Free markets. Real solutions.

R Street works to identify and advocate for free markets and limited, effective government policies that improve cybersecurity (like minimizing the regulatory burden placed on industry) while maximizing opportunities for innovation.

EXPLAINER

Key Cybersecurity and AI Policy Priorities for Trump's Second Administration and the 119th Congress

January 2025

Background

As emerging technologies like artificial intelligence (AI) continue to shape our digital landscape, cybersecurity is quickly becoming an interdisciplinary challenge, where evolving threats transcend industries and borders. Moreover, individuals, companies, and governments are not only finding ways to use technology and AI to improve our lives, but also to improve cybersecurity. Still, threat actors, unbound by ethical or regulatory constraints, can leverage AI for nefarious purposes, including targeting critical infrastructure sectors, so it is imperative that we stay ahead of such actors in this arena.

R Street works to identify and advocate for free markets and limited, effective government policies that improve cybersecurity (like minimizing the regulatory burden placed on industry) while maximizing opportunities for innovation. While we work on a range of cyber-related and data privacy topics, two are particularly ripe for action in 2025.

I. Advancing Cybersecurity Regulatory Harmonization

Numerous federal agencies, industry regulators, and standalone state and federal laws set forth cyber requirements around incident reporting and baseline security requirements. This has led to duplicative—even contradictory—requirements and has created an opportunity to improve our cyber posture, free cybersecurity teams of the burden of excessive compliance tasks, and promote government efficiency. Specific recommended actions include:

1. Establishing a Clear Expectation for Cybersecurity Regulatory Harmonization

- Define a comprehensive end goal for harmonization, including establishing the scope of what should be covered and considering reciprocity or uniform baseline security requirements across sectors in a way that is not onerous but, instead, reasonable for companies of all sizes.

2. Empowering a Coordinating Authority for Cyber Harmonization

- No single central entity currently has the authority to bring independent regulators to the table. Congress could grant such authority to an entity like the Office of the National Cyber Director so that it could establish and pilot baseline security rules and incident-reporting requirements to reduce duplicative and contradictory rules. The Department of Government Efficiency should coordinate with related Hill committees on deregulation and regulatory-alignment efforts and resolve interagency conflicts in the context of broader efforts.

II. Harnessing AI's Potential: Balancing Risks and Rewards

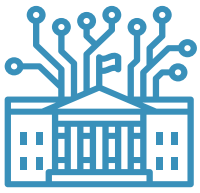
Continued advances in AI are redefining industries and reshaping national security priorities, offering transformative opportunities for innovation, efficiency, and resilience. In cybersecurity, AI has already compressed cybersecurity incident analysis time from minutes to milliseconds and promises to identify never-before-seen threats and vulnerabilities through predictive threat intelligence.

These benefits, however, are paired with risks that demand our attention. AI systems are susceptible to exploitation—whether through adversarial attacks, weaponization, data poisoning, or unintentional breaches of the infrastructure supporting their use. Left unchecked, these vulnerabilities can disrupt critical infrastructure operations and expose sensitive data. To maintain our technological leadership, military advantage, and international influence, we must adopt strategies that harness AI's potential while balancing the need for safeguards against emerging threats. Congress, federal agencies, and the White House all have a role in striking this balance, and those roles overlap at times. Specific recommended actions include:

1. Promoting Responsible AI Use

- The White House, Congress, and relevant agencies should account for cybersecurity risks in AI systems while also evaluating their applications, such as digital twins, along with their limitations and benefits. This includes avoiding inadvertently limiting AI uses in cybersecurity, as some proposals have done, and distinguishing between exaggerated fears and genuine risks.

Free markets. Real solutions.



To maintain our technological leadership, military advantage, and international influence, we must adopt strategies that harness AI's potential while balancing the need for safeguards against emerging threats. Congress, federal agencies, and the White House, all have a role in striking this balance, and those roles overlap at times.

EXPLAINER

Key Cybersecurity and AI Policy Priorities for Trump's Second Administration and the 119th Congress

January 2025

- The White House, Congress, and relevant agencies should incorporate risk-tolerance principles—which involve defining acceptable risks—into any AI regulation and governance solutions. Congress should direct the National Institute of Standards and Technology (NIST) to collaborate with stakeholders across industry, academia, and the public to develop and advance voluntary best practices for improved transparency and oversight in AI applications.
- The White House, with support from Congress, should modernize legacy systems throughout the government to ensure that these systems can support both emerging security updates and responsible-use standards.

2. **Issuing Federal Guidance Clarifying Key Ambiguities in AI Development and Use**
   - NIST and the Cybersecurity and Infrastructure Security Agency (CISA) should define permissible actions for researchers in security-centric AI development across public and private sectors.
   - The Department of Defense, in collaboration with other agencies like the National Security Agency (NSA), should expand offensive cyber capabilities to improve deterrence and attribution.
   - NIST should establish risk-tolerance parameters for federal entities to guide AI implementation.
   - NIST, in collaboration with CISA, should develop a voluntary framework to guide state and local governments in evaluating and addressing AI-related security and safety concerns.
3. **Securing U.S. Data from Foreign Adversaries**
   - Congress, in coordination with the Department of Energy (DOE), should prioritize the expansion of secure, domestically operated data centers to reduce U.S. reliance on foreign-sourced hardware and infrastructure across public and private sectors.
   - The White House should direct agencies like NIST and CISA to establish clear standards for secure collection, storage, and handling protocols for AI training datasets to prevent tampering, data poisoning, and unauthorized access across private and public sectors.
4. **Facilitating Cross-Sector Partnerships and Fostering Stakeholder Engagement and Research**
   - Congress should fund partnerships between agencies (e.g., NIST, DOE, National Science Foundation) and stakeholders across industry, academia, and the public to gain insights into the real-world impact of AI technologies, including opportunities and risks of combining large language models with other AI and legacy cybersecurity capabilities.
   - NIST should develop reliable metrics for assessing data security, AI model protection, and resilience against attacks, providing a foundation for consistent audits across sectors.
   - CISA, in coordination with the Federal Bureau of Investigation and the NSA, should leverage AI-driven cloud security innovations for enhanced threat detection, posture management, and configuration enforcement.
5. **Prioritizing Industry-Specific Frameworks and Risk Assessments**
   - CISA, with sector-specific agencies, should develop tailored AI security frameworks and risk assessments that address unique industry needs and vulnerabilities, prioritizing the proactive identification and mitigation of supply chain vulnerabilities, critical infrastructure risks, and security threats to AI ecosystems, avoiding a top-down regulatory approach.
6. **Addressing the Cybersecurity and AI Workforce Challenge**
   - Congress should support legislation to upskill the workforce and develop incentives for businesses to implement training and reskilling programs that prepare non-technical workers to work in an AI-enabled economy.
   - Federal agencies should revise hiring policies to attract technical talent, streamline security clearance processes, and offer competitive incentives to recruit and retain top AI and cybersecurity talent.

Contact us

For more information, please contact:

Haiman Wong
Resident Fellow
Cybersecurity and Emerging Threats
hwong@rstreet.org

Brandon Pugh
Policy Director and
Resident Senior Fellow
Cybersecurity and Emerging Threats
bpugh@rstreet.org