President Trump's Cyber Strategy for America: An Analysis of Pillar 2, Promote Common Sense Regulation

Morgan Brown

School of Cybersecurity

Cyber Strategy and Policy

Professor Cooper

September 27, 2026

I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community, it is my responsibility to turn in all suspected violations of the Honor Code.

Introduction

Cybersecurity has become an important component of United States national security because government operations, economic activity, critical infrastructure, and everyday life increasingly depend on interconnected digital systems. In March 2026, the Trump administration released President Trump's Cyber Strategy for America to establish the administration's priorities for addressing cyber threats and strengthening U.S. interests in cyberspace (The White House, 2026). The strategy describes cyberspace as essential to American economic opportunity, technological development, military power, manufacturing, and national security while identifying adversaries and cybercriminals as continuing threats to these interests (The White House, 2026). Rather than limiting cybersecurity to federal computer networks, the strategy presents it as a national effort involving government, private industry, academia, state and local authorities, international partners, and individual Americans. The strategy organizes its priorities into six policy pillars that collectively establish its approach to cybersecurity and provide the basis for subsequent policy actions (The White House, 2026). Examining the strategy provides an opportunity to understand the administration's cybersecurity priorities while considering the policy implications of one of its central approaches to regulating private-sector cybersecurity.

Overview of the Six Policy Pillars

The first pillar, Shape Adversary Behavior, focuses on using U.S. defensive and offensive cyber capabilities, private-sector participation, and other instruments of national power to disrupt adversaries and cybercriminal organizations and impose consequences for malicious activity (The White House, 2026). The second pillar, Promote Common Sense Regulation, seeks to streamline cybersecurity and data regulations, reduce compliance burdens, address liability, and improve coordination between regulators and

industry while emphasizing privacy for Americans and American data (The White House, 2026). The third pillar, Modernize and Secure Federal Government Networks, focuses on strengthening federal information systems through cybersecurity best practices, zero-trust architecture, post-quantum cryptography, cloud migration, artificial intelligence, and improved technology procurement (The White House, 2026). The fourth pillar, Secure Critical Infrastructure, emphasizes protecting essential infrastructure and supply chains, including energy, financial, telecommunications, water, healthcare, and defense-related systems (The White House, 2026). The fifth pillar, Sustain Superiority in Critical and Emerging Technologies, addresses the security of technologies such as artificial intelligence, quantum computing, cryptocurrency, and blockchain while emphasizing American technological leadership and innovation (The White House, 2026). Finally, the sixth pillar, Build Talent and Capacity, seeks to strengthen the cybersecurity workforce through greater cooperation among government, industry, academia, technical schools, and the military (The White House, 2026).

Policy Focus: Pillar 2 | Promote Common Sense Regulation

Although all six pillars contribute to the strategy's overall approach, Pillar 2 presents particularly important questions concerning the relationship between government regulation and private-sector cybersecurity responsibilities. The strategy argues that cyber defense should not become a costly compliance exercise that delays an organization's ability to prepare for, respond to, and recover from threats (The White House, 2026). At the same time, the strategy identifies privacy and the protection of American data as continuing priorities, creating a policy tension between regulatory flexibility and security protections. This approach is significant because private

organizations operate many of the systems and services that are important to national security and economic activity. The effectiveness of the strategy therefore depends partly on how government and private organizations divide cybersecurity responsibilities. This paper examines Pillar 2 by analyzing its regulatory approach, rationale, policy implications, and the challenges involved in balancing flexibility with accountability.

Policy Overview: President Trump's Cyber Strategy for America

Pillar 2 establishes the administration's approach to cybersecurity regulation and its relationship with private industry. Rather than treating regulation as the primary means of securing private-sector systems, the strategy seeks to reduce requirements that it considers unnecessary while improving coordination between government and industry (The White House, 2026). The following subsection examines the rationale for this approach and the responsibilities it assigns to government and private organizations.

Purpose and Strategic Approach

President Trump's Cyber Strategy for America establishes the Trump administration's overall approach to protecting U.S. interests in cyberspace and identifies priorities that will guide subsequent cybersecurity actions and resources (The White House, 2026). The strategy presents cyberspace as an important part of American economic opportunity, technological innovation, military power, manufacturing, and national security. It also identifies adversaries and cybercriminals as threats capable of disrupting essential services, imposing economic costs, and affecting Americans, businesses, and critical infrastructure. Rather than limiting cybersecurity to the protection of government networks, the strategy describes a broader effort involving federal agencies, private industry, academia, state and local authorities, international partners,

and individual Americans. This approach reflects the interconnected nature of modern cyberspace, where responsibility for security is distributed among organizations that operate and depend upon digital systems. The strategy therefore establishes a national framework intended to coordinate government action, private-sector participation, technological development, and international engagement in response to evolving cyber threats (The White House, 2026).

The strategy's overall approach emphasizes proactive defense, resilience, technological leadership, and cooperation across the public and private sectors. It states that the United States will use defensive and offensive cyber capabilities, work with international partners, strengthen federal systems and critical infrastructure, and promote the development of secure emerging technologies (The White House, 2026). At the same time, the strategy places significant emphasis on reducing what it characterizes as burdensome and ineffective regulations so that private organizations can respond more rapidly to changing cyber threats. This regulatory approach is connected to the strategy's broader goal of encouraging innovation and maintaining American technological and economic advantages. The strategy also recognizes that cybersecurity responsibilities cannot rest exclusively with the federal government and calls for greater cooperation between public and private organizations (The White House, 2026). These priorities establish the foundation for examining how the strategy balances government involvement, private-sector responsibility, security requirements, and individual interests.

Pillar 2: Promote Common Sense Regulation

The second pillar of President Trump's Cyber Strategy for America focuses on the role of federal regulation in protecting the nation's digital systems and information. The strategy argues that cybersecurity requirements should strengthen organizations' ability to defend themselves rather than create administrative processes that interfere with timely preparation and response (The White House, 2026). It therefore emphasizes reducing compliance burdens, addressing liability, improving coordination between regulators and industry, and maintaining protections for Americans' privacy and data (The White House, 2026). Examining this pillar provides an opportunity to consider how the strategy attempts to balance cybersecurity objectives with the government's regulatory role and the private sector's responsibility for protecting many of the systems on which the country depends.

Regulatory Approach and Rationale

Pillar 2 begins with the position that cybersecurity should not be reduced to a costly checklist that interferes with an organization's ability to respond to threats (The White House, 2026). The strategy therefore calls for streamlining cybersecurity regulations, reducing compliance burdens, addressing liability, and improving coordination between regulators and industry. This approach is based on the view that private organizations need sufficient flexibility to adapt their security practices as technologies and cyber threats change. The strategy also seeks to reduce duplication among regulatory requirements so that organizations can devote more attention and resources to actual cybersecurity rather than overlapping compliance activities (The White House, 2026). The Government Accountability Office provides evidence that regulatory duplication is a legitimate policy concern, identifying 117 cybersecurity

regulations affecting private entities across nine critical infrastructure sectors and finding that 80 of those regulations, approximately 70 percent, contained reporting requirements that overlapped with requirements in other regulations (U.S. Government Accountability Office, 2026). These findings provide context for Pillar 2 because they demonstrate how multiple cybersecurity requirements can create overlapping reporting responsibilities for organizations operating critical infrastructure.

The regulatory approach also reflects a broader question concerning how government and private organizations should share responsibility for cybersecurity. Private organizations often possess specialized knowledge about the systems they operate, while government agencies have broader responsibilities for addressing risks that can affect national security and the public. McCarthy (2018) describes cybersecurity as existing at the intersection of public security concerns and private interests involving property rights and civil liberties. This relationship creates a challenge for policymakers because increasing government control may strengthen oversight while also placing greater restrictions on organizations that operate privately owned infrastructure. Conversely, relying too heavily on private-sector discretion may create differences in cybersecurity practices and leave some risks insufficiently addressed. Pillar 2 therefore does not eliminate government involvement in cybersecurity; instead, it proposes changing the government's role from one focused on extensive regulatory requirements toward greater coordination, streamlined requirements, and private-sector flexibility (The White House, 2026).

Policy Implications of Pillar 2

One major implication of Pillar 2 concerns the potential effect of regulatory flexibility on cybersecurity investment and effectiveness. Reducing unnecessary requirements could allow organizations to redirect resources toward security measures that better reflect their individual systems, risks, and operational needs. This flexibility may be particularly valuable in cybersecurity because threats and technologies can develop faster than traditional regulatory processes. However, regulation can also establish minimum expectations for organizations that may otherwise underinvest in cybersecurity. Gordon et al. (2015) explain that the effectiveness of government incentives and regulations depends partly on whether organizations are already using appropriate cybersecurity practices and whether they are willing and able to increase their investments. This suggests that regulatory reform may produce different results among organizations with different levels of resources, expertise, and existing cybersecurity capabilities. Consequently, reducing regulatory requirements does not necessarily mean that cybersecurity outcomes will improve or decline uniformly; the effects depend on how organizations respond to the greater flexibility.

Cybersecurity Effectiveness and Regulatory Flexibility

Another implication concerns accountability. Cybersecurity risks do not always remain within the boundaries of the organization that experiences a vulnerability or incident because interconnected systems can create consequences for customers, business partners, critical infrastructure, and other organizations. A company may therefore have private control over a system while its cybersecurity decisions affect broader public interests. This creates a challenge for a regulatory framework that seeks to provide organizations with greater discretion while maintaining adequate national cybersecurity

protections. The strategy addresses this issue by retaining a federal role in establishing cybersecurity policy while seeking to eliminate regulations that it considers burdensome or ineffective (The White House, 2026). The GAO's findings concerning overlapping reporting requirements demonstrate that reducing duplication could address administrative burdens, but regulatory reform must also preserve requirements that provide meaningful security information and accountability (U.S. Government Accountability Office, 2026). The policy challenge is therefore not simply whether regulations should be reduced but whether the remaining regulatory framework continues to encourage organizations to address risks that extend beyond their individual interests.

Privacy and Data Protection

Privacy and data protection represent another important consideration within Pillar 2. The strategy explicitly states that it will emphasize the right to privacy for Americans and American data while pursuing greater flexibility in cybersecurity and data regulation (The White House, 2026). These objectives can create competing considerations because cybersecurity organizations may need to collect, process, or share information to identify and respond to threats, while excessive collection or use of information can create privacy concerns. McCarthy (2018) notes that cybersecurity policy exists alongside concerns involving civil liberties, demonstrating that security decisions can have consequences beyond the technical protection of systems. The strategy's inclusion of privacy indicates that reducing regulation is not intended to remove all protections for personal information. Instead, Pillar 2 seeks to distinguish between regulations that contribute to meaningful cybersecurity and those that impose burdens without providing comparable security benefits (The White House, 2026).

Maintaining that distinction will be important because a regulatory system that promotes flexibility without adequately protecting personal information could create a different set of cybersecurity and civil-liberties concerns.

Critical Analysis of Pillar 2

The central policy issue presented by Pillar 2 is how to balance regulatory flexibility with accountability. The strategy's argument for reducing unnecessary and duplicative requirements has support in the documented existence of overlapping cybersecurity reporting requirements identified by the GAO (U.S. Government Accountability Office, 2026). Streamlining such requirements could reduce administrative costs and allow organizations to focus resources on security activities rather than duplicative reporting. However, regulatory requirements also serve a purpose by establishing expectations that can encourage organizations to address cybersecurity risks consistently. Gordon et al. (2015) demonstrate that government policies can influence private-sector cybersecurity investment, which indicates that removing requirements may affect organizational incentives as well as administrative workloads. The effectiveness of Pillar 2 will therefore depend on whether regulatory reform removes unnecessary burdens while preserving requirements that provide meaningful incentives and protections. A successful implementation would need to distinguish between regulation that merely creates duplication and regulation that addresses risks that private organizations may have insufficient incentives or resources to manage independently.

Implementation Considerations

Implementation will also be important because the strategy establishes broad objectives rather than providing a detailed regulatory framework for every sector. The strategy calls for agencies to streamline cybersecurity regulations and improve

coordination with industry, meaning that subsequent actions will determine how these objectives affect individual organizations (The White House, 2026). Agencies will need to identify which requirements are duplicative, determine which protections remain necessary, and coordinate across regulatory authorities. This process could be complicated because cybersecurity requirements differ among critical infrastructure sectors and because organizations may be subject to requirements from multiple federal agencies. The GAO's findings demonstrate the scale of this issue and provide evidence that regulatory coordination could address genuine areas of overlap (U.S. Government Accountability Office, 2026). Implementation must therefore involve more than simply reducing the number of regulations; it must ensure that the remaining requirements provide clear expectations and continue to address significant cybersecurity risks.

Conclusion

President Trump's Cyber Strategy for America establishes a national cybersecurity framework organized around six policy pillars addressing adversary behavior, regulation, federal networks, critical infrastructure, emerging technologies, and workforce development (The White House, 2026). Within that framework, Pillar 2, Promote Common Sense Regulation, seeks to change the government's approach to cybersecurity regulation by reducing unnecessary requirements, addressing liability, improving regulatory coordination, and providing private organizations with greater flexibility. The strategy's approach responds to concerns about regulatory burdens while maintaining privacy and data protection as policy priorities. Evidence from the GAO indicates that overlapping cybersecurity reporting requirements exist across multiple critical infrastructure sectors, providing a concrete policy context for the strategy's emphasis on regulatory streamlining (U.S. Government Accountability Office, 2026). At the

same time, research concerning government regulation and private-sector cybersecurity investment demonstrates that regulatory changes can affect organizations differently depending on their existing practices and ability to invest in security (Gordon et al., 2015). Pillar 2 therefore presents a significant policy challenge involving the appropriate balance between regulatory flexibility, cybersecurity investment, accountability, and government oversight.

The broader significance of Pillar 2 is its treatment of cybersecurity as a shared responsibility between government and private organizations. The federal government retains responsibility for establishing national cybersecurity priorities, while private organizations remain responsible for protecting many of the systems and services on which the country depends. Reducing unnecessary regulatory requirements may provide organizations with greater flexibility to respond to changing threats, but that flexibility must be accompanied by sufficient accountability to ensure that important cybersecurity risks are not neglected. The strategy's emphasis on privacy also demonstrates that cybersecurity regulation involves considerations beyond protecting networks and systems, including the protection of individual information and civil liberties (The White House, 2026; McCarthy, 2018). Ultimately, Pillar 2 represents an effort to restructure the relationship between government regulation and private-sector cybersecurity rather than simply reducing government involvement. Its policy significance will depend on whether the administration can streamline regulatory requirements while maintaining the security expectations, incentives, and protections necessary to address risks that extend beyond individual organizations.

References

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), tyv011. https://doi.org/10.1093/cybsec/tyv011

McCarthy, D. R. (2018). Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

The White House. (2026). President Trump's Cyber Strategy for America. In *www.whitehouse.gov*. The White House. https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf

U.S. Government Accountability Office. (2026). U.S. GAO - cybersecurity regulations: Multiple sectors are subject to potentially duplicative reporting requirements. In *Cybersecurity Regulations: Multiple Sectors Are Subject to Potentially Duplicative Reporting Requirements*. Government Accountability Office. https://www.gao.gov/products/gao-26-108606