National Security Science & Technology Strategy

August 2026

Overview

This document establishes a National Security Science and Technology Strategy (NSSTS) to support and enable the 2025 National Security Strategy (NSS). It satisfies the Congressional requirement for a "Strategy…on the nation's economic security, science, research, and innovation to support the national security strategy" (42 USC 19221; Sec. 10612 of the CHIPS and Science Act, P.L. 117-167) to be submitted by the Director of the Office of Science and Technology Policy (OSTP) after the transmission of each National Security Strategy.

The NSSTS describes how the United States will leverage its science and technology (S&T) enterprise to support and enable the objectives of the 2025 NSS. In doing so, it highlights and connects directly to many of those objectives. The NSS recognizes the integral role for S&T in achieving the vision it lays out, so much so that S&T leadership is itself a national security objective.

This strategy focuses on S&T competition as it relates to military capabilities, homeland defense and resilience, and other direct intersections with national security. Similarly, this strategy complements and is consistent with National Science and Technology Memorandum 5 (NSTM-5) on Fiscal Year 2028 Administration Research and Development Budget Priorities. NSTM-5 sets Fiscal Year 2028 research and development (R&D) budget priorities; this strategy provides detailed guidance for organizing Federally-funded R&D and S&T efforts to support national security objectives.

> *"We want to remain the world's most scientifically and technologically advanced and innovative country, and to build upon these strengths."*
>
> – National Security Strategy of the United States, 2025

Trends and challenges that impact U.S. national security S&T competition

Geopolitical factors reflect a world where foreign states with growing economic power seek to challenge U.S. S&T leadership, military dominance, and homeland defense:

- Potential adversaries are investing heavily in advanced technology development and military applications, and actively contesting U.S. leadership in key areas.
- Potential adversaries seek asymmetric capabilities to counter U.S. military superiority, and ways to pursue their objectives below our threshold for military response.
- Potential adversaries seek means to disrupt and exploit complex, interconnected national and global economies, supply chains, and infrastructure, including by controlling the extraction, refining, export, and manufacturing of critical minerals.
- Potential adversaries are attempting to steal U.S. intellectual property, sensitive data, and emerging technologies.

Technology factors underscore the need for the U.S. to move decisively to maintain technological advantage:

- Military applications of advanced technologies compress decision timescales and extend the reach of military forces.
- Technologies advance rapidly and converge in ways that can provide significant economic potential alongside national security risk, necessitating agile development and acquisition cycles.
- Technology and enabling supply chains are diffuse and abilities to influence different portions of the supply chain and S&T sectors vary.
- For some rapidly evolving technologies, there remains significant uncertainty about the implications for national security and timelines on which they will materialize.

Legal, policy, and structural factors must be addressed to maximize the options space for U.S. strategy:

- Efforts to protect sensitive S&T must protect Americans' rights and liberties without unduly slowing the pace of innovation.
- Excessive regulation and inefficient legacy policies must be changed or eliminated so that they do not inhibit the ability of American industry to contribute to national security needs.
- The Federal Government must partner effectively with the private sector, recognizing that the private sector contributes critical capabilities that the government does not possess.

Strategy overview

To achieve U.S. objectives in the face of existing and future challenges, America's national security S&T posture must be *focused*, *resilient, agile*, and *secure*.

- **Focused**: Focus techno-strategic competition in directions and ways that leverage American strengths to advance our interests.
- **Resilient**: Build technological resilience to reduce risk across critical mission and technology areas.
- **Agile**: Accelerate the pace of innovation, technology adoption, and adaptation within the national security arena.
- **Secure**: Protect national security S&T from foreign theft, diversion, and exploitation.

Federal departments and agencies (agencies) will work together to strengthen and apply the means of implementing our national security S&T strategy. This will include:

- Building our S&T workforce;
- Enhancing R&D infrastructure;
- Targeting Federal R&D funding;
- Fostering partnerships with non-Federal stakeholders, and;
- Leveraging ally and partner capabilities.

Pillar 1: Focusing Techno-Strategic Competition

America will focus S&T toward maintaining battlefield advantage, countering strategic threats to the homeland, and shaping the competition toward areas of U.S. strength. Focused prioritization is what makes the strategy affordable as well as effective.

Maintain and advance U.S. technological advantage on the battlefield

The United States will prioritize technological advantage in areas integral to deterring attack and prevailing in conflict against sophisticated and capable adversaries, capitalizing on existing U.S. advantages in key areas.

The NSS identifies three priority areas for U.S. battlefield dominance and power projection:

- **Undersea**: Clear technological superiority in the undersea domain, including submarine survivability and anti-submarine warfare.
- **Space**: Clear technological superiority in the space domain, and ability to detect, characterize, and counter threats to U.S. space interests from very low-Earth orbit and through cislunar space.
- **AI and autonomy**: Competitive advantage in the rapidly evolving area of military and other national security applications of AI and autonomy.

Other areas critical to U.S. battlefield dominance and power projection include:

- **Air**: Clear air superiority enabled by stealth technology, electronic warfare, and anti-air capabilities.
- **Long-range strike capability:** Ability to penetrate advanced layered defenses, reach targets on operationally relevant timescales, and strike with precision.
- **Command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance (C5ISR):** Information dominance in all phases of conflict, and superior ability to direct, coordinate, and control forces and assets, including in the face of adversary cyber operations.

To maintain and advance U.S. dominance across these critical domains, relevant agencies should prioritize leadership in and application of key enabling technologies, including:

- Advanced manufacturing and materials
- AI and autonomy
- Communications and networking
- Directed energy
- Future computing technologies
- Hypersonics and advanced missile technologies
- Information management and cybersecurity
- Nuclear energy
- Positioning, navigation, and timing (PNT)
- Semiconductors and microelectronics
- Sensing and signature management
- Space technologies

The United States will advance general leadership in these areas, and within national security S&T will prioritize their development and application toward ensuring America's military remains the most technologically advanced in the world.

Appendix A includes these technologies among others that are critical for U.S. national security. It constitutes an update to the OSTP list of CETs relevant to U.S. national security. Appendix B illustrates alignment of CET areas across elements of the NSSTS.

Leverage technology to counter strategic threats to the homeland

While competing to sustain American advantages on the battlefield, the United States must also counter threats to the homeland, denying strategic advantage to adversaries. We will prioritize application of S&T to deny any adversary's ability to impose significant harm on America without first challenging our superior military on the battlefield. This includes:

- Securing our borders at land, air, and maritime approaches;
- Ensuring survivable and credible nuclear deterrent forces;
- Deploying and maintaining a next-generation missile defense shield as directed under the Golden Dome for America initiative;
- Protecting critical data, networks, assets, and infrastructure against cyberattacks and espionage; and
- Countering biological weapon (BW) threats.

Relevant agencies should include, within their S&T activities, a dedicated focus on supporting these elements of homeland defense. Ensuring U.S. leadership in the same set of priority technologies that are critical to battlefield advantage, and in biotechnology due to its implications for countering BW threats, will posture the United States to deny any strategic advantage adversaries may seek to achieve by threatening Americans at home. Appendix B illustrates where priority CET areas directly enable homeland defense.

Shape technology competition toward areas of U.S. strength

America's robust innovation ecosystem is a key strength that we will leverage to deliver effective and affordable solutions to national security challenges. Exercising this strength requires embracing novel approaches to meet mission needs. From establishing requirements to fielding capabilities, agencies must avoid defaulting to easy answers limited by what we possess and know how to do today, and must accept risk to enable discovery.

We will not reflexively mirror an adversary's offensive systems where our own technological edge already provides a cheaper defensive counter. Maintaining U.S. advantage will sometimes require fielding systems that less capable countries cannot match, and other times may require a direct edge over adversaries' closest equivalents. In every case, solutions must be both affordable and effective, and must anticipate and account for adversary responses. These realities combined may mean leveraging exquisite technology in platforms deployed in small numbers to defeat lower-cost systems that adversaries field at scale. In other cases, the best solutions will be innovative but lower-cost counters. To enable effective and affordable strategies for addressing complex threats, we will seek optimal combinations of lower-cost (and sometimes lower-tech or attritable) platforms that can be deployed in larger numbers and complement more limited numbers of sophisticated platforms.

In addition to delivering meaningful military capability, such technology development activities can serve to dilute and shift adversaries' allocation of resources from more

threatening offensive capabilities to defensive capabilities that pose less of a direct threat. For example, exquisite U.S. strike capabilities integrated with large numbers of lower-cost but technology-enabled assets can drive competitors to allocate more of their resources toward expensive air and missile defenses.

Successfully shaping the competition also requires avoiding forms of technology competition where capable adversaries can readily counter U.S. moves with less effort, and that therefore present effective cost imposition strategies they can employ against the United States. We must avoid situations where competing for advantage favors adversaries and works against the objectives of U.S. strategy by expending resources without improving U.S. security.

In some areas, cooperative mutual restraint can deny competitors strategic advantage while preserving U.S. resources for higher priorities, as with longstanding prohibitions on biological and chemical weapons and on stationing weapons of mass destruction in outer space. The United States will maintain persistent readiness to counter and deny such advantage through deterrence and defense should adversaries abandon agreed restraint, and to compete directly wherever necessary. Finally, focusing technology competition in directions that favor U.S. advantages includes shaping the rules that influence how the competition unfolds. The United States will work vigorously and collaboratively with like-minded partners to shape CET norms, standards, and governance in ways that enable rather than hinder U.S. competitiveness. This will include ensuring robust and deliberate American participation on international standards bodies.

Pillar 2: Building Technological Resilience

The United States will build technological resilience to reduce risk across critical mission and technology areas. This underwrites both technological advantage on the battlefield and the ability to counter strategic threats to the homeland, now and over the long term.

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.

Technological resilience contributes to deterrence by denial—dissuading attacks by denying the benefits adversaries might otherwise expect to achieve by acting against the United States. It is also a form of hedging in cases where technology development might yield fundamental changes that upset strategic stability or provide advantage to the United States or its adversaries. The United States will strengthen technological resilience by anticipating national security challenges and emerging opportunities, leading in transformative emerging technologies where national security implications remain uncertain, enabling the national resilience architecture, and keeping foreign adversaries out of critical U.S. technology systems and supply chains.

Anticipate national security challenges and emerging opportunities

The United States will conduct ongoing, iterative, and forward-looking assessments to understand the national security implications of emerging technologies, adapt to meet evolving challenges, and take advantage of new opportunities. These assessments will inform where the United States competes for advantage, where it denies advantage to adversaries, and where mutual restraint serves American interests. They should range from identifying technology-based single points of failure, to observing how technology is used and adapted in modern combat, to anticipating how fundamental scientific discovery may reshape the future security environment.

Relevant agencies should ensure and expand collaborative and consolidated sharing of threats and vulnerabilities across agencies and with the private sector as appropriate. For example, the AI Action Plan calls for a new AI Information Sharing and Analysis Center, led by the Department of Homeland Security, to promote the sharing of AI-security threat information and intelligence across U.S. critical infrastructure sectors.

Lead in transformative emerging technology areas

Resilience efforts often focus on risks that exist today or may arise in the immediate future. That is essential, but is not sufficient for true technological resilience. We must also guard against the possibility that still-nascent technologies will lead to new strategic threats in the future. In other words, we must be resilient to technology transformation. This cannot mean halting technological progress. Instead, the United States will build long-term technology resilience by leading in potentially transformative emerging technologies, where the national security implications and timelines remain uncertain. Such leadership strengthens resilience by reducing the risk that a breakthrough catches the United States by surprise. Some of these technologies appear elsewhere in this strategy; they carry significant implications today, but their future may look fundamentally different.

Potentially transformative emerging technologies include, but are not limited to:

- Artificial intelligence and autonomy - where approaching or achieving artificial general intelligence could present fundamentally new opportunities and threats;
- Biotechnology - where novel applications to human health and performance could drastically alter our competitive advantage, and adversary development of engineered bioweapons could transform the strategic threat space; and
- Quantum information technologies - where future breakthroughs could have profound implications for sensing, communications, computing, and information security.

"We want to ensure that U.S. technology and U.S. standards—particularly in AI, biotech, and quantum computing—drive the world forward."

– National Security Strategy of the United States, 2025

Enable the national resilience architecture

The United States will build technological resilience into critical national functions by modernizing critical infrastructure; distributing risk through optimal redundancy; and simplifying, streamlining, and accelerating response to adversary attacks and other unanticipated events.

The United States will modernize aging and vulnerable infrastructure critical to national security, proceeding from a risk-informed prioritization basis. Opportunities include improving energy resilience by establishing microgrids powered by advanced nuclear reactors, utilizing state-of- the-art terrestrial and space weather forecasts and Earth system models to enhance the resilience of physical assets and infrastructure to current and future natural disasters, operationalizing AI-enabled biosurveillance to better identify and characterize novel-agent bioattacks and disease outbreaks, leveraging biomanufacturing to onshore critical supply chains, building segmentation into critical network architectures, and modernizing cryptography and cyber infrastructure. This also includes prioritizing S&T to secure operational technology and industrial control systems through cyber-physical threat modeling and AI-driven anomaly detection. To mitigate supply chain vulnerabilities for critical components, we will advance R&D in novel material substitutes and digital tools for verifying component provenance.

Optimal redundancy balances between risk reduction, resource cost, and mitigation responsibility, and ensures that an adversary must solve multiple hard technical problems at once to inflict grave harm. It may be achieved through separation in space (replicating a capability in disparate locations), in time (holding reserve capability for deployment after an incident), or in technology (duplicating a function across systems that do not share the same vulnerabilities). Consider the nuclear triad. An adversary seeking to negate America's nuclear deterrent must contend simultaneously with hard problems posed by ballistic-missile

submarines hidden across the oceans, ICBMs dispersed over vast territory, and bombers with flexible alert capability. No single breakthrough defeats all three. This is the logic of redundancy, and the United States will apply it across critical national security architectures. The goal is not imperviousness, which is rarely affordable, but graceful degradation: an architecture that bends under adversary action or natural disaster rather than failing all at once.

The United States will develop technology solutions that add resilience by simplifying, streamlining, and accelerating response to adversary attacks and other unanticipated events. Opportunities include improved bio-incident response to identify and distribute therapeutics following an outbreak, responsive space launch for rapid reconstitution of critical orbital assets, and capabilities for orbital debris remediation.

Keep foreign adversaries out of critical technology systems and supply chains

The United States must guard against foreign adversary exploitation of critical technology systems and supply chains. Prioritizing homeshoring and domestic product development, which the Trump Administration is advancing by promoting balanced trade, facilitating reindustrialization, unleashing energy dominance, advancing novel material substitution for critical components, and working with suppliers from trusted partners when domestic supply is not sufficient, increases the reliability and resilience of the technology support base.

In addition, relevant agencies should use available authorities to protect against adversary efforts to access and exploit critical technology systems and supply chains, including communications and networking systems. Important protective tools—which can indirectly enable development and promotion of trusted suppliers—include the Federal Communications Commission's Covered List, the Bureau of Industry and Security's Information and Communications Technology and Services Program, and the Federal Acquisition Security Council. Coordinating such measures with ally and partner governments, including as part of technology prosperity deals, will amplify U.S. efforts and bolster the resilience of shared technology infrastructure and supply chains.

Pillar 3: Accelerate the Pace of Innovation

The United States will make its S&T enterprise more agile. Agility sustains U.S. advantage in critical areas over time, denies advantage to adversaries as their capabilities evolve, and underwrites technological resilience. We will accelerate the pace of innovation and technology adoption in the national security arena by incentivizing contributions from private sector and academic innovators, removing unnecessary administrative and regulatory burdens, and accelerating acquisition reform.

Incentivize and enable innovators in all sectors to contribute to national security needs

Agencies must do more to encourage and reward rapid innovation and adaptation to prevent adversaries from upsetting U.S. strategic advantage through their own novel applications of technology. This should include developing rapid R&D funding mechanisms for CET areas, identifying opportunities to issue short-turnaround innovation challenge competitions without unnecessarily constraining the solution space, and rewarding private and academic sector participants who deliver solutions that meet priority mission needs.

Agencies should also incentivize and empower Federally-funded researchers to understand national security mission needs and develop innovative solutions. This should include:

- Increasing opportunities to engage with policy communities and national security operators, including at classified levels where appropriate, to increase researchers' understanding of mission needs and opportunities for improvement through innovation;
- Streamlining processes for researchers to patent inventions and discoveries;
- Strengthening pathways for researchers to commercialize intellectual property;
- Establishing internal competitions to incentivize and reward development of solutions to current and long-range challenges; and
- Enabling high-performing Federally-supported researchers to allocate a portion of their time toward national security innovation within their mission area.

Across sectors engaged in national security S&T, agencies should encourage technical risk-taking to enable discovery, and rapid learning through trial-and-error. This will require working to avoid, and in some cases reverse, overly risk-averse cultures imposed on Federally-funded R&D communities. It can also mean empowering project managers and researchers to "fail fast" and pivot to adjacent or complementary research areas. Agencies should explore opportunities for contract language that provides and promotes that kind of flexibility where appropriate.

Remove unnecessary administrative and regulatory burdens

Removing unnecessary administrative and regulatory burdens, while protecting safety and security, is essential to innovation and adaptation. Agencies will strengthen the national security S&T enterprise by:

- Updating or removing overly burdensome and outdated Federal regulations;
- Exercising and streamlining application of existing national security-specific authorities for waivers and exemptions—including for technology testing and evaluation—to advance national security priorities;

- Using advisory boards appropriately – as a source of advice and recommendations and not as mechanisms for imposing (even *de facto*) requirements onto programs; and
- Streamlining and accelerating security clearance processes for personnel and facilities, while ensuring they are thorough and reliable.

Accelerate acquisition reform

To achieve greater agility in the national security S&T enterprise, we must shorten development and acquisition cycles in the defense and broader national security sectors. President Trump's Executive Order 14265 on Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base underscores the need to "rapidly reform our antiquated defense acquisition processes with an emphasis on speed, flexibility, and execution." It directs the Department of War to reform acquisition processes and promote expedited and streamlined acquisitions. Executive Order 14369 on Ensuring American Space Superiority provides analogous direction to the Department of Commerce and NASA. Finally, Executive Order 14383 on Establishing an America First Arms Transfer Strategy incentivizes foreign investment to increase the capacity and responsiveness of America's defense industrial base. Implementing these directives will enhance the agility of the national security S&T enterprise.

For example, agencies should use Other Transaction Authorities (OTA) where appropriate for eligible research, prototype, and production projects. Where allowed and appropriate, agencies should utilize milestone-based fixed-cost contracting mechanisms, with multiple competing participants and performance-based down-select. In addition, agencies should explore opportunities to use a mix of contract mechanisms to advance mission objectives, including lower-risk but potentially slower traditional mechanisms and faster non-traditional approaches that may involve higher-risk but offer high potential reward.

Pillar 4: Protect National Security S&T

The United States will protect its S&T ecosystem from foreign theft, diversion, and exploitation that could impair U.S. economic and military strength and competitiveness. We will adopt approaches that protect without inhibiting the productivity and agility of the national security S&T enterprise. This strategy element includes strengthening research security, modernizing foreign investment screening and security, and strengthening and streamlining export controls and data transfer restrictions.

> *"America's pioneering spirit is a key pillar of our continued economic dominance and military superiority; it must be preserved."*
>
> – National Security Strategy of the United States, 2025

Strengthen research security

Some foreign governments exploit open U.S. and international research environments to circumvent the costs of research, increasing their economic and military competitiveness at the expense of the United States, its allies, and partners. During his first term, President Trump issued National Security Presidential Memorandum 33 (NSPM-33) on United States Government-Supported Research and Development National Security Policy. NSPM-33 directed action to strengthen U.S. Government-supported R&D against foreign interference and exploitation. While underscoring the imperative to maintain an open environment to foster discoveries and innovation that benefit our Nation and the world, NSPM-33 directed steps to protect intellectual capital, discourage research misappropriation, and ensure responsible management of U.S. taxpayer dollars. Key efforts included building threat awareness within research communities and ensuring that participants with significant influence on the U.S. R&D enterprise fully disclose information that can reveal potential conflicts of interest and conflicts of commitment.

America's R&D enterprise remains open and is more secure as a result of NSPM-33. Key measures that will further the work of President Trump's first administration in strengthening U.S. and international R&D include:

- Establishing processes to better track individuals and institutions that are direct and indirect recipients of Federal research funding;
- Prohibiting fundamental research funding to high-risk entities, including companies on the section 1260H list of Chinese military companies operating in the United States;
- Creating risk-based review criteria and a repository of sharable information to enhance the efficiency of information collection and sharing among agencies;
- Reducing regulatory burdens by creating universal research security reporting forms;

- Developing automated research security vetting of proposals for agency-funded research and continuous monitoring of funded research projects, where appropriate;
- Bolstering counter-intelligence support to governmental and non-governmental research centers; and
- Establishing cybersecurity guidelines for researchers and research institutions.

Deeper cooperation with allies and partners is essential to protecting America's innovation base. Through the technology prosperity deals, the United States and key partners have committed to share practices and information for identifying and mitigating threats to the research enterprise. Cooperation will include building capacity at research entities, strengthening threat analysis in key technology areas, and leading allies and partners toward similarly rigorous practices. Given the evolving nature of research security threats, security experts should embrace comprehensive, new, and novel security solutions, particularly where they can be crafted to address unique or nuanced requirements of specific technology fields. For example, the FBI-led Quantum Information Science and Technology Counterintelligence Protection Team brings an interagency team of quantum experts and security professionals to fine-tune technology protection and security outreach activities for the quickly evolving quantum R&D community.

Modernize foreign investment screening and security

The United States will maintain a strong, open investment environment that ensures that America leads in building the technologies of the future. The United States will continue to support, prioritize, and facilitate adoption and improvement of foreign investment security risk review mechanisms in ally and partner countries. For countries seeking to invest in or adopt American technology, relevant agencies should encourage mechanisms for consultation with the United States in their review regimes.

Some adversaries seek to exploit the United States' openness, directing investment into U.S. companies and assets to acquire cutting-edge technologies, sensitive information, intellectual property, and leverage in strategic industries. The Trump Administration is committed to further strengthening the Committee on Foreign Investment in the United States (CFIUS) to ensure that foreign investment in U.S. technology does not harm our national security.

President Trump's America First Investment Policy will modernize and strengthen CFIUS and other foreign investment screening and security mechanisms. CFIUS must be resourced, efficient, and empowered to address the full range of risks from foreign investment in U.S. technology. CFIUS should consider U.S. technology leadership in assessing risks, including with reference to the foreign availability, the feasibility of potential military and other national security applications, and the extent to which a transaction may advance or improve U.S. innovation, resilience, or security in critical technology domains.

To further U.S. technology leadership, the Trump Administration will seek, in consultation with Congress, to monitor certain "greenfield" investments that pose acutely high potential risks to national security, and to expand CFIUS's critical technology jurisdiction. In addition, the Trump Administration will promote information sharing throughout the U.S. Government, and engage with the private and academic sectors when appropriate, to bolster CFIUS's awareness of non-notified transactions involving sensitive, advanced, or emerging technologies.

As directed through President Trump's America First Investment Policy, CFIUS will focus or ease restrictions on foreign investment in proportion to an investor's verifiable distance and independence from the malign practices of foreign adversaries or threat actors. Likewise, the United States will invite, facilitate, and expedite foreign investment from allied and partner sources, especially in advanced technology and other important areas, to the extent that those investors avoid partnering with America's adversaries, align their activities with U.S. national security priorities, and adopt appropriate security or mitigation provisions. For specific transactions, such provisions could include mitigation measures requested or imposed by CFIUS, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom), or the Defense Counterintelligence and Security Agency regarding Foreign Ownership, Control, or Influence (FOCI).

The United States must additionally ensure that adversaries do not exploit America's capital markets and investors. Overseas investment offers returns to U.S. investors and great potential for economic growth. It can also enable technological development and upscaling by facilitating access to America's innovation and talent ecosystem, leading companies and financers, and large consumer base. These benefits of U.S. investment become national security vulnerabilities if they directly or indirectly advance adversaries' military and intelligence capabilities. In particular, China's military-civil fusion strategy aims to orient private commercial activity and even investment by U.S. persons toward achieving global technological dominance, including through coercive industrial policies and state security tools.

President Trump's America First Investment Policy underscores how the United States will utilize other tools, in addition to CFIUS, to stop adversaries from exploiting the benefits of American capital. First, the United States will use all necessary legal instruments to prevent U.S. persons from investing in foreign adversaries' military industrial sectors. Second, Treasury and other relevant agencies will implement and strengthen the Outbound Investment Security Program (Outbound), which Congress has cemented through the Comprehensive Outbound Investment National Security Act of 2025. As part of these efforts, the Trump Administration will continually evaluate how to refine Outbound restrictions on investment in areas including AI, quantum information systems, semiconductors, supercomputers, and hypersonics. The Trump Administration will expand Outbound to encompass additional restrictions on U.S. investments in other areas implicated by China's military-civil fusion strategy. Finally, relevant agencies should encourage ally and partner countries to adopt similar restrictions on investment in advanced technologies with military and intelligence applications, and should view such policies as favorable indications of verifiable distance from adversaries' predatory investment and technology-acquisition practices.

Strengthen and streamline export controls and data transfer restrictions

Export controls are a strategic instrument for shaping the global technology landscape by safeguarding leading-edge capabilities and influencing where and how critical technologies develop. They help strengthen U.S. and allied technological advantages to support national security, economic competitiveness, and innovation. The Trump Administration is focused on updating export controls to keep pace with emerging risks, evolving technologies, and the broader strategic environment. At the same time, the Administration seeks to eliminate or streamline outdated controls, ensuring that the rules do not unintentionally impede innovation, competitiveness, or the ability of U.S. companies to collaborate internationally and scale emerging technologies.

To that end, the Commerce Department's Bureau of Industry and Security (BIS) is pursuing several deregulatory export control actions. In January 2026, BIS issued an interim final rule to streamline controls for drone exports to allies and partners that maintain strong export control regimes, as directed through Executive Order 14307 on Unleashing American Drone Dominance.

Additional reforms to our national policy on implementation of the Missile Technology Control Regime may be appropriate to enable increased contributions by close allies and partners while still maintaining adequate protections. Agencies should coordinate and seek ways to strengthen and streamline export control regimes—particularly those governing arms transfers—as appropriate to better enable ally and partner contributions to the collective defense.

New approaches must also account for the evolving technology landscape, including the unlawful export of Americans' sensitive data. Such exports threaten national security when foreign actors use the data to conduct malign operations against the United States or to train certain AI capabilities. Relevant agencies should continue prioritizing the Data Security Program, established in May 2025 in response to the national emergency President Trump declared through Executive Order 13873. Through the Data Security Program and other tools, the United States will protect government-related data and bulk genomic, geolocation, biometric, health, financial, and other sensitive personal data of Americans against foreign adversary access and exploitation.

Strategy Implementation

America's unmatched S&T enterprise—including workforce and infrastructure—is the primary means of implementing the NSSTS. Targeted Federal R&D funding and mechanisms for effective partnership with the private and academic sectors will enable the S&T enterprise to meet national security needs. We will also leverage ally and partner S&T capabilities to strengthen U.S. security and enhance our collective defense.

S&T workforce

America will ensure a skilled cross-sector national security S&T workforce, and will leverage the broader S&T workforce to address national security challenges.

Strengthening education and training in science, technology, engineering, and mathematics (STEM) at all levels, as outlined in President Trump's Cyber Strategy for America and America's Talent Strategy, will bolster America's competitiveness in national security S&T. Relevant efforts include working with and encouraging non-Federal partners to:

- Enhance K-12 STEM education and professional teacher development:
    - Expand access to Advanced Placement courses; and
    - Incorporate age-appropriate CET concepts—including in AI, quantum, and space—into general science education and teacher development.
- Strengthen, expand, and encourage pathways for skilled trades and technicians:
    - Increase the number and capacity of trade and technician Registered Apprenticeships, co-ops, and internships, including in AI infrastructure and microelectronics;
    - Expand the use of existing training programs and curricula developed by and in coordination with industry; and
    - Facilitate partnerships between educational institutions, including community colleges, and industry to create new certifications, credentialing, and competency models for emerging fields, including AI infrastructure, quantum, biotechnology, and advanced nuclear reactor construction and operation.
- Prioritize critical national security S&T fields for higher education attention and investment:
    - Evolve undergraduate and graduate curricula to broaden and deepen exposure to quantum information science and other emerging fields;
    - Enhance AI fluency in degree requirements to equip students with AI-related competency across S&T fields;
    - Support existing Federal programs that encourage STEM careers, such as the Army STEM Education Consortium;
    - Increase and target scholarships and fellowships in designated CETs; and
    - Leverage scholarship-for-service programs to increase expertise, including in the Federal Government.

The United States will further strengthen its workforce by attracting and retaining top-tier global talent in critical national security S&T fields. Agencies will collaborate on using existing

authorities to recruit the exquisite talent necessary to ensure the national security S&T Enterprise leads the world in developing and applying these technologies.

We will also work to ensure necessary S&T expertise within the Federal workforce, utilizing the full range of available approaches for permanent and temporary access to expertise, including:

- Direct Federal hire, including through use of relevant special hiring authorities;
- Fellowship programs that sponsor temporary placement of early-career or experienced individuals in Federal laboratories or agencies;
- Internship and externship programs that temporarily place early-career individuals in Federal agencies for experience and exposure to career opportunities;
- Review of job qualifications to ensure that there are no unnecessary requirements, e.g., college degrees when certification would suffice; and
- Temporary assignment of non-Federal employees with needed S&T expertise to Federal agencies through the Intergovernmental Personnel Act mobility program.

Finally, we will accelerate the ability of experts to contribute to national security missions by expediting security clearance review for relevant Federal and non-Federal members of the national security S&T workforce, and by avoiding and working to roll back over-classification that unnecessarily constrains participation.

R&D infrastructure

The conduct of national security-supporting R&D depends on a diverse range of laboratories, research equipment, computational infrastructure, research databases, experimental facilities, and test and evaluation capabilities. Critical R&D infrastructure exists domestically within the Federal government, academic, and private sectors, as well as internationally.

Each relevant agency should review and reform its R&D enterprise to better support national security missions. These reviews should identify how R&D infrastructure can contribute to those missions, prioritize national security-supporting infrastructure for sustainment, accelerate adoption of AI/ML and digital engineering tools, and remove regulatory and administrative impediments. Agencies should coordinate their findings and plans to promote collaboration, avoid duplication, share costs, and enable rather than hinder commercial-sector innovation. To the extent possible and consistent with agency operations, security protections, laws, and regulations, agencies should enable U.S. companies, including small and nontraditional entities, to access Federal R&D infrastructure for activities aligned with U.S. national security needs.

Agencies should also work to maximize the ability of academic and private sector R&D infrastructure to contribute to national security missions, such as developing and promoting partnerships for the private sector to invest in relevant infrastructure.

Federal R&D funding

The Federal Government provides substantial funding for research and development. In alignment with the Fiscal Year 2028 R&D Priorities Memorandum, agencies should focus resources where they can best complement rather than compete with private sector investment; leveraging private funds to amplify outcomes when incentives are or can be aligned, and shouldering more of the burden to meet critical security needs where there is less incentive for private investment. That includes supporting fundamental and basic research in

the physical and biological sciences, in areas where there is insufficient commercial profit motive to drive scientific progress.

For early- and mid-stage development, agencies should pursue public-private partnerships, prioritizing the Appendix A technology areas, including AI, quantum, nuclear, biotechnology, and space. For later-stage development, agencies should in most cases rely still more on the private sector, including as a customer for technology solutions and services. Among the Appendix A technology areas, this might include advanced communications networks, advanced sensing capabilities, advanced manufacturing, future computing technologies, and PNT.

The Administration will coordinate with Congress to achieve and exercise greater agility for the Federally-funded S&T enterprise. This may include shifting R&D resources where necessary to align with National priorities and meet rapidly emerging security needs, including within budget cycles.

Partnerships with non-Federal stakeholders

Agencies will strengthen partnerships with industry, academia, and other non-Federal performers by:

- Establishing streamlined pathways for companies, including small and non-traditional performers, to secure Cooperative Research and Development Agreements (CRADAs) and Agreements for Commercializing Technology (ACTs);
- Streamlining technology transition processes by reforming reporting mechanisms for intra- and extra-mural intellectual property transfer to private industry;
- Ensuring alignment of University Affiliated Research Center (UARC) and Federally-Funded Research and Development Center (FFRDC) R&D missions with priority national security needs and strategy;
- Facilitating strategic capital investment structures aimed at enabling and accelerating the application of commercial technology to national security missions.
- Targeting the technical expertise and work of relevant Federal advisory groups toward implementation of the NSS and NSSTS;
- Protecting academic institutions and personnel from foreign adversaries, including safeguarding students and professors from recruitment and espionage efforts or undue influence by adversarial countries; and
- Supporting technology adoption, training, and interoperability among State, Local, Tribal and Territorial partners who provide critical services to the homeland.

Agencies should also explore pathways for U.S. partners to support national security technology development through passive investment.

Ally and partner capabilities

America benefits from networks of allies and partners with ability to contribute to our collective defense and a growing recognition of the need to do so. The United States will leverage S&T capabilities of international allies and partners as a force multiplier to advance national security objectives and outcompete adversaries.

For example, under bilateral technology prosperity deals, the Trump Administration is expanding cooperation in CET areas including AI, nuclear energy, quantum, advanced

communications, PNT, and space. We are also expanding cooperation on protective elements including research security, investment security, and supply chain security. The United States is similarly working with Australia and the United Kingdom to expand cooperation in CET areas, critical minerals and energy projects, and strengthening the U.S. submarine industrial base.

Adopting a balanced approach to export control and foreign military sales, as outlined under the technology protection element of this strategy, will work to protect against proliferation of advanced military capabilities to potential adversaries without handicapping the ability of U.S. allies and partners to contribute meaningfully to our collective defense and their own security.

Implementing the Strategy in Support of U.S. National Security

Implementing this NSSTS will support and enable the NSS and the National Defense Strategy. Focusing technology competition on battlefield advantage and countering strategic threats will posture the United States to defend the homeland and sustain deterrence in the Indo-Pacific.

Agencies should plan their national security S&T activities in a manner consistent with this strategy. For CETs listed in Appendix A, OSTP and NSC will coordinate supporting technology-specific strategies or plans at the next level of detail. Technology-specific plans should address how the United States can advance the NSSTS within that area, and should account for competitor moves and countermoves.

Congressional support is essential. The Administration will engage with Congress on authorizing and appropriating relevant funding and on legislative initiatives that enable a focused, resilient, agile, and secure national security S&T enterprise.

"In the long term, maintaining American economic and technological preeminence is the surest way to deter and prevent a large-scale military conflict."

– *National Security Strategy of the United States, 2025*

Appendix A: Critical and Emerging Technologies List Update

Critical and emerging technologies (CETs) are a subset of advanced technologies that are or may become critically important to U.S. national security. This is a narrower focus than listing all technologies relevant or even important to national security. Each identified CET area includes a set of subfields that illustrate its scope but are not meant to be comprehensive. Relevant departments and agencies should include, within their R&D activities, a dedicated focus on maintaining U.S. leadership in identified CET areas, and within national security S&T should prioritize their application toward supporting and enabling national security objectives.

Advanced manufacturing and materials

- Advanced additive manufacturing beyond prototyping, especially for metals, ceramics, and large-scale structures
- Smart manufacturing and use of digital threads and digital twins
- Nanomanufacturing
- Materials by design utilizing AI and autonomous development and production
- High entropy alloys
- Advanced composites and lightweight metals
- Materials with novel, tailored, and improved properties, including biomaterials and substitution of rare-earth or critical minerals-based alloys with earth-abundant minerals

Artificial intelligence (AI) and autonomy

- Perception, recognition, and sensor fusion
- Planning, reasoning, and decision-making
- Robotics and embodied intelligence
- Foundation models, including large language, multimodal, and world systems
- Multi-agent systems and swarm intelligence
- Autonomous systems for surface, air, maritime, space, and cyber domains
- Autonomous command and control
- Autonomous agent identification and authentication
- Interpretability and control
- Adversarial robustness and AI security
- Techniques to enable next-generation AI systems, such as continual learning
- Distributed and privacy-preserving machine learning

Biotechnology

- Novel synthetic biology including nucleic acid synthesis; genome and epigenome engineering; protein design, synthesis, and engineering; and computational modeling
- Engineering of sub-cellular, multicellular, multi-scale, cell-free, and viral systems
- Novel therapeutic design and manufacturing
- Biotic/abiotic interfaces and novel materials
- Biomanufacturing and bioprocessing technologies
- Neurotechnologies

Communications and networking

- Future generation wireless networks
- Optical links and fiber technologies
- Spectrum access technologies
- Software-defined networking and radios
- Modern data exchange techniques
- Adaptive network controls
- Resilient and path-diverse communications, including delay-tolerant and infrastructure-independent networking, adaptive waveforms, and space and stratospheric modalities

Directed energy

- Lasers
- High-power microwaves
- Particle beams

Future computing technologies

- Advanced and next-generation computing architectures
- Photonic, neuromorphic, and other non-Von Neumann computing modalities
- High-performance supercomputing, including for AI applications
- Edge computing and devices for tactical environments
- Brain-computer interfaces
- Enabling technologies for high security computing
- Hardened operating systems for consumer use
- Advanced spatial computing

Hypersonics and advanced missile technologies

- Propulsion
- Aerodynamics and control
- Materials, structures, and manufacturing
- Testing
- Detection, tracking, characterization, and defense

Information management and cybersecurity

- Data management, including storage and security
- AI-enabled and autonomous cyber capabilities
- Distributed ledger technologies and digital assets
- Digital identity technologies and biometrics
- Computing supply chain security and assurance
- Communications, network, and cyber-physical systems security
- Post-quantum cryptography
- Operational technology and industrial control system security and resilience

Nuclear energy

- Advanced fission reactors
- Fusion energy

- Space nuclear power and propulsion systems
- High-temperature and radiation resistant materials

Positioning, navigation, and timing (PNT)

- Diversified PNT-enabling technologies for airborne, space-based, terrestrial, subterranean, and underwater settings
- Interference, jamming, and spoofing detection
- Disruption/denial-resisting and hardening technologies
- Chip-scale frequency standards, inertial sensors, and atomic clocks

Quantum information technologies

- Quantum computing
- Quantum sensing
- Quantum communications and networking
- Enabling components, algorithms, materials, and fabrication techniques

Semiconductors and microelectronics

- Design automation tools
- Advanced manufacturing process technologies and equipment
- Beyond complementary metal-oxide-semiconductor (CMOS) technology
- Heterogeneous integration and advanced packaging
- Specialized hardware components for AI, RF and optical applications, elevated radiation environments, high-power devices, and other critical applications
- Novel materials for advanced microelectronics, including 2D materials
- Microelectromechanical and Nanoelectromechanical systems (MEMS and NEMS)
- Integrated photonics

Sensing and signature management

- Advanced sensors and sensor systems, including distributed apertures
- Data processing and fusion
- Adaptive optics
- Detection and characterization of pathogens and of chemical, biological, radiological, and nuclear weapons and threat materials

Space technologies

- Cost-effective on-demand and reusable space launch
- Advanced space vehicle power generation and propulsion
- Novel space vehicle thermal management
- Access to and use of cislunar space and novel orbits
- In-space aggregation and assembly
- Biotechnologies for space applications
- Crewed spaceflight enablers

Appendix B: Alignment of Critical and Emerging Technologies with Priority National Security Needs

Critical and emerging technology (CET) areas support and enable elements of the NSSTS. Most have significant implications that are readily apparent in the current security environment. In some cases (denoted by parenthesis in the table below), specific implications have yet to emerge but are on the horizon.

Critical and Emerging Technology Areas	*Maintain and advance U.S. technological advantage on the battlefield*			*Protect the homeland and deny strategic advantage to adversaries*				*Lead in trans-formative ET*
	Space; Air; Long-range strike	Under-sea	Nat. sec. AI & auto-nomy	Border sec.	Nuclear deter-rence; Missile defense	Cyber def.	BW def.	
Advanced manuf. & materials	✓	✓			✓		✓	
AI & autonomy	✓	✓	✓	✓	✓	✓	✓	✓
Biotechnology				✓			✓	✓
Communications & networking	✓	✓	✓	✓	✓	✓		
Directed energy	✓				✓			
Future computing	✓	✓	✓	✓	✓	✓	✓	
Hypersonics & advanced missiles	✓		✓		✓			
Information security & cybersecurity	✓	✓	✓	✓	✓	✓	✓	
Nuclear energy	✓	✓			✓			
Quantum information	(✓)	(✓)			(✓)	(✓)		✓
PNT	✓	✓	✓	✓	✓	✓		
Semiconductors & microelectronics	✓	✓	✓	✓	✓	✓		
Sensing & signature management	✓	✓	✓	✓	✓	✓	✓	
Space technologies	✓	✓	✓	✓	✓	✓		

The WHITE HOUSE