of proposals. — Increase counterintelligence and cybersecurity measures. — Cooperate with allies and partners for research security.
Foreign Investment Screening and Security	Modernize foreign investment screening and security while maintaining an open investment environment by strengthening the Committee on Foreign Investment in the United States (CFIUS): — Monitor "greenfield" investments for national security concerns. — Bolster CFIUS awareness through information-sharing. — Focus or ease restrictions on foreign investment "in proportion to an investor's verifiable distance and independence" from foreign adversaries or threat actors. Protect against U.S. persons investing in adversary military industrial sectors by implementing and strengthening the Outbound Investment Security Program (Outbound) in areas such as AI, quantum information systems, semiconductors, supercomputers, and hypersonics.
Export Controls and Data Security	Strengthen and streamline export controls and data transfer restrictions, by taking steps to: — Update export controls to keep pace with emerging risks, evolving technologies, and the broader strategic environment. — Eliminate identified outdated controls. — Coordinate export control regimes across agencies. — Prioritize implementation of the Data Security Program, covering government-related data, as well as bulk genomic, geolocation, biometric, health, financial, and other sensitive personal data.

Strategy Implementation

Federal departments and agencies are expected to plan national security S&T activities "in a manner consistent with this strategy," including:

- Following technology-specific strategies and plans for CETs as supported by the Office of Science and Technology Policy (OSTP) and National Security Council (NSC).
- Accounting for competitors' moves and countermoves.
- Pursuing Congressional authorization, appropriations, and legislative initiatives, as appropriate.

Implementation areas and priorities include:

- **S&T Workforce:** Ensure a skilled cross-sector national security S&T workforce.
- **R&D Infrastructure:** Review and reform each agency's R&D enterprise.
- **Federal R&D Funding:** Align with the Fiscal Year 2028 R&D Priorities Memorandum and focus resources where they can best complement private sector investment rather than compete with it.
- **Public-Private Partnerships:** Strengthen partnerships with non-federal partners such as industry and academia.
- **Ally/Partners Capabilities:** Use allied and partner capabilities as a force multiplier.

For more information, please contact Tom Frame, Michael Isensee or Ellen Ozderman.

Contact

Laura Byerly
Managing Director
Regulatory Insights
lbyerly@kpmg.com

Brian Hart
Principal
Risk, Regulatory and Compliance
bhart@kpmg.com